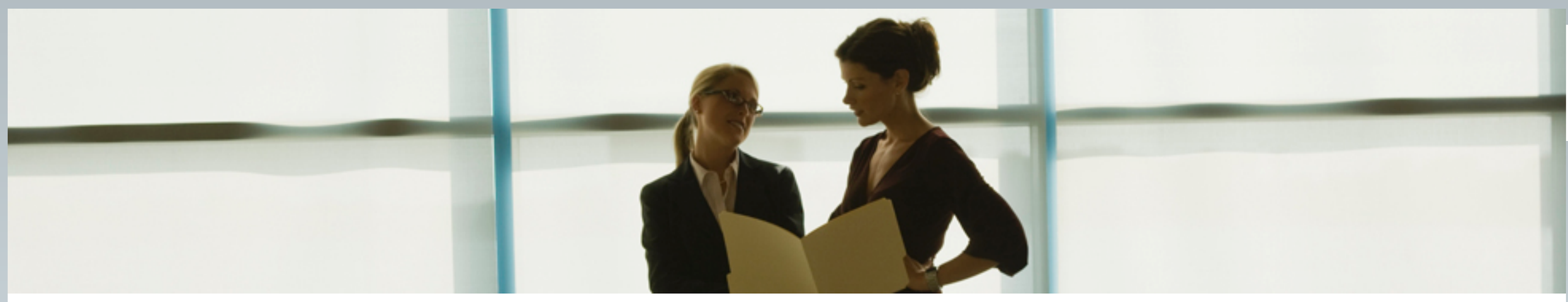

LAW|PRACTICE
THE BUSINESS OF PRACTICING LAW

AVOIDING MALPRACTICE – ARE YOU AT RISK?

Table of Contents | Features | Frontlines | Technology | Business

July/August 2010 Issue | Volume 36 Number 4 | Page 49

FEATURES

SAFEGUARDING CONFIDENTIAL DATA: Your Ethical and Legal Obligations

By David G. Ries

Taking steps to protect the confidential information in your computer systems is more than a sound business decision. As a lawyer, you have ethical and legal obligations to exercise the vigilance needed to protect client data. Are you clear on what those obligations are?

Confidential data in computer and information systems faces greater security threats today than ever before—and the dangers to lawyers and their firms are very real. In a March 20, 2010, article titled "Law Firms Are Lucrative Targets of Cyberscams," the *San Francisco Chronicle* discussed recent attacks on firms, ranging from phishing scams to intrusions into a law firm network to steal lawsuit-related information. It noted that:

> Security experts said criminals gain access into law firms' networks using highly tailored schemes to trick attorneys into downloading customized malware into their computers. It is not uncommon for them to remain

> undetected for long periods of time and come and go as they please, they said.

A March 8, 2010, *National Law Journal* article reported that one leading security firm has assisted over 50 law firms after security breaches. In witness to how sophisticated such breaches can be, a February 3, 2010, *Wired Magazine* article reported on advanced persistent threats (APTs), a particularly nasty form of coordinated hacking attack. It discussed this example of a 2008 APT attack on a law firm that was representing a client in Chinese litigation:

> The attackers were in the firm's network for a year before the firm learned from law enforcement that it had been hacked. By then, the intruders harvested thousands of e-mails and attachments from mail servers. They also had access to every other server, desktop workstation and laptop on the firm's network.

Thankfully, most law firms do not currently face sophisticated attacks like these, but there are still m any other forms of threats to the data on your systems. Moreover, they can come from many sources, including externally from hackers, cybercriminals, economic spies or dishonest adverse parties, and internally from trusted insiders, including staff members who are dishonest, disgruntled, bored or simply fooled by a clever malware program.

To help ensure that you take the right steps in response, it's critical to understand the ethical, common law and regulatory duties lawyers are under to safeguard client data. Here are key obligations to address.

Ethical Obligations

Competent representation and confidentiality are at the foundation of the attorney-client relationship. ABA Model Rule 1.1 covers the general duty of competent representation and provides that "Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation." ABA Model Rule 1.6 generally defines the duty of confidentiality—and significantly, it broadly extends that duty to "information relating to the representation of a client." It's now commonly accepted that this duty applies to client information in computer and information systems as well.

In addition, an amendment to Model Rule 1.6, part of the Ethics 2000 revisions, added new Comment 16 to the rule. This comment requires reasonable precautions to safeguard and preserve confidential information:

> A lawyer must act competently to safeguard information

> relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision.

However, while it has become clear that the obligations with respect to competence and confidentiality apply equally to electronic client data on stored computers and elsewhere, it has been unclear, until rather recently, what reasonable precautions lawyers must take to protect that data. The State Bar of Arizona has issued two well-reasoned ethics opinions that provide some specific direction on the information security requirements.

The first opinion, State Bar of Arizona Opinion No. 05-04, issued in July 2005, responds to an inquiry about the steps a law firm must take to safeguard client data from hackers and viruses. In addressing how to comply with the ethics rules as they relate to the client's electronic files or communications, it concludes that:

> … an attorney or law firm is obligated to take competent and reasonable steps to assure that the client's confidences are not disclosed to third parties through theft or inadvertence. In addition, an attorney or law firm is obligated to take reasonable and competent steps to assure that the client's electronic information is not lost or destroyed. In order to do that, an attorney must either have the competence to evaluate the nature of the potential threat to the client's electronic files and to evaluate and deploy appropriate computer hardware and software to accomplish that end, or if the attorney lacks or cannot reasonably obtain that competence, to retain an expert consultant who does have such competence.

Arizona Bar Opinion No. 09-04, issued in December 2009, deals with an online file storage and retrieval system for client access to documents. It restates the ethical requirement of competent and reasonable measures to protect client confidences, further advising that:

> It is also important that lawyers recognize their own competence limitations regarding computer security measures and take the necessary time and energy to become competent or alternatively consult available experts in the field.

The opinion discusses specific safeguards for lawyers to consider, such as secure socket layer (SSL) protocol, firewalls, password

protection, encryption and antivirus measures, but it also cautions that:

> As technology advances occur, lawyers should periodically review security measures in place to ensure that they still reasonably protect the security and confidentiality of the clients' documents and information.

Several other states' ethics opinions address requirements for safeguard ing client electronic data, including New Jersey Committee on Professional Ethics Opinion 701 (April 24, 2006), Nevada Standing Committee on Ethics and Professional Responsibility Formal Opinion 33 (February 9, 2006) and Virginia Standing Committee on Legal Ethics Opinion 1818 (September 3, 2005). While they vary in their degree of specificity, at their core they all require lawyers to take reasonable measures to protect the confidentiality of client information.

Common Law Duties

Along with the ethical duties described in the foregoing, there are also parallel common law duties defined by case law in the various states. The Restatement (3rd) of the Law Governing Lawyers (2000) summarizes this area of the law. See Section 16(2) on competence and diligence, Section 16(3) on complying with obligations concerning client's confidences, and Chapter 5, "Confidential Client Information." Breach of these duties can result in a malpractice action.

There are also instances when lawyers may have contractual duties to protect client data. This is particularly the case for clients in regulated industries, such as health care and financial services, that have regulatory requirements to protect privacy and security.

Laws and Regulations Covering Personal Information

In addition to the ethical and common law duties to protect client information, various state and federal statutes and regulations require protection of defined categories of personal information. Some of these are likely to apply to lawyers who possess any specified personal information about their employees, clients, clients' employees or customers, opposing parties and their employees, or even witnesses.

At least 10 states now have general security laws that require reasonable measures to protect defined categories of personal information (including California, Massachusetts, Maryland, New Jersey and Rhode Island). While the scope of coverage, the specificity of the requirements and the definitions vary among

these laws, personal information is usually defined to include general or specific facts about an identifiable individual. The exceptions tend to be information that is presumed public and does not have to be protected (e.g., a business address).

There are now a number of state laws that require specific safeguards for defined types of personal information as well. They generally cover Social Security numbers, driver's license numbers and financial account numbers, but some also cover health information. They include laws requiring reasonable security, breach notices and secure disposal.

The most comprehensive of this type to date is a recent Massachusetts law, M.G.L. c. 93H, which applies to "persons who own, license, store or maintain personal information about a resident of the Commonwealth of Massachusetts." Covered "personal information" includes Social Security numbers, driver's license numbers, state-issued identification card numbers, financial account numbers and credit card numbers.

The implementing regulation became effective March 1, 2010. With its broad coverage of "persons," this law may well be applied to persons nationwide, including attorneys and law firms, when they have sufficient contacts with Massachusetts to satisfy personal jurisdiction requirements.

It requires covered persons to "develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards." In addition to requiring a risk assessment, the regulation contains detailed requirements for the information security program and detailed computer system security requirements. The security requirements include:

> Encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly; and
>
> Encryption of all personal information stored on laptops or other portable devices.

Additional system security requirements are secure user authentication, secure access control, reasonable monitoring to detect unauthorized access, reasonably up-to-date firewall protection, reasonably up-to-date security software (including current patches and virus definitions), and education and training of employees.

Lawyers and their firms should think about and understand the

consequences of the Massachusetts law, as some observers believe that it will become a model for comprehensive protection of personal information.

Nevada also has laws that require "reasonable security measures" and encryption (NRS 603A.210 and NRS 597.970), although they are much less detailed than the Massachusetts law. Note, too, that encryption is already required for federal agencies that have information about individuals on laptops and portable media. As encryption becomes a security standard, it is likely to become the standard of what is reasonable for lawyers.

The obligations don't stop, however, at protecting the confidentiality of information. Forty-six states (all but Kentucky, Mississippi, New Mexico and South Dakota), the District of Columbia and the Virgin Islands have laws that require notification concerning data breaches. While there are differences in their scope and requirements, they generally require entities that own, license or possess defined categories of personally identifiable information about consumers to notify affected consumers if there is a breach. Like the reasonable security laws, many of these laws apply to covered information "about" residents of the state. Some require notice to a state agency in addition to notice to consumers.

In addition, in December 2009, the U.S. House of Representatives passed H.R. 2221, which provides for comprehensive protection of defined personal information, including breach notification. If passed by the Senate, it will establish a uniform federal standard.

To add to the web of issues involved, at least 19 states also now have laws that require secure disposal of paper and electronic records that contain defined personal information. The Federal Trade Commission's Disposal Rule, 16 C.F.R. Part 682, has similar requirements for consumer credit reports and information derived from them.

Also on the federal level, an attorney who receives protected individually identifiable health information (PHI) from a covered entity under the Health Insurance Portability & Accountability Act (HIPAA) will generally be a "business associate" and be required to comply with the HIPAA security requirements. The 2009 HIGHTECH Act enhanced HIPAA security requirements, extended them directly to business associates, and added a new breach notification requirement.

Standards for Competent and Reasonable Measures

The core challenge for lawyers in establishing information security programs is deciding what security measures are necessary and

then implementing them. Determining what "competent and reasonable measures" are can be difficult. Legal standards that apply in other areas, like financial services, can be helpful in providing a framework, even though they do not legally apply to the practice of law.

The FTC's Safeguards Rule under the Gramm-Leach-Bliley Act provides a helpful framework that lawyers can use to comply with their obligations to safeguard client data. The requirements in the rule, *Standards for Safeguarding Customer Information*, 16 C.F.R., Part 314, are general and cover less than two pages in the Federal Register. They provide a short yet comprehensive list of the components of a complete security program.

For larger firms, standards published by the International Organization for Standardization (ISO), at www.iso.org, provide a good framework. They include ISO/IEC 17799:2005, *Information Technology—Code of Practice for Information Security Management* and ISO/IEC 27001:2005, *Information Technology—Security Techniques—Information Security Management System—Requirements*.

The Evolution of "Reasonable"

The wealth of confidential data maintained in lawyers' computers and information systems today faces substantial and very real security risks. Therefore, as discussed here, it's critical for all lawyers to understand and address these risks to ensure they comply with their ethical, common law and regulatory obligations to safeguard client data. Taking "reasonable measures" is a good start. At the same time, remember that what is seen to be reasonable is evolving, which means that lawyers must also work to stay familiar with any changing obligations placed on them by state or federal law, so they can ensure they comply with the same.

About the Author

David G. Ries is a partner in the Pittsburgh, PA, office of Thorp Reed & Armstrong, LLP, where he practices in the areas of environmental, commercial and technology litigation. He regularly speaks and writes on technology law and ethics issues, including information security, and he is a member of the ABA Law Practice Management Section Council.