MASSACHUSETTS Lawyers Weekly

More on cybersecurity and the rules of professional conduct

By: Thomas E. Peisch and Erin K. Higgins April 9, 2015

Ethical Questions & Dilemmas is a regularly appearing column devoted to the subject of lawyer ethics and the Rules of Professional Conduct.

In the first installment of this column (Feb. 23 issue), we discussed recent changes to the Massachusetts Rules of Professional Conduct that explicitly recognize a lawyer's obligation to guard against hacking and other attacks on electronically stored information. Those changes (and other important changes to the Rules of Professional Conduct) will go into effect on July 1.

We also made recommendations regarding steps that Massachusetts lawyers can take to safeguard their clients' confidential information. A lawyer's duties of confidentiality (Rule 1.6), competence (Rule 1.1), and safekeeping (Rule 1.15) are all implicated in that endeavor. We cautioned against the "head in the sand" attitude about technology that is common among attorneys.

So what happens when the lawyer's "reasonable" efforts, now required by new Rule 1.6(c), fail to prevent an attack or breach? What are the lawyer's obligations when a third party wrongfully obtains access to confidential information, or when a lawyer's own inadvertence, or that of his information technology vendor, results in a breach?

Practically speaking, we recommend a three-part response: assessment, disclosure and remediation.

• **Assessment.** This is the first step in response to an apparent breach. What has been hacked or accessed? Is it financial information, medical records or something else? Has the data loss stopped, or is there something else that needs to be done to stop additional data loss?

The attorney's first step should be to document what happened in connection with the breach, and the commencement of response efforts. Record the date and time the breach was discovered, all facts known about the breach, and the date and time when the lawyer began an investigation into the matter.

A lawyer should immediately report the breach to the firm's risk management partner (or managing partner, if there is no designated risk management partner). All affected machines (computers, laptops, tablets and mobile phones) should be taken offline and secured for future investigation.

If there is a breach of the firm's firewall, the firm likely will need to shut down its network to prevent further incursion, while an investigation is being undertaken.

At this point, the lawyer should bring in expert assistance, in the form of a technology vendor with experience in investigating data breaches. The lawyer should work with the vendor to establish a plan for determining the scope of the data loss, the number of affected clients, and whether efforts can be made to retrieve the lost data.

If the firm has no disaster recovery plan in place, a sophisticated vendor may be able to work with the lawyer or law firm to find some way to get the computer network back up and running, so that the attorney can continue to service clients while the data breach is under investigation.

• **Disclosure.** A lawyer's duty to disclose information regarding a data breach stems from both the Rules of Professional Conduct and pertinent state law. Rule 1.4 requires a lawyer to keep the client "reasonably informed" regarding the status of the lawyer's engagement.

The broad requirement of "diligence" also is implicated here. See Rule 3.1. More explicitly, G.L.c. 93H, §3 requires that any person who maintains or stores data that includes personal information about a Massachusetts resident,

and knows or has reason to know of a data breach involving that information, must inform the "owner" of the data, presumably the client, of the data breach. *Id.*

Additionally, there is pending federal legislation that, if enacted, would mandate similar data breach reporting on a national scale. See Jason C. Gavejian, "The Data Security and Breach Notification Act of 2015," The National Law Review (April 3, 2015), http://www.natlawreview.com/print/article/data-security-and-breach-notification-act-2015.

Notice to clients should be provided as soon as reasonably practicable. However, since a lawyer may not immediately apprehend the extent of the data breach, he may not be in a position to make disclosure to all affected clients until a forensic investigation has been completed.

In that regard, if the data breach appears extensive, the lawyer may want to consider retaining outside counsel to advise on disclosure obligations. A firm may need to consider hiring a public relations expert to manage any fallout from an extensive breach, including an assessment of whether the firm should issue any kind of press release or post information on its website about the steps that are being taken by the firm to assist affected clients and to prevent such breaches from occurring in the future.

The lawyer also should promptly notify his malpractice carrier of the incident. While the malpractice policy may exclude or limit coverage for claims arising out of a data breach, a lawyer should not forfeit any coverage available under a malpractice policy by failing to provide prompt notice.

If the lawyer had the foresight and financial wherewithal to purchase separate "cyberliability" coverage, he obviously should provide notice under that policy as well.

Finally, the attorney should consider notifying appropriate law enforcement authorities, as any unauthorized hacking likely is a criminal act. The lawyer will need to be careful in any subsequent investigation, however, to limit law enforcement access to confidential client information.

● **Remediation.** The process of fashioning a remedy for a breach should begin as soon as the breach is revealed, and should begin even before or at the same time the client is notified. The lawyer's information technology service provider is obviously the first and best source for help.

The lawyer will need to identify and correct any deficiencies in his methods of protecting electronically stored information. Typical deficiencies include the failure to encrypt information when it leaves the lawyer's office, the failure to require and use "strong" and frequently changed passwords, the use of multiple devices to store and send client information, and the failure to train attorneys and employees on the importance of following security protocols.

Note that any changes in protocol following a data breach event must be documented in the lawyer's written information security program, or WISP, as required by 201 CMR 17.03(j).

It is becoming increasingly clear that hacking attacks are here to stay as electronic communications become more a part of a lawyer's daily life. A sophisticated hacker likely will be able to penetrate even the most sophisticated of storage systems.

As outlined in this two-part column, however, a lawyer must take reasonable steps to protect against an incursion and to address the effects of such an incursion on clients. By doing so, the lawyer also may minimize his exposure (or his law firm's exposure) in the event of a data breach.

Thomas E. Peisch and Erin K. Higgins are partners at Conn, Kavanaugh, Rosenthal, Peisch & Ford in Boston, where they advise and defend lawyers and law firms on liability and ethical issues. Peisch is a former vice chairman of the Board of Bar Overseers.

Issue: APRIL 13 2015 ISSUE

Arguing dispositive motions remotely in COVID times

July 23, 2020

Excellence in the Law 2020

July 17, 2020

The Most Important Opinions: January – June 2020

July 9, 2020