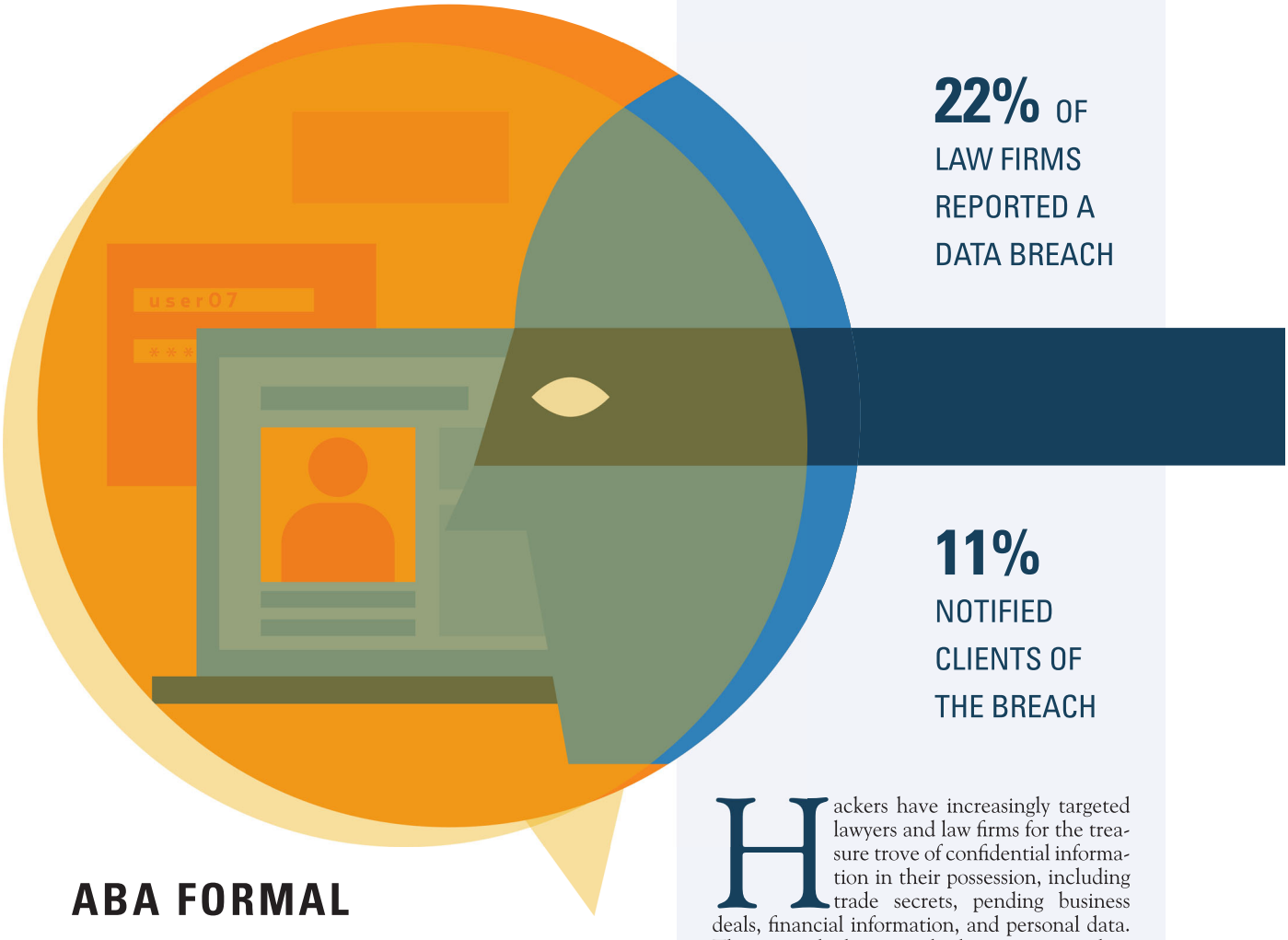

22% OF LAW FIRMS REPORTED A DATA BREACH

11% NOTIFIED CLIENTS OF THE BREACH

ABA FORMAL OPINION NO. 483, DATA BREACHES, AND YOU

What's your plan? New ethics opinion requires lawyers to take steps to protect client data from cyber threats.

By Kevin P. Hickey and Jeff Alluri

Hackers have increasingly targeted lawyers and law firms for the treasure trove of confidential information in their possession, including trade secrets, pending business deals, financial information, and personal data. These attacks have resulted in numerous data breaches compromising confidential client information at firms of all sizes in recent years. According to the American Bar Association (ABA) 2017 Legal Technology Survey, 22 percent of responding law firms reported a data breach at some time, a substantial increase from 14 percent the year before.

Law firm security breaches were not limited to larger firms that might be expected to have more valuable data. Rather, law firms of all sizes, including solo practitioners, suffered data breaches. The highest rate of data breaches was in law firms with 10-49 attorneys, at 35 percent. Because of these security breaches, 17 percent of law firms reported the breach to law enforcement and 11 percent notified clients of the breach.

These ever-increasing threats are constantly changing and are limited only by the imaginations of the hackers and cyber-thieves behind them. While there has always been a legal and ethical basis for protecting client data from these threats, this responsibility has been made even clearer by the issuance of ABA Formal Opinion No. 483.

FORMAL OPINION NO. 483

The ABA's Standing Committee on Ethics and Professional Responsibility has recently issued an ethics opinion addressing a lawyer's duties to protect against data breaches. ABA Formal Opinion No. 483 provides:

> *Model Rule 1.4 requires lawyers to keep clients "reasonably informed" about the status of a matter and to explain matters "to the extent reasonably necessary to permit a client to make an informed decision regarding the representation." Model Rules 1.1, 1.6, 5.1 and 5.3, as amended in 2012, address the risks that accompany the benefits of the use of technology by lawyers. When a data breach occurs involving, or having a substantial likelihood of involving, material client information, lawyers have a duty to notify clients of the breach and to take other reasonable steps consistent with their obligations under these Model Rules.*

This opinion is grounded in three fundamental ethical principles. First, a lawyer's duty of competence under Model Rule 1.1 requires the lawyer to provide competent representation to a client. The comment to this Rule makes it clear that this duty of competence includes "the benefits and risks associated with relevant technology…." From a practical standpoint, this duty of competence includes an obligation to monitor for a data breach, stopping and restoring any such breach, and determining what occurred so that any harm or loss can be assessed and corrected.

Second, the opinion is based on a lawyer's duty of confidentiality under Model Rule 1.6. The comments to this Rule emphasize that a lawyer must take reasonable measures to safeguard client information and protect it from unauthorized access or disclosure. This does not mean that the lawyer's information systems must be impenetrable. Instead, the comments provide a multi-factor "reasonable efforts" approach that includes consideration of the sensitivity of the information, the likelihood of disclosure, and the costs and difficulties of employing additional safeguards.

Third, the opinion is grounded on a lawyer's duty to keep clients reasonably informed regarding their matter under Model Rule 1.4. This duty requires the lawyer to communicate with clients about a data breach. This includes a duty to notify clients of a data breach when it involves or is likely to involve material client confidential information.

What this opinion makes clear is that lawyers need to have a detailed plan in place to: (1) assess whether a data breach has occurred involving material client information; (2) notify clients of any such breach; and (3) to take reasonable steps to address the situation. Many lawyers and law firms do not have such a plan, or the plan is not updated to reflect the latest cyber security threats. (See also Robert Cattanach and Samir Islam, "Preparing for a Hack of Your Law Firm," B&B Sept. 2017.) Formal Opinion No. 483 is a call to all lawyers and legal organizations to develop or update such a plan in order to comply with ethical obligations to clients. In short, lawyers and legal organizations must be prepared to protect against and respond to a cyber security incident.

DEVELOPING AN INCIDENT RESPONSE PLAN

Developing an incident response plan is not as painful as it sounds. The plan will necessarily evolve over time as technology changes and new threats arise. The starting point is that lawyers should collaborate with their IT professionals and others in the field to gain insight and knowledge that will form the basis of the plan. Key personnel from the organization and its vendors should be included in developing the plan.

The first step is to form an incident response team that may consist of the firm administrator, head of IT, general counsel, the managing partner, or other key personnel. While it is common for "incidents" to be handled by the IT department or vendor, developing a plan is a shared responsibility that should not be placed solely on the shoulders of IT. Each member of the team should have a clearly defined role to allow the team to move quickly and competently to address a threat or breach.

With the team formed, the next step is to document all of the ways the firm interacts with its employees and its clients. In the event a breach affects any of these communication systems, what is the backup plan to communicate? Document all mission-critical systems and note weaknesses in the systems to ensure the firm can mitigate incidents properly.

The next step is to begin drafting the incident response plan. The plan should be very detailed and address all foreseeable contingencies. The National Institute of Standards and Technology (NIST) cybersecurity framework 1.1 is a critical resource in developing a plan and should be carefully followed. In general, the plan should focus on five main areas: assess, contain, communicate, document, and mitigate.

1

ASSESS

The entire organization should be educated on how to quickly identify and assess a potential breach. The organization should implement a security awareness program that includes regular and relevant education on the latest cyber security threats. This should include raising awareness by testing vulnerabilities through a mock phishing exercise or other programs. All lawyers and other end-users should be trained to report anything unusual while using their computer systems or other devices.

Establishing a baseline is critical to effective assessment of the breach. The organization needs to know how something normally behaves to recognize that it is no longer doing so. This means documenting and tracking behavior on a network to recognize changes as well as having a firm grasp of fundamentals to know when something is amiss. For end-users, this means recognizing abnormal behavior and reporting it immediately to IT and other firm personnel as identified within the plan.

2

CONTAIN

It doesn't take long for bad actors to make things a lot worse. Containment should focus on preventing further harm. The best way to contain the threat is to restrict access by closing open network ports, changing passwords, suspending elevated privilege accounts, or isolating the computer(s) from the network.

Take caution in the actions during containment and make sure to thoroughly communicate. While these actions may prevent the bad actors from causing more damage, they can also interfere with employee productivity. IT should discuss the potential impact of these actions with firm management to ensure continuity of mission-critical functions during containment.

3

COMMUNICATE

Formal Opinion No. 483 emphasizes the importance of communication in the event of a breach. Lawyers are required to act promptly and responsibly in notifying clients of a breach. It is equally important to increase internal communication to ensure everyone is aware of the situation and is working together to help mitigate further risk.

Outline communication details in the plan and identify a point person to coordinate communication throughout the remediation of the breach. Identify who will communicate with clients, personnel, vendors, and law enforcement if necessary. Draft or form communications are advisable to expedite notification if a breach occurs. If the breach impacts any communication system, make sure there is a back-up method to communicate (for example, use texting if the email system is compromised). The bottom line is that everyone must know who to communicate with, how to communicate with them, and when to communicate.

4

DOCUMENT

It is extremely important to document each step taken during an incident. Not only can this help with communication, it can also help to mitigate the current problem and prevent the next one. This may include imaging the affected computer(s) for later analysis.

The document phase should identify what computer(s) were accessed, the origin of the attack, whether malware was used, connections made to and from the system, and finally, whether data was taken, altered or destroyed. If confidential client information has been compromised, this information must be immediately identified and documented so that any harm can be assessed and mitigated, and so that the client can be adequately informed of the impact of the breach.

5

MITIGATE

Common mitigation techniques focus on the removal of malware and/or ransomware, patching vulnerabilities, shutting down any improper access that may have been gained during the incident, and resetting passwords. It is very common to identify additional vulnerabilities during the mitigation process. These vulnerabilities should be documented and addressed promptly.

CONCLUSION

Formal Opinion No. 483 makes it clear that now, more than ever, lawyers and legal organizations must be fully prepared to address a cyber security incident. Developing a comprehensive incident response plan is a necessary first step. But beyond that, lawyers should strive to create an organizational culture of security and privacy through response plans, ethical and legal compliance, and best practices. ▲

***KEVIN P. HICKEY** is a shareholder at Bassford Remele, PA, where his litigation practice includes representing lawyers and law firms. He also serves as general counsel to the firm.*
KHICKEY@BASSFORD.COM

***JEFF ALLURI** is a principal and VP of consulting at Element Technologies, LLC, a full-service information technology firm.*
JALLURI@ELE-MENT.COM