Cybersecurity for Attorneys: Addressing the Legal and Ethical Duties

BY DAVID G. RIES
NOVEMBER 14, 2019

As attorneys continue to embrace the latest technology, it is critical for them to understand and address the legal and ethical obligations that go with it.

Threats to data in computers, mobile devices, and information systems used by attorneys are at an all-time high. They take a variety of forms, ranging from e-mail phishing scams and social engineering attacks to sophisticated technical exploits resulting in long term intrusions into law firm networks. They also include lost or stolen laptops, tablets, smartphones, and USB drives, as well as inside threats—malicious, untrained, inattentive, and even bored personnel.

These threats are a particular concern to attorneys because of their duties of competence in technology and confidentiality. Attorneys have ethical and common law duties to take competent and reasonable measures to safeguard information relating to clients. They also often have contractual and regulatory duties to protect client information and other types of confidential information.

Breaches have become so prevalent that a common saying in cybersecurity today is: "there are two kinds of companies: those that have been breached and know it and those that have been breached and don't know it." This is true for attorneys and law firms as well as other businesses and enterprises.

ABA Formal Opinion 477R (May 2017) describes the same threat environment: "Cybersecurity recognizes a … world where law enforcement discusses hacking and data loss in terms of 'when,' and not 'if…'"

Security threats to lawyers and law firms continue to be substantial, real and growing. Attorneys and law firms must recognize these threats and address them through comprehensive cybersecurity programs.

Duty to Safeguard

Attorneys have ethical and common law duties to take competent and reasonable measures to safeguard information relating to clients and also often have contractual and regulatory duties to protect confidential information.

Ethics Rules.

Several of the ABA Model Rules have particular application to the protection of client information, including competence (Model Rule 1.1), communication (Model Rule 1.4), the confidentiality of information (Model Rule 1.6), safeguarding property (Model Rule 1.15), and supervision (Model Rules 5.1, 5.2 and 5.3).

Model Rule 1.1: Competence covers the general duty of competence. It provides that "A lawyer shall provide competent representation to a client." This "requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation." It also includes

competence in selecting and using technology, including cybersecurity. It requires attorneys who lack the necessary technical competence for security to learn it or to consult with qualified people who have the requisite expertise.

The 2012 amendments to the Model Rules, based on the recommendations of the ABA Commission on Ethics 20/20, include the addition of the following underlined language to the Comment to Model Rule 1.1:

> [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…

As of September 2019, 37 states have adopted this addition to the comment to Model Rule 1.1, some with variations from the ABA language.

Model Rule 1.4: Communications also applies to attorneys' use of technology. It requires appropriate communications with clients "about how the client's objectives are to be accomplished," including the use of technology. It requires keeping the client informed and, depending on the circumstances, may require obtaining "informed consent." It requires notice to a client of a compromise of confidential information relating to the client.

Model Rule 1.6: This rule generally defines the duty of confidentiality. It begins as follows:

> 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)…

Rule 1.6 broadly requires protection of "information relating to the representation of a client;" it is not limited to confidential communications and privileged information. Disclosure of covered information generally requires express or implied client consent (in the absence of special circumstances like misconduct by the client).

The 2012 amendments added the following new subsection (underlined) to Model Rule 1.6:

> (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.

This requirement covers two areas—inadvertent disclosure and unauthorized access. Inadvertent disclosure includes threats like leaving a briefcase, laptop or smartphone in a taxi or restaurant, sending a confidential e-mail to the wrong recipient, producing privileged documents or data in litigation, or exposing confidential metadata. Unauthorized access includes threats like hackers, criminals, malware and insider threats.

The 2012 amendments also include additions to Comment [18] to Rule 1.6, providing that "reasonable efforts" require a risk-based analysis, considering 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 them, and the extent to which they would

adversely affect the lawyer's ability to use the technology. The amendment also provides that a client may require the lawyer to implement special security measures not required by the rule or may give informed consent to forego security measures that would otherwise be required by the rule.

Significantly, the Ethics 20/20 Commission noted that these revisions to Model Rules 1.1 and 1.6 make explicit what was already required rather than adding new requirements.

Model Rule 1.15: Safeguarding Property requires attorneys to segregate and protect money and property of clients and third parties that is held by attorneys. Some ethics opinions and articles have applied it to electronic data held by attorneys.

Model Rule 5.1: Responsibilities of Partners, Managers, and Supervisory Lawyers and Model Rule 5.2: Responsibilities of a Subordinate Lawyer include the duties of competence and confidentiality. Model Rule 5.3: Responsibilities Regarding Nonlawyer Assistants was amended in 2012 to expand its scope. "Assistants" was expanded to "Assistance," extending its coverage to all levels of staff and outsourced services ranging from copying services to outsourced legal services. This requires attorneys to employ reasonable safeguards, like due diligence, contractual requirements, supervision and monitoring, to ensure that nonlawyers, both inside and outside a law firm, provide services in compliance with an attorney's ethical duties, including confidentiality.

Ethics Opinions.

A number of state ethics opinions, for over a decade, have addressed professional responsibility issues related to security in attorneys' use of various technologies. Consistent with the Ethics 20/20 amendments, they generally require competent and reasonable safeguards.

A recent opinion on safeguarding client data is ABA Formal Opinion 477R, "Securing Communication of Protected Client Information" (May 2017). While focusing on electronic communications, it also explores the general duties to safeguard information relating to clients in light of current threats and the Ethics 20/20 technology amendments to the Model Rules. Its conclusion includes:

> Rule 1.1 requires a lawyer to provide competent representation to a client. Comment [8] to Rule 1.1 advises lawyers that to maintain the requisite knowledge and skill for competent representation, a lawyer should keep abreast of the benefits and risks associated with relevant technology. Rule 1.6(c) requires a lawyer to make "reasonable efforts" to prevent the inadvertent or unauthorized disclosure of or access to information relating to the representation.

Most recently, the ABA issued Formal Opinion 483, "Lawyers' Obligations After an Electronic Data Breach or Cyberattack" (October 17, 2018). The opinion reviews lawyers' duties of competence, confidentiality, and supervision in safeguarding confidential data and in responding to data breaches. It discusses the obligations of monitoring for a data breach, stopping a breach, restoring systems, and determining what occurred. It finds that Model Rule

1.15: Safeguarding Property applies to electronic client files as well as paper files and requires the care required of a professional fiduciary.

The opinion concludes:

> Even lawyers who, (i) under Model Rule 1.6(c), make "reasonable efforts to prevent the unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client," (ii) under Model Rule 1.1, stay abreast of changes in technology, and (iii) under Model Rules 5.1 and 5.3, properly supervise other lawyers and third-party electronic-information storage vendors, may suffer a data breach. When they do, they have a duty to notify clients of the data breach under Model Rule 1.4 in sufficient detail to keep clients "reasonably informed" and with an explanation "to the extent necessary to permit the client to make informed decisions regarding the representation."

The key professional responsibility requirements from these various opinions on attorneys' use of technology are competent and reasonable measures to safeguard client data, including an understanding of limitations in attorneys' knowledge, obtaining appropriate assistance, continuing security awareness, appropriate supervision, and ongoing review as technology, threats, and available safeguards evolve. They also require obtaining clients' informed consent, in some circumstances, and notifying clients of a breach or compromise. It is important for attorneys to consult the rules, comments, and ethics opinions in the relevant jurisdiction(s).

Ethics Rules – Electronic Communications.

E-mail and electronic communications have become everyday communications forms for attorneys and other professionals. They are fast, convenient and inexpensive, but also present serious risks to confidentiality. It is important for attorneys to understand and address these risks.

The Ethics 2000 revisions to the Model Rules, over 15 years ago, added Comment [17] (now 19]) to Model Rule 1.6. For electronic communications, it requires "reasonable precautions to prevent the information from coming into the hands of unintended recipients." It provides:

> …This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement…

This comment requires attorneys to take "reasonable precautions" to protect the confidentiality of electronic communications. Its language about "special security measures" has often been viewed by attorneys as meaning that they never need to use special measures, like encryption. While it does state that "special security measures" are not generally required, it contains qualifications and notes that "special circumstances" may warrant "special

precautions." It includes the important qualification – "if the method of communication affords a reasonable expectation of privacy."

Whether unencrypted e-mail affords a reasonable expectation of privacy is questionable. Respected security professionals for years have compared the security of unencrypted e-mail to postcards or postcards written in pencil. A June 2014 post by Google on the *Google Official Blog* and a July 2014 *New York Times* article use the same analogy—comparing the security of unencrypted e-mails to postcards and comparing encryption to envelopes.

Comment [19] to Rule 1.6 also lists "the extent to which the privacy of the communication is protected by law" as a factor to be considered. The federal Electronic Communications Privacy Act and similar state laws make unauthorized interception of electronic communications a crime. Some observers say that this should be determinative and attorneys should not be required to use encryption. The better view is to treat legal protection as only one of the factors to be considered.

Ethics Opinions – Electronic Communications.

An ABA ethics opinion in 1999 and several state ethics opinions concluded that special security measures, like encryption, are not generally required for confidential attorney e-mail. However, these opinions, like Comment [19], contain qualifications that limit their general conclusions.

In May 2017, the ABA Standing Committee on Ethics and Professional Responsibility issued Formal Opinion 477R, "Securing Communication of Protected Client Information." The opinion revisits attorneys' duty to use encryption and other safeguards to protect e-mail and electronic communications in light of evolving threats, developing technology, and available safeguards. It suggests a fact-based analysis and finds that "the use of unencrypted routine email generally remains an acceptable method of lawyer-client communication," but "particularly strong protective measures, like encryption, are warranted in some circumstances." It concludes that "…a lawyer may be required to take special security precautions to protect against the inadvertent or unauthorized disclosure of client information when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security."

The opinion provides general guidance and leaves details of the application to attorneys and law firms, based on analyzing the facts of each case.

In addition to complying with any applicable ethics and legal requirements, the most prudent approach to the ethical duty of protecting electronic communications is to have an express understanding with clients (preferably in an engagement letter or other writing) about the nature of communications that will be (and will not be) sent electronically, and whether or not encryption and other security measures will be utilized. It has now reached the point where all attorneys should have encryption available for use in appropriate circumstances.

Common-Law and Contractual Duties.

Along with the ethical duties, lawyers have 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, including 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.

Lawyers increasingly also have contractual duties to protect client data, particularly for clients in regulated industries, such as health care and financial services, with specific regulatory requirements to protect privacy and security.

Regulatory Duties.

Attorneys and law firms that have specified personal information about their employees, clients, clients' employees or customers, opposing parties and their employees, or even witnesses may also be covered by federal and state laws that variously require reasonable safeguards for covered information and notice in the event of a data breach.

Complying with the Duties

Understanding all of the applicable duties is the first step, before moving to the challenges of compliance by designing, implementing and maintaining an appropriate risk-based cybersecurity program.

Cybersecurity is a process to protect the confidentiality, integrity, and availability of information. An important concept is that security requires training and ongoing attention. It must go beyond a one-time "set it and forget it" approach. A critical component of a law firm security program is constant vigilance and security awareness by all users of technology.

The first step for a security program is assigning responsibility for security. This includes defining who is in charge of security and defining everyone's role, including management, attorneys and support personnel.

Security starts with an inventory of information assets to determine what needs to be protected and then a risk assessment to identify anticipated threats to the information assets. The next step is the development, implementation, and maintenance of a comprehensive cybersecurity program to employ reasonable physical, administrative and technical safeguards to protect against identified risks. This is generally the most difficult part of the process. It must address people, policies and procedures, and technology, and include policies and procedures, controls, training, ongoing security awareness, monitoring for compliance, and periodic review and updating. Cyber insurance should also be considered as part of the program.

A cybersecurity program should cover the core security functions: identify, protect, detect, respond, and recover.

The requirement for lawyers is reasonable security, not absolute security. Recognizing this concept, the Ethics 20/20 amendments to Comment [18]to Model Rule 1.6 include "…[t]he unauthorized access to, or the inadvertent or unauthorized disclosure of, confidential information does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure." The comment calls for a risk-based analysis, considering the sensitivity of the information, the likelihood of disclosure if additional

safeguards are not employed and consideration of available safeguards. The analysis includes the cost of employing additional safeguards, the difficulty of implementing them, and the extent to which they would adversely affect the lawyer's ability to use the technology. This risk-based approach is now standard in cybersecurity.

A comprehensive security program should be based on a standard or framework, like those published by the National Institute for Standards and Technology (NIST) and the International Organization for Standardization's (ISO). For small and mid-size firms, information is available on the Federal Trade Commission website, Cybersecurity for Small Business, and NIST's Small Business Cybersecurity Corner website.

Attorneys and law firms will often need assistance with cybersecurity programs because they do not have the requisite knowledge and experience. For those who need assistance, it is important to find an IT consultant with knowledge and experience in security, or a qualified security consultant.

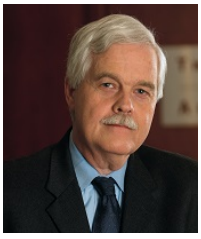
Conclusion

The ethical and common law duties discussed in this article provide minimum standards that attorneys must meet. Attorneys should aim for even stronger safeguards as a matter of sound professional practice and client service. The safeguards should be included in a risk-based, comprehensive security program.

Additional Information

- American Bar Association, Law Practice Division, including the Legal Technology Resource Center
- American Bar Association, Cybersecurity Legal Task Force
- Sharon D. Nelson, David G. Ries, and John W. Simek, *Encryption Made Simple for Lawyers* (ABA 2015)
- Sharon D. Nelson, David G. Ries, and John W. Simek, *Locked Down: Practical Information Security for Lawyers, Second Edition* (ABA 2016)
- Jill D. Rhodes and Robert S. Litt, *The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals, Second Edition* (ABA 2017)

About the Author



David G. Ries *is of counsel in the Pittsburgh, PA office of Clark Hill PLC, where he practices in the areas of environmental, technology, and data protection law and litigation. He is a coauthor of Encryption Made Simple for Lawyers (ABA 2015) and Locked Down: Practical Information Security for Lawyers, Second Ed. (ABA 2016).*