Ruminations on the Ethics of Law Firm Information Security

By Sharon D. Nelson, Esq. and John W. Simek

Lest anyone may have forgotten Rule 1.6 of the ABA Model Rules, here it is – and similar rules apply everywhere:

Rule 1.6 Confidentiality Of Information

(a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).

(b) A lawyer may reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary:

(1) to prevent reasonably certain death or substantial bodily harm;

(2) to prevent the client from committing a crime or fraud that is reasonably certain to result in substantial injury to the financial interests or property of another and in furtherance of which the client has used or is using the lawyer's services;

(3) to prevent, mitigate or rectify substantial injury to the financial interests or property of another that is reasonably certain to result or has resulted from the client's commission of a crime or fraud in furtherance of which the client has used the lawyer's services;

(4) to secure legal advice about the lawyer's compliance with these Rules;

(5) to establish a claim or defense on behalf of the lawyer in a controversy between the lawyer and the client, to establish a defense to a criminal charge or civil claim against the lawyer based upon conduct in which the client was involved, or to respond to allegations in any proceeding concerning the lawyer's representation of the client; or

(6) to comply with other law or a court order.

The trick, of course is how to keep client data secure in the digital era. It isn't easy. Computer security is expensive – and it takes time to understand it – and you will never be done learning because technology morphs constantly.

Are lawyers abiding by their ethical duty to preserve client confidences? Our opinion is that they are not. Here are a few reasons why we have that opinion:

- Security expert Rob Lee, a noted lecturer from the security firm Mandiant has reported to us that Mandiant spent approximately 10% of its time in 2010 investigating data breaches at law firms.

- Security expert Matt Kesner, who is in charge of information security at a major law firm, reports that his firm has been breached twice – and that he is aware that other law firms have suffered security breaches – and failed to report them to clients.

- Our own company, Sensei Enterprises, Inc., has never performed a security assessment at a law firm (or for that matter, at any kind of business) without finding severe vulnerabilities that needed to be addressed.

Why do otherwise competent lawyers fail so miserably in their ethical duty to maintain the confidentiality of client data? Here are some of the reasons.

- Ignorance – they simply need education.

- The "it can't happen here" mentality. This is flatly wrong – even the FBI issued an advisory in 2009 that law firms were specifically being targeted by identity thieves and by those performing business espionage – much of it originating in China and state-sponsored, though of course the Chinese government has vehemently denied involvement in such activities. Matt Kesner, mentioned above as an expert, reports that the Chinese don't bother using their "A" squad hackers to infiltrate law firms – their security is so bad that the rookie "C" squads are able to penetrate law firms.

- It's expensive. And it is. Protecting the security of client data can present a big burden for solos and small law firms. This does not take away a lawyer's ethical duty, however – and it is one reason why the authors lecture so often on computer security. Once a lawyer sees the most common vulnerabilities, he or she can take remedial steps – or engage their IT consultant to do those things that are beyond the skill of the lawyer.

- Vigilance never stops. You cannot secure your data once and think you're done – the rules of information security change on darn near a daily basis – certainly someone in the firm needs to keep up with changes on a regular basis or the firm needs to engage an security consultant to do periodic reviews – the standard

advice is that security assessments need to be done twice a year. While that is desirable, it is in our judgment mandatory that assessments be done at least annually.

In the paper world, keeping client data confidential was easy and cheap. In the digital era, abiding by this particular ethical rule is hard and expensive – but it must be done.

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, information security and computer forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com