




Safeguard Client Data

By || **HADLEY LUNDBACK MATARAZZO**

Attorneys, who are constantly entrusted with sensitive client information, must know how to secure that data—and their ethical obligations if a breach occurs.



To successfully represent clients, plaintiff attorneys must rely on technology to store and transmit confidential and sensitive information such as personally identifiable information (PII), personal health information (PHI), financial data, and attorney-client privileged communications. Storing this type of information—and the perception that we are less sophisticated regarding cybersecurity—makes lawyers and law firms particularly vulnerable to cyberattacks.¹

According to the ABA Standing Committee on Ethics and Professional Responsibility's Formal Opinion 477R, issued in 2017, it's not a question of whether a law firm will be a victim of a cyberattack but when and to what extent.² When a cyberattack causes a data breach, it erodes client trust and is costly both monetarily and with respect to the firm's reputation. Lawyers must understand cybersecurity risks; our ethical obligations for protecting the data we store and transmit; how to prevent, detect, and thwart cyberattacks; and our duties if we experience a data breach.

For more than two decades, lawyers and the ABA have grappled with a lawyer’s ethical obligations pertaining to the constantly evolving use of technology. In 2012, the “technology amendments” were added to the ABA Model Rules of Professional Conduct.³ Updates included the obligation to understand the risks and benefits of relevant technology⁴ and the obligation to take reasonable measures to prevent inadvertent or unauthorized disclosure of information pertaining to the representation.⁵ They also require lawyers to ensure their staff are trained on and take reasonable measures to prevent unauthorized disclosure of or access to this information.⁶

While the ethics committee does not dictate what constitutes reasonable steps a lawyer must or should take to protect sensitive data, it provides numerous

considerations to guide lawyers in this process.⁷ In practice, a lawyer can protect client information from inadvertent disclosure in various ways, so there is no one-size-fits-all approach.

Inadvertent Disclosure

Stopping all cyberattacks may be impossible, but 97% of cyberattacks can be thwarted by common security practices that firms of all sizes can use.⁸ At the outset, law firms must develop a culture that prioritizes cybersecurity. This starts by ensuring management has a basic understanding of cybersecurity and its importance to the firm. Management should then instill this belief in all lawyers and staff.

Cybersecurity policies. Management should create a cybersecurity policy and enforce it.⁹ It should cover areas such as

- requiring the use of strong passwords that must be changed on a quarterly basis and be substantially different from prior passwords
- prohibiting the use of work email for personal matters
- prohibiting logging onto personal email from a work computer
- limiting access to unauthorized websites

- installing software that tells email recipients whether emails are from internal or external senders
- designating a staff member to alert when phishing emails are received so suspicious email addresses can be blocked
- prohibiting clicking on links or opening attachments if emails are not from trusted sources.

Attorneys and staff should be educated about cybersecurity generally and the firm’s cybersecurity policies specifically, and these policies should be reinforced regularly in meetings and email communications.

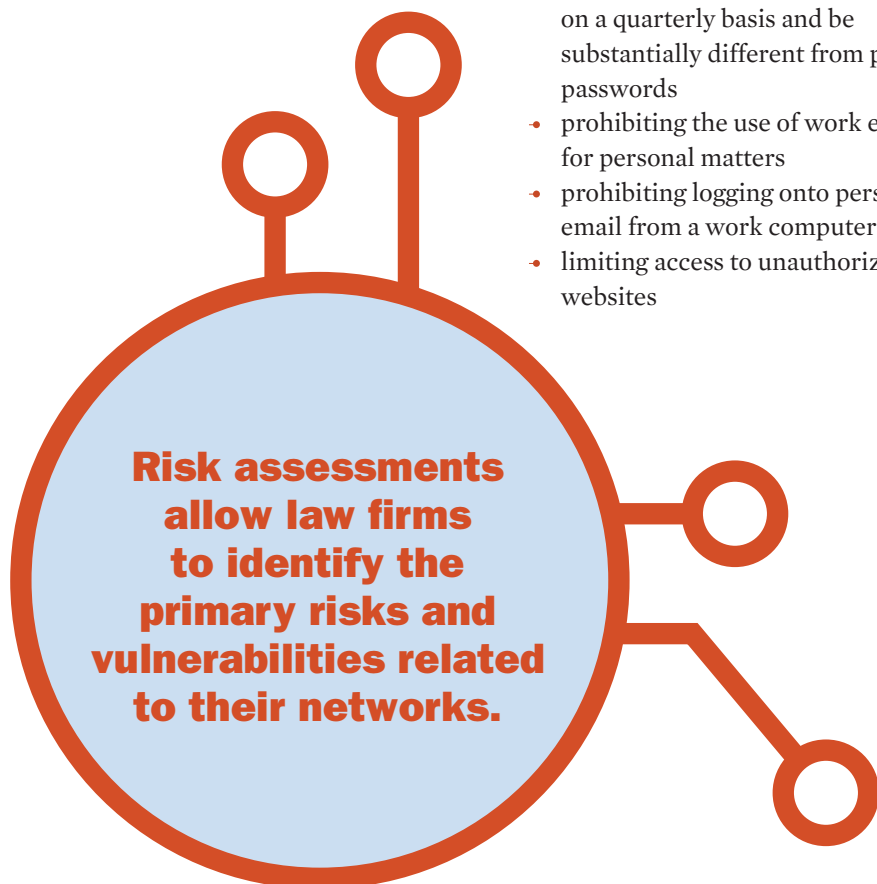
Technology inventory and risk assessment. Once an appropriate culture has been established, conduct an inventory of technology and sensitive data, as well as a risk assessment.¹⁰ Risk assessments allow firms to identify the primary risks and vulnerabilities related to their networks and to focus on the best way to mitigate those risks. The firm or its information security vendor will assess system or network boundaries, conduct data mapping, and consider existing security controls.

When evaluating system or network boundaries, the firm needs to answer questions such as:

- How many offices does the firm have?
- How many people have access to the firm’s network? Who are they, and what are their roles?
- How do these people have access to the network (through phones, tablets, or remote access)?

Once these boundaries have been delineated, determine what data is stored and exchanged; where that data is stored (for example, on the server, cloud, or local hard drives); and how that data is exchanged (possibly through email or file transfer protocols).

Security control review. Finally, analyze current security controls by



An ethical violation may be found when **reasonable efforts were not taken to protect confidential information** and because of this lapse, a breach occurred or was undetected for some period of time.



looking at management controls, operational controls, and technical controls. Management controls are actions taken to handle the development, maintenance, and use of the system, including system-specific policies, procedures, and rules of behavior; individual roles and responsibilities; individual accountability; and security decisions involving law firm staff and lawyers.

Operational controls are network security controls (such as safeguards or countermeasures) primarily implemented by people, not systems. This includes decisions about who at the firm should have access to sensitive data; procedures for how data should be maintained, sanitized for reuse, or destroyed; and contingency planning and disaster recovery. Technical controls are things such as software controls, including anti-virus software and intrusion detection and prevention software; firewalls; access limiters; forced password changes; and automatic device log offs after a brief period of inactivity.

After you identify the primary risks and vulnerabilities, analyze the trade-offs between cybersecurity and business disruption. Determine the general level of risk the firm is willing to accept to efficiently conduct its business and whether that level of risk is reasonable under the circumstances. For example, requiring additional password

protection within a network to access certain sensitive data may be generally desirable, but not if it slows down work flow in a network that already has dual authentication access protections.

Data security plans. Next, establish a data security plan within your firm's IT department or with IT vendors. Critical components of this plan include recurrent employee training and education; protective measures such as two-factor authentication for remote access; encryption of sensitive data at rest and in transit; and secure network use such as a private VPN for remote access.

The ABA also recommends "continuous maintenance of operating systems and software programs; installation of antivirus and firewalls to prevent common malware infections; conducting third-party vulnerability scans, penetration tests, and malware scans; and ensuring that the firm's protective measures extend to its remote access programs (e.g., Citrix, iTwin, Remote Control) for employees who use remote access."¹¹

Firms also should develop cybersecurity incident response plans.¹² These plans "strategically identify the protective measures that the firm has in place, what to do in the event of an attack, and long-term and short-term plans for updating the program overall."¹³

Designate a person at your firm responsible for overseeing these plans or responsible for overseeing the vendor doing so.

Cybersecurity insurance. Finally, seriously consider purchasing cybersecurity insurance, which can be obtained as a rider to the firm's professional liability policy or as a separate cyber policy. The policy can help defray the cost of a data breach response, cyber extortion, data recovery, business interruption, and privacy and security liability.

Ethical Obligations After a Data Breach

In the unfortunate event that data is inadvertently disclosed, lawyers now have clear guidance regarding our ethical obligations. In 2018, the ABA issued Formal Opinion 483, its first addressing the obligations of lawyers who are the victims of a data breach or cyberattack.

For purposes of this opinion, a data breach is defined as "a data event where material client confidential information is misappropriated, destroyed or otherwise compromised, or where a lawyer's ability to perform the legal services for which the lawyer is hired is significantly impaired by the episode."¹⁴ This definition is broad enough to include various situations.

For example, it could involve a data

breach in which sensitive client data is removed from a lawyer's computer network or when a ransomware attack prevents a lawyer from accessing a client's file. It also could include an attack involving destruction of a lawyer's computer network, blocking the lawyer from accessing the confidential information necessary to perform legal services.

Detecting a breach. Based on the model rules discussed earlier, the opinion concluded that "lawyers must employ reasonable efforts to monitor the technology and office resources connected to the internet, external data sources, and external vendors providing services relating to data and the use of data."¹⁵ Formal Opinion 483 clarifies that a breach or the failure to immediately detect one does not necessarily give rise to an ethical violation if reasonable steps were taken to protect the information.¹⁶ But an ethical violation may be found when reasonable efforts were not taken and because of this lapse, a breach occurred or was undetected for some period of time.¹⁷

If a breach is suspected or detected, a lawyer must "act reasonably and promptly to stop the breach and mitigate damage resulting from the breach."¹⁸ The ABA recommends having an incident response plan in place to deal with a suspected or actual breach.¹⁹ This plan supports responding to incidents systematically with a consistent methodology, ensures appropriate actions are taken, and minimizes loss or theft of information and disruption of services.

An incident response plan should include

- identifying and evaluating any potential anomaly or intrusion
- assessing the anomaly or intrusion's nature and scope
- determining whether any data or information may have been accessed or compromised
- quarantining the threat or malware

- preventing exfiltration of information, eradicating malware, and restoring the integrity of the firm's network.

Regardless of whether a plan is in place, "a competent lawyer must make all reasonable efforts to restore computer operations to be able again to service the needs of the lawyer's clients."²⁰ The lawyer also must conduct a post-breach investigation to determine that the breach has been stopped and to figure out what information, if any, has been exposed.

Client notice. Finally, to meet the requirements of Model Rule 1.4, a lawyer must notify current clients when the "unauthorized release of confidential information could reasonably be viewed as a significant factor in the representation."²¹ This includes situations when the client's position or legal matter may be impacted.

The content of the notice to the client depends on the circumstances of the data breach and must be tailored accordingly. The notice must provide sufficient information for the client to make an informed decision about what to do next.²² At a minimum, the lawyer must tell the client what sensitive information may be at risk and how it may have been accessed, unless the lawyer is unable to ascertain this information after taking reasonable steps to do so.²³

While not required, the committee recommends that lawyers inform clients of the steps being taken to respond to the breach and, when applicable and feasible, to recover the data.²⁴ Lawyers have an ongoing obligation to keep the client apprised of any material information obtained from the post-breach investigation.

Interestingly, the committee has declined to extend this requirement to former clients under Model Rule 1.9 without "a black letter provision requiring such notice."²⁵ However, Formal Opinion 483 notes that, consistent with

best practices, lawyers should reach an agreement with clients at the termination or conclusion of representation to determine how to handle the client's electronic information.²⁶ Absent an agreement, lawyers should have and follow a document retention policy, compliant with applicable laws and regulations.²⁷

Formal Opinion 483 does not address legal obligations a lawyer may have under federal or state privacy and notification laws such as HIPAA or the Gramm-Leach-Bliley Act or any other statutes that may be implicated. But the committee notes that when PII such as a client's Social Security number is implicated, lawyers should familiarize themselves with applicable federal and state notification laws.²⁸ Lawyers who have been the victims of an attack need to understand and comply with all legal obligations.

We rely on technology to store and transmit our clients' confidential and sensitive information—it's key that we understand how to secure that data and our ethical obligations if a breach occurs. ▣



Hadley Lundback Matarazzo is an attorney at *Faraci Lange* in Rochester, N.Y., and can be reached at hmatarazzo@faraci.com.

NOTES

1. Lawyers and law firms are susceptible to attack by disgruntled current and former employees, cyber criminals, and even state-sponsored hackers. Eli Wald, *Legal Ethics' Next Frontier: Lawyers and Cybersecurity*, 19 Chap. L. Rev. 501 (2016).
2. The ABA's "2020 Legal Technology Survey Report" showed that the majority of law firm respondents still have not taken adequate protection measures such as encryption, two-factor authentication, intrusion protection, intrusion detection, remote device management and wiping, web filtering, and employee monitoring.

However, the responses did show an increase in the number of firms that purchased cyber liability insurance policies. Am. Bar Ass'n, *ABA TechReport 2020*, https://www.americanbar.org/groups/law_practice/publications/techreport/2020/.

3. ABA Standing Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R, at 2 (2017).
4. Model R. Prof'l Conduct 1.1 cmt. 8.
5. Model R. Prof'l Conduct 1.6(c) cmt. 18 & 19.
6. Model R. Prof'l Conduct 5.1, 5.3.
7. See ABA Standing Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R. The committee concludes that "a lawyer generally may transmit information relating to the representation of a client over the internet without violating the Model Rules of Professional Conduct where the lawyer has undertaken reasonable efforts to prevent inadvertent or unauthorized access." *Id.* at 11. This updated Formal Opinion 99-413 (1999), which addressed a lawyer's confidentiality obligations regarding emails with clients.
8. Robert Hilson, *This Article on Lawyer*

Cybersecurity Will Scare You Out of a Malpractice Suit, Logikcull, June 10, 2016, <https://blog.logikcull.com/paper-lawyer-cybersecurity-will-scare-malpractice-suit>.

9. For more on law firm cybersecurity policies, see Karen Barth Menzies, *The New Normal: Working From Home*, Trial, June 2020, at 22; Ingrid M. Evans, *A Firm Tech Foundation*, Trial, Mar. 2019, at 18; Tad Thomas & Rich Smith, *Decoding Cybersecurity*, Trial, Mar. 2017, at 22.
10. David G. Ries, *ABA TechReport 2017: 2017 Security*, Am. Bar Ass'n, Dec. 1, 2017, <https://tinyurl.com/35dfkn4z/>.
11. Joseph Salvo & Brian Middlebrook, *Cybersecurity and the Lawyer's Standard of Care*, Am. Bar Ass'n, May 22, 2018, <https://tinyurl.com/yzx6bezx>.
12. Law firms can work with an information security or cybersecurity vendor to formulate plans, but there are also many online resources to assist firms in developing plans. For an example of an incident response plan template, see FRSecure, *Incident Response Plan Template*, <https://frsecure.com/incident-response-plan-template/>. For an example of an incident response plan, see Cynet, *6 Incident Response Plan Templates and Why You Should Automate Your Incident Response*, May 23, 2021, <https://www.cynet.com/incident-response/incident-response-plan-template/>.

13. Salvo & Middlebrook, *supra* note 11.
14. ABA Standing Comm. on Ethics & Prof'l Responsibility, Formal Op. 483, at 4 (2018).
15. *Id.* at 5.
16. *Id.* at 5-6.
17. *Id.* at 6.
18. *Id.*
19. *Id.*
20. *Id.* at 7.
21. *Id.* at 11; see also ABA Standing Comm. on Ethics & Prof'l Responsibility, Formal Op. 95-398, at 2 (1995).
22. ABA Standing Comm. on Ethics & Prof'l Responsibility, Formal Op. 483 at 14.
23. *Id.*
24. *Id.*
25. *Id.* at 13.
26. *Id.*
27. *Id.*
28. *Id.* at 15.

Brand New! Technology Section



Section Specific
List Servers



AAJ Section
Document Libraries



Strategic Advice from
other Trial Attorneys



Meetings and Section
Specific CLE's



Special
Discounts



Section Specific
Quarterly Newsletters

HOW TO JOIN

Call: 800-424-2725

Online: justice.org/TechSection