MASSACHUSETTS Lawyers Weekly

Cybersecurity and the rules of professional conduct

By: Thomas E. Peisch and Erin K. Higgins February 19, 2015

The recent hacking attacks on Sony Pictures and the Target department store chain have increased the focus on cybersecurity in all aspects of life.

At least one American law firm has had sensitive information hacked from its server and put on the Internet. Meanwhile, a couple of Canadian law firms have actually had funds converted by hackers.

An American consulting firm reported in 2012 that 80 percent of the 100 largest law firms in the United States had been the subject of at least one hacking attack during the previous year. That led to an unprecedented meeting between a high official of the FBI and the managing partners for New York City's large law firms to discuss strengthening security protocols.

On Oct. 29, 2014, the Supreme Judicial Court announced that it intends to adopt changes to the Massachusetts Rules of Professional Conduct, largely modeled on changes made to the ABA model rules. These changes are directed to lawyers' responsibilities to clients in the cybersecurity area.

While the SJC has not yet announced an effective date for these changes, the careful practitioner will review and abide by them now.

Certain of these rule changes highlight the risks for lawyers of taking a "head-in-the-sand" approach to securing their electronically stored data.

Virtually every practicing lawyer now possesses and stores confidential client information electronically, and clients expect that their lawyers will protect and preserve the integrity of their confidential information.

The rule changes will apply to all attorneys, whether practicing solo or in a large firm, and regardless of area of practice, although the application of the rules no doubt will vary depending upon particular facts and circumstances.

This column looks at the upcoming changes and their implications for Massachusetts practitioners, and then identifies practice pointers that may reduce the risks. A future column will offer suggestions for a plan of action when a hacking incident actually has taken place.

Rule 1.6 (Confidentiality of Information)

The SJC has decided to add a new provision to Rule 1.6 that is taken from ABA Model Rule 1.6.

Rule 1.6 outlines a lawyer's duty not to disclose confidential client information, except under very limited circumstances. The rule's new provision is not addressed to disclosures that are intentionally made by the lawyer, but instead requires a lawyer to guard against third parties inadvertently or intentionally gaining access to confidential client information.

Rule 1.6(c) will provide as follows:

"(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."

As can easily be seen, the new provision dramatically expands the scope of Rule 1.6. Precisely what will constitute "reasonable efforts" remains to be fleshed out, but new Comment 18 provides some guidance:

"Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use)." Rule 1.6, cmt. 18.

Thus, a lawyer who routinely handles and stores extremely sensitive client information may be expected to employ more in the way of safeguards than a lawyer whose practice largely involves documents in the public domain.

The comments to Rule 1.6 also make the following important points. First, client input is desirable. Clients who are providing their lawyers with particularly sensitive information may require their lawyers to adopt additional security measures, or may on the other hand agree to the use of less secure means of storage or communication in order to expedite matters or save costs. See Rule 1.6, cmts. 18, 19.

Second, Rule 1.6(c)'s "reasonable efforts" requirement sets a standard only with respect to a lawyer's ethical duties, and more may be required for particular types of data under pertinent state and federal law. See *id.*

Rule 1.1 (Competence)

The SJC also has announced its intent to add a new comment to Rule 1.1, the rule pertaining to attorney competence. This comment, codified in the model rules as Comment [6], will appear in a slightly modified form as Comment [8] to Rule 1.1 in the Massachusetts rules.

New Comment 8 will read as follows:

"[8] To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology*, and engage in continuing study and education." Rule 1.1, cmt. 8. (emphasis supplied).

In other words, part of a lawyer's duty to clients involves not only knowing the law, but also knowing and understanding the applicable technology and the associated risks.

The comment serves as a further reminder to lawyers that an ability to understand the basics of technology, and the ways it can be used to both preserve and gain unauthorized access to client confidences, may need to be part of the lawyer's standard toolkit.

Rule 1.15 (Safekeeping Property)

Most lawyers know that Rule 1.15 deals with a client's "trust property" and sets forth detailed record-keeping and other requirements related to it. However, many attorneys do not know that the term "trust property" as defined in the rule consists both of funds and "trust property other than funds." The latter category arguably includes confidential information given by the client to the lawyer.

With the recently announced changes to the professional conduct rules, Rule 1.15(b)(4) now will command that "[a]ll trust property shall be appropriately safeguarded." Thus, the rule also may impose an obligation on lawyers to take "reasonable steps" to protect client confidences and client funds from unauthorized access.

G.L.c. 93H

Chapter 93H, a 2007 statute, and certain regulations promulgated under it, require anyone who maintains encrypted or unencrypted electronic information regarding a Massachusetts resident to have policies and procedures in effect to protect that information. See G.L.c. 93H, §2; 201 C.M.R. 17.00 et seq.

The penalties for violating these provisions include an action by the attorney general pursuant to Chapter 93A. Although there has yet to be any significant enforcement action taken under the law or regulations, at least one commentator has taken the position that Massachusetts lawyers are specifically bound by these regulations and subject to discipline if the provisions are violated. See 51 Mass. Prac. §17.1, footnote 8.

Other guidance

The Massachusetts Bar Association's Committee on Professional Ethics also has weighed in on the "reasonableness" determination, holding that:

(a) a lawyer typically may communicate with a client via unencrypted email (Op. 00-01);

(b) a lawyer generally may provide a third-party software vendor with remote access to the lawyer's computers, so long as the attorney takes reasonable steps to preserve the confidentiality of client information, as outlined in the opinion (Op. 05-04); and

(c) a lawyer generally may use an Internet-based data storage provider to store confidential client information, so long as the lawyer undertakes reasonable efforts to ensure that the provider's data privacy policies are consistent with the lawyer's professional obligations (Op. 12-03).

In light of these requirements, what should a Massachusetts practitioner do in order to comply with his or her professional obligations with respect to preserving confidential client information stored electronically?

● Store confidential client information in an encrypted or otherwise inaccessible manner if the information ever physically leaves the firm or is transmitted to third parties outside the firm. This should apply whether the information leaves in the form of an email, a laptop, a flash drive or a mobile device.

● Entrust your electronic information-storing system only to a responsible vendor and be sure that you understand the capabilities and limits of the system. As noted, it is no longer sufficient for a lawyer not to be "competent" in this area. This does not mean that you, as a lawyer, must be as well-versed in technology as an IT professional, but you must know enough to have an informed conversation with an IT professional about whether you are meeting your professional obligations.

● Make sure that you have systems in place to at least detect, and hopefully prevent, unauthorized intrusions. While smaller law firms cannot reasonably hope to detect and prevent the most sophisticated forms of attack, virus protection software that will prevent most forms of attack should be in place.

● Be sure that your junior lawyers and non-lawyer employees are trained in the operation of your information-storing system and understand the importance of maintaining its integrity. Rules 5.1-5.3 require that lawyers take reasonable steps to insure compliance with rules by professional and non-professional staff.

● If you undertake a client matter that appears to involve the storage and/or transmission of especially sensitive client information, consider advising the client of the particulars of your data storage system so that the client can notify you of any special concerns.

● Consider obtaining insurance coverage for liabilities associated with third parties gaining unauthorized access to confidential client information on your computer system.

● If you suspect that a hacker may have obtained access to property or confidential information, the duty of candor to clients requires that you immediately notify the client and take prompt remedial action. That will be the subject of a follow-up column.

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: FEB. 23 2015 ISSUE

COVID times

July 23, 2020

Excellence in the Law 2020

July 17, 2020

The Most Important Opinions: January – June 2020

July 9, 2020