American Bar Association Section of Labor & Employment Law

Ethics and Cybersecurity: Obligations to Protect Client Data

Drew Simshaw
Policy Analyst
Center for Law, Ethics, and Applied Research in Health Information
Indiana University

Stephen S. Wu
Of Counsel
Silicon Valley Law Group

National Symposium on Technology in Labor and Employment Law
San Francisco, CA
March 15-17, 2015

Abstract

Sweeping advances in technology are not only changing the law that attorneys practice, they are also bringing profound changes to the way attorneys practice law. For instance, the combination of consumer-friendly mobile devices and cloud computing means that attorneys now have the technology to obtain access to all their work data with any device, at any time, as long as they have an Internet connection. Nonetheless, new technologies create new threats to the confidentiality of client data. Ethics rules, both from the ABA and in California, impose duties on attorneys to protect client confidences. They also require attorneys to practice competently and to supervise office staff and third parties with access to client data. The operation of these rules will require attorneys and law firms to implement reasonable information security practices to protect the confidentiality, integrity, and availability of client data. The failure to protect client data may lead to attorney discipline or malpractice liability. Information security is not just a "technology issue" that can be delegated without supervision to information technology support staff. Attorneys themselves have an obligation to manage and oversee the security function in their firms. Lessons learned from other industries and industry standard security frameworks can help law firms implement effective security programs.

I. Introduction[1]

With advancing computing technology, we live in an era of unprecedented computing power and connectivity. Modern computing devices have as much power as mainframe computers running entire government agencies in the 1960s. Internet-connected desktop and laptop computers are standard equipment for modern knowledge workers. Workers frequently telecommute by using their home computers.

Moreover, we are in the midst of a "mobile revolution." Walking around our cities and towns, it seems that everyone has a smart phone in hand. In the office, at home, and in the airports, tablet computers appear everywhere. In addition to offering us voice, email, and text communications on the go, our mobile devices are giving us access to the world's information via the Mobile Internet more or less anytime and anywhere. When a law firm's systems are connected to the Internet, technology enables today's lawyer to obtain access to client information at any time from any device from any place with Internet or cellular connectivity.

With these advances in technology, information security threats have increased. Data breaches continue to be an everyday occurrence. We see them in the news all the time. Competitors, former employees, and state-sponsored groups seek companies' trade secrets in order to bolster competing businesses. Hacktivist groups seek to damage the reputation of companies by publicizing sensitive information. Organized crime rings seek sensitive information for profit.

Law firms are not immune from attacks.[2] For instance, in 2011, a Chinese hacker group gained unauthorized access to the systems and data of Wiley Rein LLP in Washington D.C. Wiley had pursued unfair trade claims against exporters in China and, in just one case, obtained tariffs on more than $3 billion in exports on solar cells. The Chinese hacking group not only penetrated the firm's networks, it stole large amounts of data

---

[1] An earlier version of this article will be published by Mr. Simshaw. Drew T. Simshaw, *Legal Ethics and Data Security: Our Individual and Collective Obligation to Protect Client Data*, 30 AM. J. TRIAL ADVOC. (forthcoming 2015).

[2] American Bar Association, *Law firms not immune to cybersecurity risks*, YOURABA, Oct. 2013 (available at http://www.americanbar.org/newsletter/publications/youraba/201310article01.html) (interview with Jill Rhodes and Vincent Polley, who edited the ABA Cybersecurity Handbook) [hereinafter "Interview with Rhodes and Polley"].

from various entities, including the president of the European Union Council, Haliburton Co., and a Canadian magistrate.[3]

One FBI agent put it succinctly: "Computer attacks on law firms happen every day . . . ."[4] Many of these attacks fail, but some succeed. The bottom line is, "Many large law firms have been hacked; the FBI has warned that law firms are being targeted."[5] We, as attorneys, are on notice of the threat.

The ABA, recognizing these threats, adopted a House of Delegates resolution calling for "all private and public sector organizations to develop, implement, and maintain an appropriate security program."[6] The report accompanying the resolution made it clear that the resolution covers law firms and legal services organizations.[7] This resolution followed an earlier 2012 House of Delegates resolution proposed by the Commission on Ethics 20/20, approving changes to the ABA Model Rules of Professional Conduct. The resolution amended the Model Rules to impose a duty on lawyers to use reasonable efforts to prevent unauthorized access to client data and made related changes to address the advances of technology.[8] The ABA has also published a Cybersecurity Handbook to help lawyers and law firms improve their information security programs.[9]

---

[3] Bloomberg News, *Hackers Linked to China's Army Seen From EU to D.C.*, BLOOMBERG BUSINESS, Jul. 26, 2012 (available at http://www.bloomberg.com/news/articles/2012-07-26/china-hackers-hit-eu-point-man-and-d-c-with-byzantine-candor).

[4] Andrew Conte, *Unprepared Law Firms Vulnerable to Hackers*, TRIBLIVE, Sept. 13, 2014 (available at http://triblive.com/news/allegheny/6721544-74/law-firms-information#axzz3TuTnls4O).

[5] Interview with Rhodes and Polley, *supra*.

[6] Resolution 109, American Bar Association, Cybersecurity Legal Task Force, Section of Science & Technology Law, Resolution and Report to the House of Delegates, August 2013, Resolution at 1 (available at http://www.americanbar.org/content/dam/aba/administrative/house_of_delegates/resolutions/2014_hod_annual_meeting_109.authcheckdam.pdf) [hereinafter "ABA Cybersecurity Resolution"].

[7] *Id.*, Report at 1 & n.1.

[8] Resolution 105A, American Bar Association, Commission on Ethics 20/20, et al., Resolution and Report to the House of Delegates, August 2012, at 4 (available at http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/2012_hod_annual_meeting_105a_filed_may_2012.authcheckdam.pdf).

[9] Jill D. Rhodes & Vincent I Polley, *The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals*, ABA Cybersecurity Legal Taskforce (2013) [hereinafter "ABA Cybersecurity Handbook"].

II. Information Security Risks to Law Firms

Law firms are recognized targets for attack for a number of reasons. First, law firms have large amounts of information that would be valuable to state or non-state actor attackers. "They collect and store large amounts of critical, highly valuable corporate records, including intellectual property, strategic business data, and litigation-related theories and records collected through e-discovery."[10] For instance, attackers might want to steal trade secrets about a firm client in order to gain an advantage in the marketplace. Moreover, attackers may be interested in the identity of potential acquisition targets in order to profit by the information via stock trades.[11] Also, some firms hold personal information about individuals, whether clients or opponents, that could be used for identity theft purposes, such as names, birthdates, and social security numbers.

Second, law firms are perceived as easy targets for attacks. Attackers seeking information about a particular company may find it easier to find out the identity of the law firms representing it and trying to attack the law firms' systems than attacking the company's systems directly. Law firms are "perceived to have fewer security resources than their clients, with less understanding of and appreciation for cyber risk."[12] Finally, a hack against a law firm may be more efficient and save time, compared to an attack against a firm client. "[L]lawyers are usually involved in only their client's most important business matters, meaning hackers may not need to sift through extraneous data to find the more valuable information."[13]

---

[10] ABA Cybersecurity Resolution, *supra*, Report at 4.

[11] *See* Alan Levin & Michael Riley, *Hackers With Wall Street Savvy Stealing M&A Data: FireEye*, BLOOMBERG BUSINESS, Dec. 1, 2014 (available at http://www.bloomberg.com/news/articles/2014-12-01/hackers-with-wall-street-savvy-stealing-m-a-data-fireeye). "A group dubbed FIN4 by researchers at FireEye Inc. has been tricking executives, lawyers and consultants into providing access to confidential data and communications, and probably using the information for insider trading . . . ." *Id.*

[12] Jane LeClair & Gregory Keeley, *Cybersecurity in Our Digital Lives*, A Volume in the Excelsior College Press Series Protecting Our Future, Hudson Whitman Excelsior College Press 128 (2015) [hereinafter "Cybersecurity in Our Digital Lives"]; *see also* ABA Cybersecurity Handbook, *supra*, at 105 ("Law firms are viewed as a 'very target-rich environment' with significantly less cybersecurity protection in place than their clients have" (citing John Reed, *The New Cyber Vulnerability: Your Law Firm*, Foreign Policy—Killer Apps Blog, (Nov. 07, 2012) (available at http://foreignpolicy.com/2012/11/07/the-new-cyber-vulnerability-your-law-firm/)).

[13] Cybersecurity in Our Digital Lives, *supra*, at 128; *see also* ABA Cybersecurity Handbook, *supra*, at 127 ("[A]ttacks on law firms are likely to provide the hacker with

Threats to law firms may arise from a number of sources. For instance, some law firms may fall victim to malicious insiders. Malicious insiders may be motivated by job dissatisfaction or may seek to compromise client data for financial gain. For instance, in 2001, a paralegal at a large firm in New York downloaded a copy of a trial plan from his firm's computer system and tried to sell the plan to opposing counsel for $2 million. Fortunately for the firm, the scheme was exposed and the paralegal made the sale to an undercover FBI agent. He eventually pleaded guilty to Computer Fraud and Abuse Act violations, wire fraud, and related charges.[14] Some insiders may also have political or social activism motives.

State-sponsored attacks are another source of information security threats. State actors may be motivated by economic espionage, terrorism, or politics.[15] Foreign or domestic criminal enterprises may seek information to sell or use in order to make money. Non-state "hacktivists" may hope to achieve a political objective through attacks. Terrorists may make hacking attacks both for profit and directly to terrorize their victims. Finally, business competitors sometimes seek information about other companies in their markets using extra-legal techniques.

Given these increasing threats, our clients are now asking law firms about their security programs and are seeking written assurances of security as a condition of giving business to their outside counsel. For instance, "Wall Street banks are pressing outside law firms to demonstrate that their computer systems are employing top-tier technologies to detect and deter attacks from hackers bent on getting their hands on corporate secrets either for their own use or sale to others . . . ."[16]

A law firm's failure to protect client data may cause considerable damage. "Clients and third parties may find themselves victims of fraud, identity theft, and bankruptcy, not to mention negative publicity and tarnished business reputation."[17] Following a breach, a law firm's clients or third parties could incur liability in civil actions, administrative

---

more sensitive information per breach of a computer server or hard drive than an attack on the firm's client.").

[14] Office of the United States Attorney, Southern District of New York, *Manhattan Paralegal Sentenced for Theft of Litigation Trial Plan* (Jan. 20, 2002) (available at http://www.justice.gov/criminal/cybercrime/press-releases/2002/farrajSentence.htm).

[15] Cybersecurity in Our Digital Lives, *supra*, at 129.

[16] Matthew Goldstein, *Law Firms Are Pressed on Security for Data*, New York Times, March 26, 2014 (available at http://dealbook.nytimes.com/2014/03/26/law-firms-scrutinized-as-hacking-increases/?_r=0).

[17] Cybersecurity in Our Digital Lives, *supra*, at 129.

proceedings, or even criminal charges.[18] Attorneys or law firms that fail to protect data may face discipline from their state bars, government investigations, fines, private law suits, and malpractice claims by clients. Most importantly, a data breach may cause considerable harm to the reputation of a hacked law firm and its lawyers. Clients, judges, the legal community, and members of the public may lose trust in the firm.[19] If sufficiently serious, a data breach could be a threat to the very survival of a law firm.

III. Attorneys' Ethical Obligations to Protect Client Data

Lawyers and law firms have ethical obligations under the rules of professional conduct in their jurisdictions. The ABA published and regularly updates the ABA Model Rules of Professional Conduct.[20] States have their individual ethical rules, although most are based on the ABA's Model Rules. As mentioned above, the ABA Commission on Ethics 20/20 proposed changes to the Model Rules based on their evolving views about the impact of technology on the practice of law. The House of Delegates passed a resolution approving these changes.[21]

State ethics opinions provide an additional source of guidance for understanding attorneys' ethical obligations under their rules. In addition, secondary sources of information are available for guidance. In 2006, the ABA Section of Science & Technology Law published a book on law office security.[22] In 2013, moreover, the ABA published *The ABA Cybersecurity Handbook,* discussed above.[23]

---

[18] *Id*.
[19] *Id*.
[20] *See, generally* ABA Model Rules of Professional Conduct (available at http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/model_rules_of_professional_conduct_table_of_contents.html).
[21] *See, generally*, American Bar Association, ABA Commission on Ethics 20/20, http://www.americanbar.org/groups/professional_responsibility/aba_commission_on_ethics_20_20.html. "The ABA Commission on Ethics 20/20 was formed to consider changes to the Model Rules of Professional Conduct with an eye in part on the intersection of lawyers' conduct and advances in technology." John M. Barkett, Ethics 2015: Don't Get Tangled in the Web, Shook, Hardy & Bacon L.L.P., Miami, Florida (2014), at 2, available at http://www.americanbar.org/content/dam/aba/administrative/litigation/materials/2015-winter-leadership/010515_ethics_2015__don_t_get_tangled_in_the_web.authcheckdam.pdf.
[22] Sharon Nelson, et al., *Information Security for Lawyers and Law Firms* (2006).
[23] *See generally* ABA Cybersecurity Handbook, *supra*.

The following sections discuss the core duties under the ethics rules bearing on information security: the duty of confidentiality, the duty of competence, and the duty to supervise. This conference's location is in San Francisco. Given the likely audience of mostly California attorneys, we cover both the ABA Model Rules and the California Rules of Professional Conduct.

A. The Duty of Confidentiality

The most important ethical rule relating to lawyer and law firm information security is the duty to protect the confidentiality of client confidences. In general, under state ethical rules "[a] lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent."[24] *The ABA Cybersecurity Handbook* explains that "[t]his obligation to maintain confidentiality of all information concerning a client's representation, no matter the source, is paramount," and "is no less applicable to electronically stored information than to information contained in paper documents or not reduced to any written or stored form."[25] Confidentiality is a "core" obligation of a lawyer in the conduct of the lawyer's practice.[26]

Indeed, in California, the duty of confidentiality is phrased in the strongest terms. This duty appears in a statute imposing a duty on each lawyer "[t]o maintain inviolate the confidence, and *at every peril to himself or herself* to preserve the secrets, of his or her client."[27] The California Rule of Professional Conduct establishing the duty of confidentiality refers to this statute. "A member shall not reveal information protected from disclosure by Business and Professions Code section 6068, subdivision (e)(1) without the informed consent of the client" except to prevent a criminal act resulting in death or substantial bodily harm.[28]

Following the ABA resolution in the wake of the work of the ABA Commission on Ethics 20/20, ABA Model Rule 1.6 Part (c) now says that "[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."[29] In addition, and perhaps most

---

[24] ABA Model Rule 1.6(a).
[25] ABA Cybersecurity Handbook, *supra*, at 62.
[26] *See* David G. Reis, Cyber Security for Attorneys: Understanding the Ethical Obligations, LAW PRACTICE TODAY, March 2012, at 1 (available at http://www.americanbar.org/content/dam/aba/publications/law_practice_today/cyber-security-for-attorneys-understanding-the-ethical-obligations.authcheckdam.pdf).
[27] CAL. BUS. & PROF. CODE § 6068(e)(1) (emphasis added).
[28] Cal. R. Prof. Conduct. 3-100(A).
[29] ABA Model Rule 1.6(c) (as amended).

significantly, Comment [18] now elaborates that "[f]actors to be considered in determining the reasonableness of the lawyer's efforts" include "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)."[30]

The Ethics 20/20 Commission's work was intended to address a lawyer's obligations in the face of changing technologies. Although not specifically calling out the concept of information security, the Commission's language is similar to the language in information security legislation. The requirement to protect client information is, in essence, an information security obligation. Commentators have noted the significance of this change, and the new affirmative duty of care for securing client information.[31]

The rules do not specify requirements for the exact security measures necessary in any given situation, such as an attorney-client communication. Indeed, the Rules contemplate that the lawyer and client will discuss and then make a decision about what security is necessary. "A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule."[32]

Model Rule 1.4 also requires attorney-client communications, specifically "about the means by which the client's objectives are to be accomplished."[33] Similarly, the California Rules state that "A member shall keep a client reasonably informed about significant developments relating to the employment or representation . . . ."[34] By implication, these rules require communication about the law firm's technology for

---

[30] ABA Model Rule 1.6 comm. [18] (as amended).
[31] *See, e.g.*, Will Harrelson, *Mobile Device Security for Lawyers: How Solos and Small Firms Can Ethically Allow Bring Your Own Device*, Curo Legal, June 24, 2014, http://www.curolegal.com/mobile-device-security-lawyers-solos-small-firms-can-ethically-allow-bring-your-own-device/ ("This is a monumental change that sets a new standard suggesting that lawyers are required to implement reasonable technological safeguards to prevent even an 'inadvertent' disclosure of a client's information or data.").
[32] ABA Model Rule 1.6 comm. [19] (as amended).
[33] ABA Model Rule 1.4.
[34] Cal. R. Prof. Conduct 3-500.

communicating with clients.[35] Likewise, these rules arguably require a notification in the event of a data breach involving client information.[36]

B. The Duty of Competence

In order to maintain client confidences, lawyers must be competent and have kept abreast of changes in information technology they are using in their practices. They cannot protect client confidences unless they know of the nature of the technology they are using, the threats to that technology, and the use of safeguards to mitigate risks. The California Rules state that "A member shall not intentionally, recklessly, or repeatedly fail to perform legal services with competence."[37]

"Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."[38] "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* . . . ."[39] Competence includes the knowledge of substantive law and specific skills, such as advocacy, writing, and negotiation, but it also includes competence in using the technologies commonly used for law practice.

A lawyer does not need to personally have all the needed technology competencies. The lawyer can, and indeed must, turn to the expertise of staff or outside experts when needed.[40] According to *The ABA Cybersecurity Handbook*, "[i]f a lawyer is not competent to decide whether use of a particular technology (e.g., cloud storage, public Wi-Fi) allows reasonable measures to protect client confidentiality, the ethics rules require that the lawyer must get help, even if that means hiring an expert information technology consultant to advise the lawyer."[41]

---

[35] Reis, *supra*, at 2.
[36] *Id*.
[37] Cal. R. Prof. Conduct 3-110(A).
[38] ABA Model Rule 1.1.
[39] ABA Model Rule 1.1 comm. [8] (as amended) (emphasis added).
[40] Reis, *supra*, at 2 ("[Model Rule 1.1] requires attorneys who lack the necessary technical competence for security (many, if not most attorneys) to consult with qualified people who have the requisite expertise."); ABA Cybersecurity Handbook, *supra*, at 66 ("Getting expert help is a recurring theme (as well as good advice) in ethics opinions on this subject."). *See also* Cal. R. Prof. Conduct 3-110(C) (associating with other attorneys or learning needed skills to satisfy competence requirement).
[41] ABA Cybersecurity Handbook, *supra*, at 66.

Nonetheless, a duty of competence means that the lawyer cannot simply turn over all aspects of the security function to others. All workers at the firm have control over certain aspects of their client work and must be secure in that work. For instance, attorneys have control over what they talk about in public places. They have a duty not to discuss confidential client matters in public places. This is a concern of the attorney, and not just the staff.

Similarly, attorneys must protect paper records. They should not read sensitive paper documents in places where others can view them, such as on the plane or in coffee shops. Again, this is an attorney responsibility.

In addition, lawyers can control their use of technology. For instance, the careless use of social media can lead to compromises of client information. Preventing careless social media usage by lawyers is not a "tech issue" to be handled only by staff.

C. The Duty to Supervise Staff and Third Parties

Lawyers in a law firm must supervise junior attorneys, support staff, and third parties with access to client information. Under the ABA Model Rules, lawyers "shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that," first, "all lawyers in the firm conform to the Rules of Professional Conduct,"[42] and second, that the conduct of a non-lawyer employed by, retained by, or associated with the lawyer, "is compatible with the professional obligations of the lawyer."[43] In California, the duty of competence entails a duty of supervision. A comment to the rule states, "The duties set forth in rule 3-110 include the duty to supervise the work of subordinate attorney and non-attorney employees or agents."[44]

Again, the ethical obligation of the lawyer is to maintain ultimate responsibility for the security function in his or her practice. This is not a duty that can be delegated to others. To the contrary, the lawyer must oversee subordinate attorneys, support staff, and third parties.

One specific issue that has come up in the context of supervision is whether a law firm may ethically use cloud computing services to store, share, use, and communicate client information. While a thorough discussion of choosing and supervising cloud service providers is beyond the scope of this paper, ethics opinions have stated generally that cloud computing is permissible, as long as lawyers take proper steps

---

[42] ABA Model Rule 5.1.
[43] ABA Model Rule 5.3.
[44] Cal. R. Prof. Conduct 3-110 discussion (citing cases).

when selecting and using services.[45] For example, in 2013, an Ohio opinion acknowledged that lawyers may use cloud services as long as they competently select an appropriate vendor, preserve confidentiality and safeguard client property, provide reasonable supervision of cloud vendors, and communicate with the client as appropriate.[46]

Ethics opinions recognize the limitations of lawyers' competencies. As the New Hampshire Bar has stated, "a lawyer's duty is to take reasonable steps to protect client information, not to become an expert in information technology," and "[w]hen it comes to the use of cloud computing, the Rules of Professional Conduct do not impose a strict liability standard."[47] *The ABA Cybersecurity Handbook* notes that "rapidly evolving technology means that these factors cannot provide a 'safe harbor.'"[48] Instead, "[l]awyers should monitor and reassess the protections of the cloud provider as the technology evolves."[49]

IV. Implementing an Effective Information Security Program

The upshot of these ethics rules is that a lawyer must make "reasonable efforts" to prevent inadvertent or unauthorized disclosure of client information, and to prevent unauthorized access to client information.[50] Nonetheless, the rules don't say what "reasonable efforts" are or what specific controls are necessary. How much security is

---

[45] *See* ABA Cybersecurity Handbook, *supra*, at 78 (explaining that state ethics opinions "make clear that a lawyer must have a basic understanding of the technical aspects of cloud computing, and should conduct due diligence evaluation of the provider to ensure that they have adequate security measures").

[46] *Cloud Ethics Opinions Around the U.S*., The American Bar Association, http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html (citing OSBA Informal Advisory Opinion 2013-03 (available at https://www.ohiobar.org/ForPublic/LegalTools/Documents/OSBAInfAdvOp2013-03.pdf)). Some states provide more specific requirements. For example, Maine lists seven requirements "the attorney should ensure that the vendor of cloud computing services or hardware" follows. Maine Board of Bar Overseers Opinion #207. *The Ethics of Cloud Computing and Storage* (available at http://www.maine.gov/tools/whatsnew/index.php?topic=mebar_overseers_ethics_opinions&id=478397&v=article).

[47] Barkett, *supra*, at 10 (quoting New Hampshire Bar Ethics Op. #2012-13/4).

[48] ABA Cybersecurity Handbook, *supra,* at 77.

[49] *Id*.

[50] ABA Model Rule 1.6(c).

enough under this standard? What is "reasonable"? The factors listed in Section III.A above (such as the level of sensitivity of the information) provide guidance, but they don't provide ideas to develop specific controls to implement in a security program. The flexibility of the rule's language is helpful to cover many circumstances, but the lack of precision makes it challenging to implement specific controls.

A full listing of all the security controls a law firm could implement is beyond the scope of this paper. The other Cybersecurity panel speakers will be presenting ideas for specific controls that a law firm could implement. Many secondary sources, such as *The ABA Cybersecurity Handbook*, present controls a law firm can implement.

As a brief summary, however, we present the following ideas for security controls a law firm could implement. The list is not meant to be exhaustive. Moreover, with changes in technologies, capabilities, threats, and the cost of security controls, law firms will need to review their practices over time.

Examples of administrative safeguards:

1. The firm has policies, procedures, guidelines, and training materials to govern the security function.
2. The firm undertakes a risk assessment to determine the threats to its client information in light of the sensitivity of the information.
3. The firm implements controls that manage its risk to a reasonable level, and it should consider obtaining insurance coverage.
4. The firm has named a person or team in charge of information security.
5. The firm has employment procedures by which workers are evaluated in part based on their compliance with security policies and procedures. Workers face discipline if they violate those policies and procedures.
6. The firm manages which members of its workforce have access to which kinds of information and change such access when job duties change.
7. The firm investigates the background of workers with access to client information to provide assurances that they are trustworthy and competent.
8. The firm has procedures when a worker leaves the firm to stop access to client information.
9. The firm has a program of security and privacy awareness and training, including periodic reminders and updates. Topics include the protection of electronic information, computer systems, preventing malicious software, social media practices, the protection of paper records, and not discussing client matters in public places.
10. The firm has procedures for security incident reporting and handling. It should have an incident response team to handle incidents.
11. The firm has procedures for backing up client information.

12. The firm has a disaster recovery and business continuity plan to provide assurances of continued operation in the event of a natural or man-made disaster.
13. The firm has procedures for auditing or assessing the effectiveness of its security controls.
14. The firm supervises third parties with access to client information.

Examples of Physical Safeguards

1. The law office has walls, doors, and windows that reasonably prevent physical intrusion. Server rooms have physical barriers that prevent people in lobby areas from accessing them.
2. People in waiting areas cannot see the screens of workers in the reception areas.
3. Workers are trained to prevent the loss or theft of mobile devices or media, especially while out of the office, such as when storing a device in a parked car or when working in a restaurant or coffee shop.
4. The firm maintains an inventory of computing devices.
5. Paper records are locked and desks are cleared of paper documents when they are not needed.
6. The firm wipes electronic data off of computing devices before they are transferred, sold, or reused.

Examples of Technical Safeguards

1. The firm controls access to systems with client information using strong passwords or other authentication mechanisms.
2. Individual workers have their own accounts on the firm network and computers.
3. Workstations log off users after a period of inactivity or otherwise require the user to reauthenticate him or herself to the system.
4. Client information is encrypted while at rest or in motion with reasonably robust encryption strength.
5. Networks and computer systems log user activity.
6. The firm uses software to prevent and detect malicious software.
7. The firm's networks are protected by technologies to control access, such as firewalls.
8. When reasonable and appropriate, the firm will implement specific technologies for intrusion detection, data loss prevention, and continuous monitoring.

V. Conclusions

Lawyers have ethical duties to maintain the confidentiality of client information used in their practices, to act competently in their practices, and to supervise staff and third parties with access to client information. These duties appear in the ABA Model Rules of Professional Conduct, state rules based on the Model Rules, and the California Rules of Professional Conduct. These are non-delegable duties. Lawyers must provide leadership and manage the information security functions in their firms and not simply turn over all information security functions to their staffs.

With increasing information security threats from various state and non-state actors, coupled with rapid advances in technology and how it is used, law firms face ever-greater threats to client information. The rules call for attorneys to use reasonable care to protect client information. An effective security program of administrative, physical, and technical safeguards can help a law firm and its lawyers mitigate their information security risks and comply with ethical obligations.

For more information, contact:
Drew Simshaw, dsimshaw@indiana.edu, 812.856.1497
Stephen Wu, ssw@svlg.com, 408.573.5737