Prevention and Response: A Two-Pronged Approach to Cyber Security and Incident Response Planning

By Steven M. Puiszis

Steven M. Puiszis is a partner with Hinshaw & Culbertson LLP, and serves as the Firm's General Counsel-Privacy, Security & Compliance. He is a member of Hinshaw's Lawyers for the Professions Practice Group, which represents lawyers and law firms in liability, professional responsibility matters. Mr. Puiszis is a Fellow of the American Bar Foundation, the Chair of DRI's Center for Law and Public Policy and is a past president of the Illinois Association of Defense Trial Counsel.

Introduction

Today the issue is not if a law firm will suffer a cyber intrusion, but when, and what type. Therefore, the critical question for any law firm is how well it will respond when the inevitable happens. A law firm's response to a cyber security incident can be the difference between keeping and losing a client, and maintaining the reputation or perhaps even the stability of the firm. Clients are mandating that their law firms have safeguards in place to prevent a data breach. But technology is far from foolproof, and even the strongest technical, administrative, and physical safeguards are no guarantee that a law firm will not be breached.

A client may be willing to forgive a lawyer who was fooled by a phishing exploit and clicked on a link that launched malware onto the lawyer's computer. A client may understand how an iPhone or laptop computer could be lost or stolen. But a client may not forgive a firm that fumbles an opportunity to prevent this type of security incident from turning into a full-fledged breach resulting in the exfiltration of the client's sensitive information. A law firm's unsuccessful efforts to prevent the compromise of client or third-party data will be critically reviewed after the fact, by those clients and third parties as well as their lawyers.

A two-pronged approach addressing both prevention and response is critical to this area of law firm risk management. Law firms should: (1) implement strong safeguards to prevent cyber intrusions and data breaches; and (2) prepare to promptly address such an incident when one occurs. While some might suggest that developing an incident response plan as part of a two-pronged approach is not ethically required under the reasonable efforts standard of Model Rule 1.6(c), client guidelines are increasingly requiring them. To the extent a response plan may assist in preventing an actual breach, it could be considered a reasonable step under Rule 1.6(c). [1]

How well a law firm responds to a security incident or cyber intrusion depends on how prepared the firm is when one occurs. Security experts believe the hours immediately following a cyber intrusion are the most critical. Accordingly, the time to prepare for a breach is *before* one occurs. Trying to determine

what steps should be taken under the stress of a potential breach is far from ideal and can potentially result in delays, missteps and mistakes. The cardinal rule of law-firm risk management is to never make a problem worse, and not having measures in place to address a potential breach is inconsistent with that principle.

Cyber security sits at the intersection of law and technology. Because even tech-savvy General Counsel may not be familiar with critical features of a law firm's network architecture and its latest cyber security measures, a strong working relationship between the firm's General Counsel (or the equivalent position), and its Chief Information Officer (CIO), Chief Security Officer (CSO), Director of Information Technology (IT), or an outside IT vendor (depending on the firm's structure) is critical to this area of risk management for law firms.

There is no "one-size-fits-all approach" to how a law firm should protect the data in its possession, and the same is true when it comes to developing an incident response plan. Security professionals speak of "defense in depth" or layers of security, but what those layers may consist of can depend on a variety of factors such as a firm's size, geographic footprint, organizational structure, practice areas, technological sophistication, culture and available resources. Those same factors will also influence the processes and steps outlined in the firm's incident response process.

While incident response plans may vary from firm to firm, their goals are the same and similar concepts are consistently found in various incident response plans to achieve those goals. The primary goal of any incident response plan is to have a process in place that will allow the firm to promptly respond in a coordinated manner to any type of security incident or cyber intrusion. The incident response process should promptly: identify and evaluate any potential network anomaly or intrusion; assess its nature and scope; determine if any data or information may have been accessed or compromised; quarantine the threat or malware; prevent the exfiltration of information from the firm; eradicate the malware, and restore the integrity of the firm's network.

Incident response plans should identify the team members and their backups; provide the means to reach team members at any time an intrusion is reported, and define the roles of each team member. The plan should outline the steps to be taken at each stage of the process, designate the team member(s) responsible for each of those steps, as well as the team member charged with overall responsibility for the response.

Evidence as to how the breach occurred may prove to be critical if litigation, or an administrative or a criminal investigation, subsequently occurs and should be preserved in a forensically sound manner. The response plan should identify a team member designated by the firm's General Counsel to record information about the intrusion or breach. The record should include how and when the intrusion occurred; who, when, and how it was discovered; the nature of any malware involved; each step taken to contain the intrusion and eradicate the threat; when those steps were taken; and the team member(s) or third parties involved in each step of the process. The response plan should also address how to handle media inquiries, the firm's potential statutory and ethical reporting obligations, and procedures for notifying law enforcement when appropriate.

With the growing recognition of in-firm privilege [2] , the law firm's General Counsel should play a key role in the response process. An outside counsel equivalent may play the same role for firms that do not have a general counsel. General Counsel should be involved in contacting any third-party vendors participating in the response process to assist in the provision of legal advice to the firm in an attempt to shield those communications and work product from later discovery if necessary. *See In re Target Corp. Customer Data Security Breach Litigation*, 2015 WL 6777384 (D. Minn. Oct. 23, 2015) (recognizing and applying attorney-client privilege and work product protection following a data breach); *Genesco,Inc., v. U.S.A., Inc.*, 307 F.R.D. 168 (M.D. Tenn. 2014) (applying attorney-client privilege and work—product protection to bar deposition, records, and communications of forensic investigator following the investigation of a cyber attack). General Counsel should also be involved in assessing any statutory or ethical reporting obligations, and in the drafting process should it be determined if a notification needs to be sent.

The following sections will provide a checklist of concepts that law firms should consider in developing an incident response plan and the risk management steps to consider before a cyber intrusion occurs. A checklist of considerations for when a cyber intrusion occurs is also provided.

1. Risk Management Steps Law Firms Should Consider Before a Security Incident Occurs

There are risk management steps that a law firm should consider before a cyber intrusion occurs that may impact the firm's incident response plan and its strategic security considerations:

- Evaluate how information enters, moves through and exits the firm's network.
- Evaluate where information is stored and how it can be accessed by lawyers and staff. Don't overlook third party vendors, the Cloud, personal devices and home computers.
- Identify sensitive, highly sensitive, or confidential information in the firm's possession.

Since not all this information may be of equal value or importance, identify where sensitive or confidential information is stored and evaluate if additional safeguards should be applied to these categories of information.

Sensitive, highly sensitive or confidential information will frequently include personally identifiable information (PII); personal health information (PHI); nonpublic financial information; trademarks; trade secrets; patent or M&A information; customer data and any other information that client indicates should be treated as highly confidential.

- Identify those persons or entities that have physical or electronic access to your network and those that have potential access to sensitive and confidential information. Evaluate if they need or should have access to sensitive or confidential information and block access for those who do not need access. When third parties have electronic access to the network, evaluate segmenting the area of the network they can access.
- Identify potential vulnerabilities at each data access point.
- Evaluate the firm's existing physical, administrative and technical safeguards at each data access point.

- Take steps to remediate vulnerabilities or weaknesses at each access point.
- Prioritize remediation steps addressing the most critical vulnerabilities first in light of available resources.
- Consider an outside IT forensic or network security vendor if necessary to assist with identifying vulnerabilities or prioritizing remediation steps.

Measures that firms should consider to mitigate common attack vectors include: applying newly released patches to close identified vulnerabilities; controlling the use of unsecured public Wi-Fi and the use of dual factor authentication for remote access; encrypting laptop computers; mobile devices; back up and portable storage media; limiting and protecting administrative privileges over firm equipment and its network; training lawyers and staff about phishing and social engineering exploits, and properly disposing of digital equipment.

- Evaluate your cyber coverage for data breaches or security incidents. Cyber insurance isrelatively new and carriers' forms and terms can vary widely between different insurers.
- Review your firm's computer policies and log-on banners to ensure they include consent to real time monitoring of any email traffic or network use.
- Become familiar with the reporting obligations imposed by state data breach notification laws [3] and under HIPAA if the firm qualifies as a Business Associate. *See* 45 CFR §§ 164.400-.414(2014). HIPAA includes reporting obligations to the Secretary of HHS in §164.408 and to the news media in §164.406 (when the breach involves more than 500 residents of the state).
- Check any outside counsel guidelines and business associate agreements for additional reporting obligations.
- Train lawyers and staff on data security and cyber issues including recognizing phishing and social engineering exploits, signs that a computer may be infected and who to contact at the firm in that event. Once the response team and the process or plan have been developed, consider running tabletop exercises (hypothetical or simulated cyber incidents) to identify gaps in the plan and to insure team members are aware of the steps that each need to take.

Establishing an Incident Response Plan and Team

In planning how to deal with a cyber intrusion a firm must consider both the steps to be taken and the personnel who will take them.

The Incident Response Team

A firm's response team should be interdisciplinary because of the various issues potentially raised by a data breach or a security incident.

- Response team members assigned to particular security incidents or cyber intrusions can vary depending on the nature of the incident and the type of information or data involved.
- Each team member should have at least one designated backup person capable of performing the same function to ensure availability around the clock, 365 days a year.
- Communications between team members should be addressed in the response plan as team members should not attempt to use a potentially compromised network or phone system (or one that is not functioning) to communicate with one another about the incident or their response activities.

- Response teams frequently include internal and external members. Depending on the size and structure of the internal team, members can include: firm General Counsel or the firm's equivalent officer; a member of the firm's Management Committee; the firm's CIO, CSO, or Director of IT (or some combination thereof depending on firm structure); members of the firm's IT and Human Resources (HR) Departments (when HR data is compromised); and, members of the firm's Public Relations or Marketing Department(s).

A firm should evaluate required skill sets to complete each potential step in the response process, and if any firm employee has that skill. If not, determine, identify and evaluate outside vendor candidates. For example, there are third party vendors available to handle forensic investigations of the firm's network and equipment, support services vendors that handle mailings of breach notifications and track responses. The firm may set up outside toll-free hotlines or call centers and offer free credit/identity theft monitoring and restoration services. The firm may also consider outside communications/PR support when appropriate. A firm should consider developing law enforcement and third-party vendor contacts as a preparatory step.

Firm General Counsel should designate a team member to record relevant information about the cyber intrusion including steps taken to contain and eradicate the malware. Team members should be instructed to report information to the plan's scrivener and other designated team members on a daily basis and trained on what to say and how to say it.

General Counsel should consider designating the firm's spokesperson in the event of a breach and identifying how media inquiries should be handled, and who is responsible for working with internal or third-party communications or PR professionals.

If the firm has cyber coverage, check with the carrier about preapproved third-party vendors to handle these functions and consider adding the vendors to your response plan. Cyber carriers frequently have designated lawyers to serve as a "data-breach coach," and many provide coverage for PR assistance.

The Incident Response Plan and Process

A firm's response plan should be flexible and ideally be capable of addressing any type of cyber intrusion or security incident ranging from a lost smartphone or laptop computer to an industrial or state—sponsored intrusion or a distributed denial-of—service (DDoS) attack on the firm. The plan should include steps to address security incidents or breaches stemming from the mishandling of paper records, too.

Here are some steps to conisider incorporating into the plan:

- Determine the persons at the firm who receive notifications of these cyber alarms, how they are notified and how quickly they can react. Have more than one person receive these notifications.
- Identify and list each internal and external team member and each member's backup. Contact information, including the home, cell phone numbers and personal email address of each team member and backup should be included in the plan.

- Identify the roles and responsibilities of each team member so that every team member knows who is responsible for each step outlined in the plan. Distribute the plan to each team member and evaluate storing the plan in a secure network location that each team member can access.
- Designate a team member to record relevant information about the cyber intrusion including the steps taken to contain and eradicate the malware. Team members should be instructed to report information to the plan's scrivener and other designated team members on a daily basis and trained on what to say and how to say it.
- Identify the team members to whom a suspected incident or intrusion should be reported, and the team member(s) responsible for initially evaluating the intrusion and classifying the incident.
- Set up an 800 phone number and an email address to report suspected cyber incidents or data beaches such as: breach@[insert law firm name].com.
- Designate the firm's spokesperson in the event of a breach and identify how media inquiries should be handled, and who is responsible for internal or external communications, and for working with PR professionals.

Whenever possible, a law firm should avoid responding to press inquiries or making a public announcement before it can answer:

How and why the intrusion or incident occurred;

Whether information was acquired or compromised by a hacker or third party;

What the firm is doing to prevent it from happening again;

What the firm is doing to mitigate the harm to anyone affected by the breach and to protect its clients' interests.

The goal is to make a single response, not multiple ones, to limit the reputational harm resulting from the incident. If the firm receives a press inquiry before it is ready to provide answers, an appropriate response is that the firm is aware of the incident and is investigating.

Also, if the initial evaluation does not classify the intrusion as a false alarm, the plan should outline the next steps to be taken depending upon what the evaluation reveals about the nature of the intrusion, the malware involved and the scope of the impact on the network. Appropriate team members should be deployed depending upon the nature of the incident and the extent of the compromise.

The process outlined in the plan should include periodic or continuous evaluations of the threat and permit or require a change in the response if it is determined that the threat is greater or less than originally evaluated.

The plan should also consider:

- preserving critical information such as server and network logs.

- requiring that the team scrivener record when and how the security incident or cyber intrusion occurred, who discovered it and when it was discovered, the type of malware involved, when team members were deployed, and the steps taken to confirm, quarantine and eradicate the threat.
- having a breach communications outline in place, which takes into account state and federal reporting obligations, obligations imposed by client agreements or guidelines, as well as applicable ethical standards.
- outlining at what point in the process the firm's management should be made aware of the intrusion or incident. The contact or relationship partner for any client whose information was compromised should be notified once that determination has been made. That partner will assist with communications to the affected client.

2. Risk Management Steps Once an Actual Cyber Intrusion or Security Incident Is Confirmed

After an intrusion or security breach is confirmed, there are also steps that a firm should take in response:

- Any infected equipment should be disconnected from the network, but not otherwise disturbed. If the equipment is powered off, leave it off and if on leave it turned on. Don't forget to disconnect any WiFi connection. The infected equipment should be secured pending a forensic analysis.
- Any lost or stolen mobile device should be remotely wiped, to the extent the firm has the technological capability to do so, promptly after notification of the loss or theft. In a BYOD environment, be sure to obtain the prior written consent of the device owner to wipe any personally owned mobile device.
- Internal or external team members responsible for forensically examining any infected equipment and the network should be immediately dispatched to further evaluate the nature and extent of the intrusion.
- Critical logs from firewall, routers, servers, and network access should be preserved in a forensically sound manner.
- Details and information about the intrusion and the firm's response should be recorded as they become known.

The response team should:

- Complete the forensic analysis of any compromised equipment and the network.
- Evaluate if any client or firm information was acquired or accessed during the intrusion. Identify the clients, third parties or employees that own any data that was accessed or compromised, or who may be affected as a result of the intrusion.
- Identify, locate and eradicate any malware in the network or on the equipment and restore the integrity of the network.
- Consider retaining a third-party forensic expert to determine if any "back doors" were built into the network and that it is secure. This information may be of critical importance when notifying a client.
- Evaluate the need to contact law enforcement and how to protect client confidentiality.
- Attempt to retrieve any compromised data and take steps to potentially mitigate any harm.

- Restore any exfiltrated information, or in the case of ransomware, any encrypted data or files from backup media.
- Evaluate and address any reporting obligations under state or federal law, client guidelines or agreements, and any ethical obligation to report under Model Rule 1.4 or a state's equivalent provision.
- Evaluate if the intrusion or incident triggers a personal interest conflict for any affected clients under Model Rule 1.7 or a state's equivalent provision.
- Provide notice of the incident to the firm's professional liability or cyber carrier. Preferably this should occur promptly after confirmation of an actual cyber intrusion or security incident.
- Determine what to tell clients, employees or the public about the breach.
- Consider retaining outside counsel specializing in ethics, cyber security and/or the defense of law firms
- Consider retaining third-party support services vendors for credit monitoring, toll-free hotline, etc.

Post-Incident Evaluations Once the Response Process Is Complete

After a response team has gone through these steps, it should then:

- Critically evaluate how the intrusion occurred and what steps can be taken to prevent a reoccurrence.
- Address and remediate any vulnerability that caused or contributed to the intrusion or breach.
- Evaluate, address and remediate any other weaknesses or deficiencies uncovered during the response process in the firm's administrative, physical or technical safeguards.
- Review the response process and evaluate the performance of the team members and determine if the process or their performance can be improved.
- Identify any gaps or weaknesses in the response plan and if necessary modify the plan. Then train team members on any revisions.
- Evaluate the need for additional or specific training for lawyers and staff to address the cause of the intrusion or breach.
- Periodically review and test the plan.

3. Ethical Reporting Obligations

Model Rule 1.4(a) addresses a lawyer's duty to communicate with a client, and among other things, requires a lawyer to keep the client reasonably informed about the status of a matter, promptly comply with reasonable requests for information, and promptly inform the client of any circumstance to which informed consent may be required. This includes the "duty to inform the client of material adverse developments, including those resulting from the lawyer's own errors." Colo. Bar Ass'n, Formal Op. 113 (2005).

That does not mean a lawyer must volunteer every mistake or error that occurs during the course of representing a client. State ethics opinions recognize that "[p]rofessional errors exist along a spectrum." *Id.* These opinions recognize:

> [W]hether an attorney has an obligation to disclose a mistake to a client will depend on the nature of the lawyer's possible error or omission, whether it is possible to correct it in the pending proceeding, the extent of the harm resulting from the possible error or omission, and the likelihood that the lawyer's conduct would be deemed unreasonable and therefore give rise to a colorable malpractice claim.

N.Y. State Bar Ass'n, Ethics Op. 734 (2000); Colo. Bar Ass'n, Formal Op. 113 (2005) ("At the other end of the spectrum are errors and possible errors that may never cause harm to the client, either because any resulting harm is not reasonably foreseeable, there is no prejudice to a client's right or claim, or the lawyer takes corrective measures that are reasonably likely to avoid any such prejudice."). Obviously, whether an ethical duty to report exists will turn on the relevant facts. However, when a lawyer makes "a serious and irremediable error," an ethical duty to report that error to the client is triggered. N.Y. State Bar Ass'n, Ethics Op. 734 (2000).

These general principles should help guide the lawyer's ethical considerations about reporting a security incident or cyber intrusion. A lawyer does not have an ethical duty to report every time the lawyer clicks on a link and malware is launched onto a computer, or every time a hacker gains access to the law firm's network. When a client's data is not accessed or acquired during a security incident, a client has suffered no harm and no ethical duty to report the incident has been triggered. This view is further supported by ethics opinions that have addressed breaches of confidentiality by non-lawyers who are granted access to a law firm's computer network or a lawyer's database. ABA Formal Opinion 95-398 explained:

> Where the unauthorized release of confidential information could reasonably be viewed as a significant factor in the representation, for example where it is likely to affect the position of the client or the outcome of the client's legal matter, disclosure of the breach would be required under Rule 1.4(b).

ABA, Formal Op. 95-398 (1995); s *ee also* Vt. Bar Ass'n, Advisory Ethics Op. 2003-03 (2003) ("if the breach would affect the outcome of the client legal matter in any fashion, the lawyer would be obligated to tell the client of the breach by the non-lawyer");Ill. State Bar Ass'n, Advisory Op. 10-01 (2009) ("a lawyer may be obligated to disclose this breach to its client if it is likely to affect the position of the client or the outcome of the client's case"). Take care to also review your agreements and outside counsel guidelines for they may impose a reporting obligation upon the firm when there may be no ethical obligation to report.

A lawyer's duty is to act in the client's best interests in fulfilling a client's expectations for information. Model Rules of Prof'l Conduct R. 1.4 cmt. [5] (2013). Thus, should a data breach occur that results in the unauthorized acquisition of a client's information, Rule 1.4 requires the client be notified about that breach. While a lawyer may be justified in temporarily delaying notifying a client in order to investigate the breach and determine how it occurred, to identify the specific information involved, or at the request of law enforcement, a lawyer "may not withhold information to serve the lawyer's own interest or convenience." Model Rules of Prof'l Conduct R. 1.4 cmt. [7] (2013).

Complete candor is a must. A law firm must be reasonably certain that the information provided is accurate, which can be difficult before a forensic examination is completed. A firm should endeavor to avoid any claim that the information provided in a breach communication was only partially true or misleading. Also keep in mind that how a lawyer informs the client of a mistake can be as important as what is said. Attempts to hide a mistake or even a perceived misrepresentation in a breach notification could trigger a claim that Model Rule 8.4(c) was violated. It is professional misconduct for a lawyer to "engage in conduct involving dishonesty, fraud, deceit or misrepresentation." Model Rules of Prof'l Conduct R. 8.4(c) (2013).

Rule 4.1 prohibits making false statements of material fact to third persons. Model Rules of Prof'l Conduct R. 4.1 (2013). Rule 4.3 explains that when dealing with an unrepresented person a lawyer shall not state or imply that the lawyer is disinterested and shall not provide legal advice, other than to secure counsel, if the lawyer reasonably should know that the interests of the person have a reasonable possibility of conflicting with the interests of the lawyer's client. Model Rules of Prof'l Conduct R. 4.3 (2013).

State data breach notification laws require that notice be provided to the individuals whose personal information was acquired or materially compromised and a number also require that notice be provided to third parties including credit reporting agencies and governmental officials. Some states have specific requirements to include in a breach notification, which should be carefully followed when drafting breach notifications. Because breach notifications frequently must be sent to third parties, Model Rules 4.1 and 4.3's requirements will be triggered when notices are required to be sent under state breach notification laws.

Even when no duty to report is triggered under a state's data breach notification law, a lawyer should carefully evaluate whether under his or her state ethical rules, the client should be advised of the significance of the mistake or the potential for a claim against the lawyer as a result of the data breach. The reported decisions and advisory ethics opinions that have addressed this reporting issue in other contexts are not uniform in their approach or conclusion.

For instance Colo. Bar Ass'n, Formal Op. 113 (2005), states: "The lawyer need not advise the client about whether a claim for malpractice exists, and indeed the lawyer's conflicting interest in avoiding liability makes it improper for the lawyer to do so." See also *Fitch v. McDermott, Will & Emery, LLP*, 929 N.E.2d 1167, 1184 (Ill. App. Ct. 2010) ("We similarly find no case that would require an attorney to affirmatively advise his client of his negligence and the statute of limitations for suing him"); *Expansion Pointe Properties Ltd. P'ship. v. Procopio, Cory, Hargraves & Savitch, LLP*, 61 Cal.Rptr.3d 166, 176 (Cal. Ct. App. 2007) (holding no duty to discuss "types of recovery a client may obtain in a potential malpractice action").

However, the *Restatement (Third) of the Law Governing Lawyers* § 20 cmt. C (2000), takes the position: "If the lawyer's conduct of the matter gives the client a substantial malpractice claim against the lawyer, the lawyer must disclose that to the client." Similarly, Wisconsin Ethics Opinion E-81-12 (1998), concluded: "an attorney is obligated to inform his or her client that an omission has occurred which may constitute malpractice and that the client may have a claim against him or her for such an omission."

See also *Olds v. Donnelly*, 696 A.2d 633, 643 (N.J. 1997) ("The Rules of Professional Conduct still require an attorney to notify the client that he or she may have a legal—malpractice claim even if notification is against the attorney's own interest"); *Matter of Tallon*, 447 N.Y.S. 2d. 50, 51 (N.Y. App. Div. 1982) ("An attorney has a professional duty to promptly notify his client of his failure to act and of the possible claim his client may thus have against him."); N.Y. City Bar Ass'n, Formal Op. 2015-3 (2015) ("A lawyer who discovers he has been defrauded in a manner that results in harm to other clients of the law firm, such as the loss of client funds due to an escrow account scam, must promptly notify the harmed clients.").

This should not be confused with an admission of liability. Clearly when an ethical duty to report is triggered by the unauthorized acquisition of information, a lawyer should disclose the facts and circumstances surrounding the data breach, and evaluate if there is a need to suggest to the client that "it may be advisable to consult with an independent lawyer with respect to the potential impact of the error on the client's rights or claims." Colo. Bar Ass'n, Formal Op. 113 (2005).

Conclusion

A cyber intrusion raises a series of complex and challenging issues for law firms that involve a variety of disciplines. Further complicating the problem is the myriad of ways a security incident or cyber intrusions can occur. While the best defense against a breach is a robust data-security program, being prepared when a cyber intrusion occurs is a critical consideration for law firms. A poorly handled incident response can cause reputational harm to the firm as well as the loss of clients and client trust. The steps and considerations outlined above should help lawyers and law firms to be ready when the inevitable happens.

Endnotes

1. Model Rule 1.6(c) requires lawyers to "make reasonable efforts to prevent the . . . unauthorized access to information relating to the representation of a client." MODEL RULES OF PROF'L CONDUCT R. 1.6(c) (2013). Comment 18 to Rule 1.6 lists a series of six factors to consider in assessing whether reasonable efforts were taken including the sensitivity of the information, the likelihood of disclosure if additional safeguards are not adopted, the cost and difficulty of implementing additional safeguards, the extent to which the safeguards adversely affect the lawyer's ability to represent a client, and whether the client required special security measures be taken or provided informed consent to forego measures that might otherwise be required under the rule. MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt [18] (2013).

2. *See, e.g.*, Garvy v. Seyfarth Shaw LLP, 966 N.E.2d 523 (Ill. App. Ct. 2012); *St. Simons Waterfront LLC v. Hunter, McLean, Exley & Dunn*, 746 S.E.2d 98 (Ga. 2013); RFF Family P'ship. LP v. Burns & Levinson LLP, 991 N.E.2d 1066 (Mass. 2013); *Crimson Trace Corp. v. Davis Wright Tremaine LLP*, 326 P.3d 1181 (Or. 2014); *Edwards Wildman Palmer v. Superior Court*, 180 Cal.Rptr. 3d 620 (Cal. Ct. App. 2014).

3. Forty-eight (48) states, the District of Columbia, the Virgin Islands, Puerto Rico and Guam have adopted data breach notification laws that potentially apply to data breaches involving lawyers and law firms. See State Security Breach Notification Laws, National Conference of State Legislatures, (Jan. 12,

2015), http://www.ncsl. org/research/telecommunications-and-information-technology/ security-breach-notification-laws.aspx. Currently, only Alabama and South Dakota have not enacted a data breach notification law. Id. While state data breach notification laws have many common elements, there are significant variations between them. It is critical to carefully review the law of a particular state. Generally, state data breach laws focus on unencrypted computerized data that includes personally identifying information.

While the definition of personally identifying information varies between states, frequently it is defined as a combination of a person's first name or initial and last name, coupled with one or more of the following: the person's social security number; driver's license number or other state identification number; financial account number; credit or debit account number in combination with any required security code; access code or password that would permit access to a financial account. Several states include biometric data in the definition of personal information, as well as certain types of health insurance information such as policy or subscriber numbers, or information in the person's application or claims history. Publicly available information from federal, state or local governmental records is frequently excluded from the definition of PII under these laws. Several states also encompass the compromise of paper records in their breach notification laws.