IMPORTANT NOTICE:
This Publication Has Been Superseded

See the Most Current Publication at

https://thesedonaconference.org/publication/Commentary_on_Law_Firm_Data_Security

wgs

The Sedona Conference

Commentary on Law Firm Data Security

A Project of The Sedona Conference Working Group
on Data Security and Privacy Liability (WG11)

April 2020
Public Comment Version
Submit comments by June 8, 2020,
to comments@sedonaconference.org

The Sedona Conference Commentary on Law Firm Data Security

A Project of The Sedona Conference Working Group on Data Security and Privacy Liability (WG11)

APRIL 2020 PUBLIC COMMENT VERSION

Author: The Sedona Conference

Editors-in-Chief & Steering Committee Liaisons

David Moncure Neil Riemann

Contributing Editors

Guillermo Christensen
Sheryl Falk
Michele Gossmeyer
Christopher King
Jana Landon
Robert Levy
Anthony Lowe
Gita Radhakrishna
Daniel Sutherland
Alexander White

Staff Editors

David Lumia Michael Pomarico

We thank all of our Working Group Series Annual Sponsors, whose support is essential to our ability to develop Working Group Series publications. For a listing of our sponsors, just click on the "Sponsors" navigation bar on the homepage of our website.

Preface

Welcome to the public comment version of The Sedona Conference *Commentary on Law Firm Data Security* ("*Commentary*"), a project of The Sedona Conference Working Group 11 on Data Security and Privacy Liability (WG11). This is one of a series of Working Group commentaries published by The Sedona Conference, a 501(c)(3) research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, and intellectual property rights. The mission of The Sedona Conference is to move the law forward in a reasoned and just way.

The mission of WG11 is to identify and comment on trends in data security and privacy law, in an effort to help organizations prepare for and respond to data breaches, and to assist attorneys and judicial officers in resolving questions of legal liability and damages.

The Sedona Conference acknowledges Editors-in-Chief Neil Riemann and David Moncure for their leadership and commitment to the project. We also thank contributing editors Guillermo Christensen, Sheryl Falk, Michele Gossmeyer, Christopher King, Jana Landon, Robert Levy, Anthony Lowe, Gita Radhakrishna, Daniel Sutherland, and Alexander White for their efforts. We also thank Elise Houlik for her contributions.

In addition to the drafters, this nonpartisan, consensus-based publication represents the collective effort of other members of WG11 who reviewed, commented on, and proposed edits to early drafts of the *Commentary* that were circulated for feedback from the Working Group membership. Other members provided feedback at WG11 annual and midyear meetings where drafts of the *Commentary* were the subject of the dialogue. On behalf of The Sedona Conference, I thank all of them for their contributions.

Please note that this version of the *Commentary* is open for public comment, and suggestions for improvement are welcome. Please submit comments by June 8, 2020, to comments@sedonaconference.org. The editors will review the public comments and determine what edits are appropriate for the final version.

We encourage your active engagement in the dialogue. Membership in The Sedona Conference Working Group Series is open to all. The Series includes WG11 and several other Working Groups in the areas of electronic document management and discovery, cross-border discovery and data protection laws, international data transfers, patent litigation, patent remedies and damages, and trade secrets. The Sedona Conference hopes and anticipates that the output of its Working Groups will evolve into authoritative statements of law, both as it is and as it should be. Information on membership and a description of current Working Group activities is available at https://thesedonaconference.org/wgs.

Craig Weinlein
Executive Director
The Sedona Conference
April 2020

Table of Contents

I. INTRODUCTION

Client organizations[1] undertake considerable business risk when they entrust law firms with personal, proprietary, or otherwise confidential data to facilitate effective representation. Law firms undertake similarly substantial liability and reputational risks by accepting such data.

Organizations have legal and market-based obligations to ensure their data is protected and remains secure. One of those obligations is a duty to choose outside counsel who will protect such data properly and to ensure that outside counsel do so.

Outside counsel have a duty to protect client data. The duty arises from the ethical rules applicable to attorneys; federal and state statutes and regulations; foreign laws, where applicable; the common law; and contractual obligations the firm has agreed to undertake.

Notwithstanding these complementary duties, organizations and law firms do not always approach data security the same way. Although sound risk management supports treating different enterprises differently, organizations may prefer to impose the same data security requirements on all service providers. Organizations often resist pleas from law firms to be treated differently than other service providers. Law firms provide an expensive, high-margin service. They operate under the same statutes and common law that govern other providers. They can undertake specific contractual obligations to secure organization data, just like other service providers. Firms use many of the same technologies used by organizations and the organizations' other service providers. From the organization perspective, law firms may be different than other vendors, but are they materially different for purposes of imposing data security requirements?

Law firms, on the other hand, see valid reasons for distinctive treatment. First and foremost, they are—unlike most service providers—ethically bound to maintain the confidentiality of client information, regardless of contractual obligation. Second, but related, law firms are ethically obligated to pursue the best interests of their clients, not just maximize profits. Organization demands for special, one-off handling of organization data can impair effective representation by altering the firm's workflow or requiring the use of alternative tools.

While strides have been made in understanding and addressing data security at law firms, there is consensus that more must be done to secure the sensitive data held by law firms. Tensions have grown as cybersecurity vaults to the top of the national agenda, and it has become increasingly obvious that law firms are more attractive targets for information theft, and less capable of preventing it, than previously thought.

---

[1] Some of the discussion in this *Commentary* may prove useful to individual clients as well as organizational ones, but it does not focus on individual clients or the ways the situation of an individual client may differ from that of an organizational one.

In recent years, organizations have developed a host of approaches to this problem. Law firms have struggled to keep up with the volume and variety of demands for information about their data security posture. Firms continue to differ in their understanding of data security issues and the sophistication with which they can address and have addressed them. While some large firms have embraced collaboration with their peers on data security issues, smaller firms lack readily accessible vehicles for such interfirm cooperation, and efforts to collaborate tend to focus on the mechanics of security rather than streamlining the process of addressing organization inquiries about data security.

In response to these problems, the Sedona Conference's Working Group 11 developed a brainstorming group, and then a drafting team, to identify ways that organizations and law firms should approach and address organization concerns about law firm data security. This *Commentary* is the result of that effort. The *Commentary* is intended to foster respectful and mutually beneficial dialogue between organizations and their firms regarding organization expectations and law firm capabilities. The *Commentary* seeks to move this dialogue forward by providing best practices focused on data security requirements that are meaningful considering the organization's obligation to protect the data, the type of data the organization is providing to the law firm, and the law firm's operating environment. In short, this *Commentary* intends to provide an effective road map for more efficient, effective communication to address data security issues and scenarios confronted by organizations and the law firms they engage.

While the *Commentary* may be of interest to other audiences, it is primarily directed toward two: first, to in-house counsel and an organization's technical personnel charged with ensuring that organizational service providers handle data securely; and second, to the law firm professionals and technical personnel overseeing and implementing data security at law firms.

The Sedona Conference has done prior work relating to data security, to which the reader is also referred. The most directly relevant work is *The Sedona Conference Commentary on Privacy and Information Security: Principles and Guidelines for Lawyers, Law Firms, and Other Legal Service Providers.* This Commentary was developed by Working Group 1, which focuses on Electronic Document Retention and Production. It provides guidance to law firms on the sources of their duties to protect client information and, more importantly, on the development of a risk-based data security program. Less directly relevant work that nevertheless touches on the law firm's handling of client information includes work by Working Group 2 that concern protective orders and public access to litigation documents; numerous papers developed by Working Groups 1 and 6 that address various aspects of information governance and the protection of client information in the discovery process; and this Working Group's Draft *Commentary on Privacy and Information Security in Civil Litigation.*

Note that the drafting team has not undertaken to comprehensively analyze the data security situation faced by every organizational client seeking to retain counsel. The team recognizes that some organizations work in regulated fields or have highly particularized data security needs, like those in the health care, financial, and classified contracting sectors. While most of the considerations taken up in this *Commentary* will apply to organizations in these sectors as well, they do not analyze in detail the legal requirements governing their specialized data.

Additionally, the *Commentary* does not address privacy concerns. The drafting team declined to undertake that task for a few reasons. First, ensuring the secure handling of any personal information an organization conveys to a law firm is necessary to protect privacy, but it is not sufficient. Personal information can be divulged in violation of privacy laws despite a perfectly secure environment, and security practices can also pose privacy risks. Second, privacy law is a multi-jurisdictional enterprise that imposes different requirements in different locales, and privacy laws apply differently to different types of personal information and different types of custodians. Finally, privacy issues have not, to date, led to the same proliferation of competing questionnaires and extended interactions between organizations and firms as have data security issues.

The *Commentary* that follows contains three distinct sections. In the first, the *Commentary* identifies some common criteria and protocols for assessing information security at law firms. The discussion focuses first on organization expectations for outside counsel in terms of the law firm's governance, as well as the technologies, people, and third-party service providers that make security happen. Following extended discussion of these topics, brief consideration is given to what organizations might expect from law firms with international operations and what organizations might expect of law firms in terms of cooperation with information-sharing efforts around data security.

In the second section, the *Commentary* discusses the practicalities of an organization's communications with law firms regarding data security. Nine topics are discussed, covering the entire relationship life cycle by addressing matters that should be considered before a firm is even consulted all the way through to matters that should be addressed with firms throughout the life of the relationship.

The third and final section consists of two appendices. Appendix 1 offers some model clauses regarding data security that could be used in an engagement letter. These are merely a starting point; the actual clauses should turn on the outcome of the organization's discussion with the firm. Appendix 2 offers a model questionnaire for organizations to present to law firms as a way of initiating a conversation about data security. The latter includes some sample answers and some commentary about how the actual answers should be evaluated.

No single *Commentary* will satisfy every use case for every engagement. As stated above, it is hoped that this one provides an effective road map for more efficient, effective communication to address most of the data security issues and scenarios confronted by organizations and the law firms that handle and store their data.

II. COMMON CRITERIA AND PROTOCOLS FOR ASSESSING INFORMATION SECURITY AT A LAW FIRM

The goal of this section is to develop a set of common criteria and protocols for organizations to use when assessing the cybersecurity of a law firm. Where possible, the objective of this proposed approach is to fashion a set of criteria and protocols that allows for organizations to use the same or similar types of questions to get to the same information about a law firm.

A. Organization Expectations for Outside Counsel

Organizations and firms alike have explicit or implicit expectations about how law firms should secure their information systems and the organization's data. Organizational concerns are increasingly extending beyond the protection of confidences. Organizations expect timely, effective advice and representation, as well as for the law firm to have a comprehensive security program that includes a holistic approach of managing people, processes, and technology. A security incident that prevents a firm from providing advice and representation can be as injurious to the organization as a security breach that discloses its confidences. Similarly, organizations also have an expectation that firms will provide services effectively and timely by relying on technology to achieve efficiencies. The following sections consider information security expectations organizations might reasonably have for outside counsel in the areas of governance, technology, people, use of third-party service providers, and insurance.

1. Governance

Governance, not technology, should be the starting point for an organization's assessment of a firm's security posture. This section discusses six key questions about governance that organizations should ask—and firms should expect to answer—about how they govern their information security apparatus. An added benefit of focusing on governance is that it can address not only cybersecurity systems and tools but also the culture of a law firm, which may not be adequately assessed when the spotlight is focused on technology.

1. Any lawyer should have the authority to require security measures, but which lawyers bear the ultimate responsibility for any failure of those measures?

2. Can the firm establish that it satisfies the expectations of its governing bar(s) and other general legal requirements?

3. Can the firm establish that it can satisfy the requirements of other laws, regulations, industry standards, and frameworks that apply or should be considered, given the type of information the organization is providing the firm or the magnitude of the engagement?

4. What policies and procedures does the firm have in place to implement the agreed requirements and ensure the confidentiality, integrity, and availability of the organization's information?

5. How does the firm assess and ensure that the applicable lawyers, support personnel, and service providers have the knowledge and experience necessary to successfully implement these policies and procedures, including required training of all personnel?

6. How do the organization and the firm propose to address a firm security incident that exposes the organization to potential legal liability or reputational harm?

a. Authority and Responsibility

As discussed in more detail below, lawyers are required to safeguard client confidences. In many jurisdictions, explicit or implicit duties are imposed on lawyers to develop and maintain the technological competence necessary to do that. For those reasons, every firm, regardless of size, should have one or more *lawyers* who have the authority to require the firm and other lawyers to implement information security measures. These may be a combination of General Counsel, Chief Security Officer, Managing Partner, and Practice Lead/Relationship Partner. Typically, these same lawyers bear ultimate responsibility for the failure of those measures. Organizations should reasonably expect to know the identity of the lawyers who are accountable for providing answers about their firm's information security programs.

While it may be important for organizations to understand who is making the firm's information security decisions, most firms will be relying heavily on professional information technology staff, information security staff, or service providers to provide the information necessary for the firm's lawyers to make those decisions. However, the final authority should rest with the lawyer leader(s) of the firm who carry the ethical duties noted above. Evaluation of this capability is discussed below.

b. State Bar Requirements for Protecting Client Confidences and Secrets

Once the accountable law firm personnel are identified, organizations will likely wish to explore, at varying degrees of depth, whether those lawyers understand the efforts required of them, starting with the requirements of professional ethics. Rule 1.6 of the ABA's Model Rules of Professional Conduct—adopted with minimal variation by most state bar regulators—requires as an enforceable matter of professional ethics that lawyers safeguard the confidentiality of information relating to their representations of organizations. This includes a duty to "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to" that information.[2] Comment 18 to the Rule discusses the concept of reasonable efforts in some detail. Both firms and

[2] *Rule 1.6(c): Confidentiality of Information*, AMERICAN BAR ASSOCIATION, https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information/ (last visited April 2, 2020).

organizations should expect organizations to explore how well the accountable personnel understand those requirements.[3]

Rule 1.1 of those same rules requires the lawyer to act competently in fulfilling the command of Rule 1.6. In most American jurisdictions, the official commentary on this duty of competence now makes explicit reference to the need for lawyers to keep abreast of changes in technology.[4] For that reason, it is also appropriate for organizations to explore the technological competence of the accountable lawyers and any nonlawyer technology advisors to ensure that the commands of the Rules of Professional Responsibility can be and are being met.

The American Bar Association issued Formal Opinion 477R on Securing Communication of Protected Client Information,[5] which further emphasizes the ethical duties of counsel (based on the Model Rules Referenced above) to protect communications with clients and the general obligation to ensure that an organization's information remains confidential. The Opinion cites to attorneys' general obligations of (a) technological competency (Comments to Model Rule 1.1) and (b) taking reasonable measures to prevent inadvertent or authorized disclosure of information relating to the representation (Comments to Model Rule 1.6). This Opinion also notes the responsibility of law firms to ensure that their software and infrastructure service providers have appropriate controls in place to protect the organization's data stored on a provider's systems, particularly cloud systems.

c. Other Applicable Regulations, Industry Standards, and Frameworks

The aforementioned bar guidance is codified in state law by many jurisdictions. It will be, for many firms, the only legal requirement governing law firm information security, at least as it relates to the organization's information. However, many organizations will have additional compliance concerns centered around statutes, regulations, industry standards, and frameworks relevant to their lines of business. These concerns will lead many organizations to vet firms and impose minimum security requirements on them based on security frameworks like the National Institute of Standards and Testing's (NIST) Cybersecurity Framework or the International Standards Organization's ISO 27001 standard for Information Security Management. Organizations undertaking that kind of vetting process will need to assess whether firms understand the information security requirements for service providers under such frameworks.

---

[3] *Rule 1.6 Confidentiality of Information—Comment 18*, AMERICAN BAR ASSOCIATION, https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information/comment_on_rule_1_6/ (last visited April 2, 2020).

[4] *Rule 1.1 Competence—Comment 8*, AMERICAN BAR ASSOCIATION, https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence/comment_on_rule_1_1/ (last visited April 2, 2020).

[5] AMERICAN BAR ASSOCIATION, https://www.americanbar.org/news/abanews/publications/youraba/2017/june-2017/aba-formal-opinion-477r--securing-communication-of-protected-cli/ (June 2017).

We discuss below some considerations regarding the security requirements of international organizations or offices, as well as domestic security requirements that sector-specific regulation in the United States might impose on law firms handling certain types of information.

d. Law Firm Data-Security-Related Policies and Procedures

Organizations and firms should be prepared to discuss the firm's data-security-related policies and procedures to ensure they are adequate to implement the requirements of state bar rules and any other laws identified by the analysis described above. The adequacy of such policies and procedures should be evaluated considering the size of the firm, the volume and sensitivity of the organization's data being shared, and any requirements imposed by applicable law. While a firm's small size will not excuse the absence of policies and procedures related to data security, it may be relevant to the detail with which those policies and procedures are documented and the way they are implemented. It may not make sense, for example, to ask for detailed written training materials from, or impose guest-name-badge requirements on, a firm composed of two lawyers and one assistant operating in a 1000-square-foot office. The absence of such materials or requirements in this context does not mean that the small firm is insecure. Indeed, depending very much on the circumstances, a larger firm might be more vulnerable due to size, systems budget, and complexity.

e. Knowledge and Experience

Organizations will want to explore the knowledge and experience of the firm personnel who will be accessing and protecting their data. While the accountable lawyers should understand the issues of concern at some level, organizations should not ordinarily expect the accountable lawyers themselves to have technical security knowledge. They should expect instead that a firm can demonstrate that it has the professional staff who have that knowledge and experience. Firms without in-house information technology and information security staff should be able to demonstrate the necessary knowledge and experience via vetted service providers.

f. Incidents and Breaches

Organizations and law firms should strive to reach agreement within the scope of their engagement as to the firm's obligation in the event of a security incident or breach that threatens to or does result in the misuse or theft of the organization's data. Organizations are increasingly likely to demand that law firms go beyond any state or federal laws mandating disclosure of data breaches, particularly since many existing data breach laws only address personal data and do not address disclosure or compromises of types of nonpersonal data that organizations consider sensitive.

Firms should plan notification protocols in advance: Will the firm notify any third parties, such as state Attorneys General, of the breach? Will it notify the organization itself? Who will bear the cost

of any necessary breach notification? Will the firm defend or indemnify the organization against claims arising because the firm suffered a breach and the organization's information was disclosed?[6]

During due diligence, organizations may request that law firms provide data on previous incidents or breaches as a means of evaluating the firm's information security program. In any negotiation on the exchange of security information like this, the focus must be on how the data would help engage the parties in a discussion regarding resources and risk evaluation. Each party needs to understand the duty associated with handling the other party's data and should limit the volume to only that which is necessary.

There are a variety of reasons for such a request for security details. Organizations may wish to use the descriptions of incident handling and breach response to evaluate the maturity of the organization or assess whether resources are directed appropriately. A lack of investment in security resources could be an important risk factor to the organization. They may use this data to better understand if the law firm has been a target in the recent past. Some organizations may wish to have ongoing updates regarding incidents or breaches even after the relationship has been formalized to continuously evaluate the law firm according to their own level of risk comfort.

Note that incident details will be of less practical value in evaluating a law firm's maturity than breach details. An incident includes every attempted intrusion or mere chance of data breach. All law firms will address incidents, and often these incidents pose little to no risk of harm, thanks to existing controls or closer analysis of the situation in the context of the prevailing regulations. If a firm states that it experiences no incidents, an organization may want to question the firm's awareness of security risks. However, if a firm provides full details of all incidents, the organization may get a false impression about the firm's ability to keep data secure. The organization may conflate mere incidents with confirmed breaches or may struggle to identify and evaluate true causes of concern due to the sheer quantity of incidents. Organizations should find more value in examining confirmed breaches and the details of how the firm responded to those breaches.

In providing information about incidents and breaches to organizations,[7] law firms must contemplate the risks created by sharing this data. A full description of a breach may include details of the personal or confidential information that was disclosed; however, the law firm could create a new instance of a data breach by providing such details to an organization. Any information shared should be carefully evaluated against relevant data protection laws, and regulations and should be presented in summary fashion or, if necessary, in more detail but with all legally protected

---

[6] Some firms take the position that indemnification imperils their ability to vigorously represent clients. Discussion of this topic is beyond the scope of this paper.

[7] Considerations may differ when firms contemplate whether to share information with the government or with Information Sharing and Analysis Centers or Organizations. Some sharing mechanisms, notably those set forth in the Cybersecurity Information Sharing Act, 6 U.S.C. § 1501 *et seq.,* contain protections from liability and mechanisms designed to protect against the inadvertent redisclosure of personal information. Organizational inquiries regarding firms' information sharing practices are discussed briefly in Section I.C.

information appropriately redacted, anonymized, or pseudonymized before sharing. The law firm should focus on sharing details regarding its breach response process, including its ability to effectively remedy the cause of the breach, instead of sharing specific and confidential details.

Above all, law firms should ensure they maintain their own privacy and confidentiality commitments. Sharing data with client organizations should only be done according to an established procedure that includes a secure method of transfer and appropriate administrative controls, such as nondisclosure agreements. Organizations should identify the purposes behind such a request, to ensure that the details they receive are only those relevant to meeting their goals.

Firms should clearly plan their protocols for advising organizations in the event of breaches. Organizations will want to learn early of any issues that might impact their data or interests. Firms that withhold early notification run the significant risk of alienating relationships, even if the strict letter of the law did not require disclosure. Many larger organizations will have substantial expertise inhouse that can provide additional resources to support a law firm facing an attack or breach situation. Law firms are well served to consult in advance of any incident with leading information security service providers as well as outside counsel with expertise in this field, particularly if the firm does not have internal expertise. Firms should run annual tabletop exercises and include a list of key contacts with government, service providers, and outside counsel who can advise in the event of a breach.

2. Technology and Infrastructure

Interactions between law firms and organizations on the issue of cybersecurity often revolve around organizational expectations of the firm's technology and infrastructure used to store and process the organization's data. Technology can be easier for an outside party to evaluate and audit than data governance, but the latter is often more important. Most security vulnerabilities and their associated risks tend to be caused by business practices and the way human beings interact with information systems and data, which cannot be mitigated through technology alone. For this reason, organizations may want to focus more on the human element and less on technology solutions in isolation. The approach suggested in this section is to focus any assessment of technology on those aspects that can most reliably mitigate human errors or malicious behavior.

The elements of technology impacting cybersecurity that are likely to be of key concern to organizations break down into several areas, all of them primarily concerned with: (1) the protection of the organization's data (confidentiality and integrity), and (2) ensuring that the firm can detect, respond, and recover from any attacks on its systems (availability). These two areas of concern can arise in many technology areas that organizations should consider assessing. The priority/ranking will vary depending on the types of data involved and environment in which it is handled.

a. Authentication and Access Controls

Most serious breaches and compromises of information systems and data typically involve unauthorized access into a firm's network, email system, or other information services. Current best practices

are to ensure that access to a firm's information systems should be protected by additional measures beyond a login and password. Multifactor approvals are a commonly used security approach, but other developments in the authentication area that rely on more complex methods to authenticate a user are increasingly available.

In addition to authentication, organizations should examine the way a firm regulates levels of access/privileges on network accounts. A guiding principle should be to provide the lowest level of privilege needed for a particular user, a concept known as "least privilege" or "need to know." Additionally, notification systems and split passwords are becoming the standard for empowering administrative personnel with powerful IDs.

Given the myriad issues with insider threats and disgruntled employees, organizations should expect that firms will integrate governance of user accounts with human resources (HR) and physical security processes to ensure that employees who depart or are terminated are removed from access. The existence of multiple generic administrative level accounts used by Information Technology (IT) personnel or other administrative functions should also be audited.

b. Mobile Devices

The sophistication and large data storage capabilities of mobile devices (smartphones, tablets, laptops) present a particularly challenging and growing risk to a firm's cybersecurity. Organizations should consider examining the degree to which a firm incorporates governance and technical measures focused on the security of mobile devices. These may include the use of mobile-device management applications to limit access to information and to provide means to remotely erase or lock devices that may be lost or stolen. Additionally, organizations may seek to understand the scope of information that a firm may provide through its mobile devices. Organizations will increasingly expect that firms will curtail or prohibit the use of certain types of mobile devices such as USB drives or portable hard drives, which pose a higher risk if they are misplaced, stolen, or used to exfiltrate large amounts of data.

c. Encryption

As more regulators consider the use of encryption to enhance data privacy or protect export-controlled technology or information, legal industry standards have developed to expect at-rest and in-motion/in-transit encryption, particularly regarding internal firm data. The capability to secure communications between organizations and firms will also increasingly be viewed as necessary, and some organizations are mandating encryption at the transport level (TLS) between the lawyer and organization domains (or at the very least the use of opportunistic TLS encryption when both sides use encryption tools). For organizations with particularly sensitive matters or those involving risks of surveillance by nation states, more secure communications capabilities such as those offered by applications designed for point-to-point encryption may be required.

d. Backup and Restore Capabilities

The resiliency of a law firm's network is of considerable interest to organizations, something that has been made clearer in the aftermath of recent attacks aimed at destroying access to systems and data. Organizations will be expected to focus on the extent to which a firm has the proven and tested capability to restore systems, whether from an attack, a power outage, or another natural or man-made emergency. Organizations may expect firms not only to have such plans in place, but to be able to demonstrate that they test these on a regular basis. This is one area where extensive industry practices exist, and organizations can rely on these best practices to audit a firm, including ensuring backups are stored in different locations.

e. Cloud-Based Storage and Services

Any communication system connecting two entities raises the potential for compromise and the dissemination of malware or other attacks. The primary concern most organizations have regarding law firm use of cloud services revolves around this cybersecurity issue and its potential impact on the organization's confidential information, so organizations may need to review whether a firm has in place methodologies or protocols for addressing the risks posed by these systems. Some organizations with particularized needs because of their work with export-controlled information may also have requirements to ensure that such information is segregated and is not being exported due to being hosted on a cloud service or being accessible to unauthorized persons. A firm should expect to be asked for an inventory of cloud-based storage and services and for assurances that the firm has undertaken diligence of these services and appropriate contract provisions to safeguard confidential information.

f. eDiscovery Tools and Databases

The proliferation of eDiscovery applications used in litigation or databases for the review of confidential deal information risks exposing massive amounts of the organization's data, sometimes involving the most sensitive aspects of an organization's operation. Firms involved in litigation, acquisitions, or other work involving the review of organizational or opposing party information may be expected to factor in the security of these systems, but this may pose challenges when these systems are put in place by the organization versus being maintained by third parties. To the extent the law firm is involved in the vetting and selection of these systems, it should put in place a process to ensure that the litigation support department—typically in charge of these resources—adequately reviews cybersecurity risks and vulnerabilities, including periodically reviewing and testing service provider controls as appropriate.

g. Billing Software/E-Billing Connections

As with cloud-based services, the extent to which privileged or sensitive information is shared by the law firm with e-billing service providers will be an area of concern for organizations, particularly if the system is a cloud-based application.

h. Server and Infrastructure Protection

The protection of physical and electronic access to electronic systems should be considered a priority by organizations. Law firms should expect to be queried regarding their process to ensure physical security of server rooms and other sensitive equipment as well as system controls. The server rooms and sensitive equipment should be segregated, protected by industry-standard endpoint protection, and access limited to authorized users, with logging of access. However, firms should not be expected to provide detailed information regarding these measures, as doing so will put these measures at risk of unauthorized disclosure. Third-party certification can be effective in resolving an organization's concerns regarding the sufficiency of these controls and protections.

i. Auditing and Network Monitoring

Organizations may increasingly expect that law firms will have in place more extensive network security tools to permit in-depth monitoring of activity, including indications of large-scale exfiltration of data or efforts to conduct reconnaissance inside the network. Such capabilities will need to be integrated into the firm's operations to ensure that information, when received, is acted upon timely. Organizations also are likely to be concerned about logging and preservation of network activity, which will help identify the nature and extent of any compromise post-incident. These logs should also be a part of retention policies to minimize the complexity of managing old data.

j. Firewalls, Antivirus Software, and Malware Protection Tools

Organizations will look for law firms to have in place the standard suite of firewall, antivirus, and malware security tools. Organizations may press firms to have regular reviews and updates to the technology as such technologies advance. A key challenge for firms and organizations will be finding consensus on the utility of these evolving technologies relative to the cost and complexity to manage.

k. Records Retention

Law firms should implement an appropriate records retention policy that considers both legally required retention as well as best practices related to the disposition of data. Firms should work with organizations to clarify how long the organization's data will be retained following the completion of a matter or the end of the relationship. This should be driven by a retention policy that is consistently followed. Firms that fail to appropriately dispose of data increase their vulnerability to breaches and may face a difficult defensibility argument if the firm's failure to timely dispose of information prejudiced the organization in the event of a breach.

3. People

One of the main areas of concern for most organizations is and will continue to be managing the cybersecurity risks posed by a firm's lawyers and staff. These risks break down into several main areas, each with unique challenges for mitigation.

a. Malicious Insider Threats

Malicious insiders who steal or destroy law firm systems are a difficult vulnerability to mitigate. Organizations may increasingly expect that firms of a certain scale, or those working with particularly sensitive information such as national security or critical infrastructure, have in place some type of insider threat program. Implementing these programs is challenging even for larger organizations with extensive security resources and requires close integration of management, HR, IT, and security. Such programs also have resource implications involving the education of staff and lawyers and putting in place more focused monitoring of employees. For example, a firm may require lawyers and staff to undergo regular background checks and to self-disclose life events that may be early indicators of heightened risk. This needs to be considered in conjunction with jurisdictional regulations and appropriate handling of this data.

b. Lack of Technical Competence

Organizations will assess how well a law firm manages the human factor in cybersecurity by focusing on the firm's policies and governance, the way the firm educates and trains its employees, and how it implements remedial measures. Taken together, these factors likely will be perceived by organizations as equating to a security culture rating for the firm. Organizations may want to look at these issues through several prisms:

- Education—focused on broader concepts and expectations around information security.
- Training—focused on mandatory training for all computer users, including competency or testing assessments built into the training modules; competency on systems and software; and familiarity with risks, vulnerabilities, and threats.
- Governance—standards the firm sets for lawyers and staff through policies and expectations and how these standards are enforced through discipline.

Organizations should be particularly mindful that law firm culture often is markedly different than those of many organizations, public or private. Many firm partners function effectively as their own CEO, leading to more prevalent risks from behaviors that are not in compliance with firm policies but are not addressed by the firm's professional staff, who may perceive they lack the standing or influence to challenge lawyer, and particularly partner, behavior.

It is also particularly important to ensure that law firms have committed to training requirements for all personnel that includes intra-course tests to determine whether the participants comprehended the learning offered in the course. One of the weaker links of a law firm security system can be the vulnerability of partners who are focused on billable work and less attentive to security issues. Effective phishing and malware strategies focus on these vulnerabilities by designing campaigns intended to encourage partners to "fall for" malicious emails.

c. Service Providers

Organizations will want to look at the law firm's selection and contracting processes for service providers that provide legal services for the organization. This is particularly true when firm service providers will receive the organization's sensitive data, such as a cloud-based service for file transfer or document management. Best-practice checklists and frameworks have been published by other organizations and may be useful resources to identify detailed topics of discussion between organizations and firms.[8]

Organizations likely will be interested in how firms selected any service providers who might handle the organization's data. Two key questions organizations may have about a firm's provider selection process are: (1) Does the firm use a selection process that will provide the firm with a sound understanding of a provider's service delivery model; and (2) Does the firm use a selection process that will select providers who facilitate, rather than undermine, the firm's own assurances to organizations. It is important for organizations to approach these inquiries with the right frame of mind, recognizing that for many or most law firms, deployment of service providers is as likely to improve security as to undermine it.

Fundamentally, if a firm selects a service provider on behalf of an organization or otherwise uses a provider's services for law firm systems, the law firm has an ethical duty to ensure that the provider is appropriately addressing cybersecurity issues, particularly if the provider's systems hold data that if released or compromised would prejudice the organization. Where firm service providers may gain access to the organization's data or to a firm's critical information systems, organizations have an interest in the firm's vetting of those providers and their privacy and security posture.

4. Insurance Coverage

Organizations have an interest in understanding how firms have chosen to transfer or share the risk of a cybersecurity incident. These questions and their answers can indicate the law firm's ability to make the organization whole if the latter is harmed by such an incident. Details about a firm's insurance coverage can indicate a level of cybersecurity maturity. The insurance company may have performed an assessment of a firm's cybersecurity practices or provided guidance on appropriate risk management actions.

A firm may have a variety of insurance coverages to protect against risks, such as damage to property or malpractice lawsuits. The following questions may provide an organization with insight about cybersecurity issues. Since the insurance market for cybersecurity risks is far from standardized, and

---

[8] The Vendor Contracting Project of the American Bar Association's Cybersecurity Legal Task Force published a Cybersecurity Checklist that addresses vendor selection and contracting, *available at* https://www.americanbar.org/content/dam/aba/images/law_national_security/Cybersecurity%20Task%20Force%20Vendor%20Contracting%20Checklist%20v%201%2010-17-2016%20cmb%20edits%20clean.pdf (Oct. 17, 2016). The Draft Version 1.1 of NIST's Cybersecurity Framework includes discussion on supplier selection, contracting, and oversight, *available at* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (April 16, 2018).

many insurers create their own, custom coverage forms, the organization and firm may wish to review, in high-level terms, the scope of the coverage and the organization's protection under it.

- Does the law firm use insurance to supplement information security?
- If so, does the insurance coverage provide:
    - First-Party Coverage: to reimburse the firm for costs that occur when a breach is discovered? These costs may arise from hiring professional investigators and advisors, notifying affected individuals and providing credit monitoring, and restoring the firm's operations so they can continue to serve organizations.
    - Third-Party Coverage: to reimburse third parties, such as the organization itself, for harm that results from a breach? This coverage may include the cost to defend the firm against lawsuits and cover regulatory penalties.

These coverage details will indicate to the organization that a cybersecurity incident is not necessarily an existential or solvency risk to the law firm.

Firms should indicate if organizations will be named as an additional insured, which provides an organization with an added benefit by making their coverage claims easier to verify. Organizations should consider requesting a copy of the additional insured endorsement. Firms should explain how the policy will address incidents that occur before the effective date of the coverage, since cybersecurity incidents can be ongoing or can take time to discover.

Additional questions regarding audits and security practices:

- Did the insurer perform an audit or other assessment as part of the application or underwriting, and may the organization access or receive a copy of their report?
- Does the insurance policy require the firm to meet minimum security practices, or include an exclusion for the firm's failure to follow such minimum practices? If so, what procedures and risk controls are set forth in the application or policy?
- Does the firm perform audits directed by the insurance broker to assess risks, and may the organization access or receive a copy of the latest version?

Additional details (if desired):

- What coverage and limits does the insurance provide for customer data?
- What deductible, if any, could an organization have to pay for a claim?
- Does the policy cover losses caused by third-party vendors of the law firm?

- Does the policy cover ransomware and/or cyber extortion?
- Does the policy cover misdirected email or other "Business Email Compromises"?
- What is the claims process? Do additional insureds control their rights to recovery?
- Is the policy a duty-to-defend or duty-to-reimburse-defense-costs policy? Do defense costs exhaust the policy's limit? What are the provisions regarding the selection of defense counsel?
- Will the law firm provide a certificate of insurance at the outset of the engagement and annually?
- Does the law firm need or have international coverage or separate social engineering attack coverage?

B. Outside Counsel with International Operations

Due to modern technological and regulatory advancements, many organizations now conduct some level of operations in an international jurisdiction other than the one in which they are domiciled. Likewise, law firms may represent organizations in international matters and have worldwide offices as part of a global practice, or they may simply employ a third-party service provider based in another country who has access to the firm's data.

Firms should provide organizations with details regarding the parties with whom, and locations where, their data will be shared. Organizations should consider cross-border security issues in the context of both: (1) the firm's ability to comply with jurisdictional requirements, and (2) what elements of risk will be introduced if the organization's data travels across borders.

Some jurisdictions may have unique information security requirements, along with unique mandates relating to an individual's ability to access data about oneself. While it is beyond the scope of this document to list all possibilities, of note in this regard is the European Union (EU) General Data Protection Regulation (GDPR), which organizations must follow if they collect or process information relating to residents of the EU. Organizations whose data includes information on EU residents should request details on how firms will ensure their practices comply with GDPR requirements.

Governments vary in their abilities and willingness to abrogate confidentiality and compel the disclosure of data held by private parties. Organizations must be cognizant of the fact that data stored in or passing through a country other than their own may become subject to that foreign jurisdiction's laws and enforcement mechanisms, and they should inquire whether firms with international offices have considered local-law limitations on the use of encryption or VPNs and rule-of-law challenges posed by less-developed search-and-seizure frameworks in the countries where they use or store

client information—paying particular attention to any policies the firm has in place regarding travel across borders with confidential information.

Organizations should ensure they understand any outside parties in international jurisdictions with whom law firms will share the organization's data, such as local contract or agency attorneys. For example, firms that rely extensively on contract attorneys for patent work or document review in local jurisdictions should have a more developed process to assess the risks of sharing information and work product with these service providers. Organizations should request details on this risk assessment if this situation applies to their data.

C. Efforts to Coordinate Among Industries and to Set Common Standards

Organizations may also have questions about law firm efforts to coordinate among themselves. Mature firms should consider participating in Information Sharing and Analysis Centers (ISAC) or Organizations (ISAO) or other risk-focused groups that disseminate the most recent intelligence about threats, incidents, and mitigating steps the firm can take to prevent or reduce risk. Organizations should request details on the firm's participation in such information sharing groups and other cybersecurity and data protection trade organizations.

The Cybersecurity and Infrastructure Security Agency (CISA) has engaged in outreach, including to law firms, designed to provide resources and guidance on trends and tools and to serve as a clearinghouse for information sharing. Under the Cybersecurity Information Sharing Act of 2015, private entities, including law firms, receive antitrust protection if they participate in information sharing activities. Further, the provision of cyber threat indicators and defensive measures to the government does not waive an otherwise applicable privilege or legal protection. Finally, properly designated shared information remains proprietary and exempt from scrutiny under freedom of information acts. CISA and the Department of Justice regularly hold joint conferences on cybersecurity issues, including conferences for lawyers that focus on the unique exposures facing the legal industry.

The FBI also provides extensive support to the private sector, including law firms, on cybersecurity issues. Law firms should reach out to their local FBI and Secret Service field offices to develop a relationship with these law enforcement personnel who can serve as a resource as well as a key contact in the event of a cybersecurity incident.

III. CONSIDERATIONS FOR HOW AN ORGANIZATION SHOULD COMMUNICATE WITH OUTSIDE COUNSEL ABOUT THE SECURITY OF THE ORGANIZATION'S DATA

This section will discuss practical steps regarding communications about data security between an organization and its law firm(s), including how to begin such discussions and how to maintain an ongoing dialogue about data security. No single approach is appropriate for every organization. Factors to consider include: the nature of the organization's business, the degree of regulation of data security and privacy applicable to the organization's business or information, the nature of the work done for the organization by a firm, the type of information received from or created for that organization that the law firm will retain, and issues of organizational culture.

A. How Outside Counsel's Data Security Becomes Part of the Process at the Organization

The best way to encourage stakeholders at the organization to focus on law firm data security will depend upon the structure and culture of the organization. In most instances, it is likely that the in-house counsel function will take a leadership role. In most instances, outside counsel is engaged through the organization's legal function, and the in-house counsel's office acts as gatekeeper. In organizations where outside counsel hiring is decentralized, or delegated to a nonlegal function, in-house counsel's role may be one of educating the gatekeepers about the importance of data security and providing them the tools with which to protect organization data. In all organizations, the people performing the IT function and responsible for data security should be consulted. For example, suppose responsibility for the selection of outside counsel to defend insurance coverage litigation is delegated to the leadership of the underwriting function. In those circumstances, the office of the chief legal officer, working in conjunction with the organization's IT security personnel, might create information security standards with which outside counsel should comply, provide those standards to the underwriting function leadership, and then provide training to that leadership about the data security issues behind the standards and best practices for their implementation.

B. When to Engage Outside Counsel about Its Data Security Practices

In theory, outside counsel's data security capabilities should be thoroughly evaluated and approved *before* outside counsel is engaged. Where the law firm regularly does work for the organization, or is part of an outside counsel panel, data security vetting can readily be implemented before outside counsel is engaged. However, there will be many instances due to a matter of urgency in which the organization must engage counsel who is not on a panel or with whom the organization has not previously worked. Examples of such an urgent situation include litigation in an unfamiliar jurisdiction or requiring specialized expertise, government or internal investigations, and certain types of transactions. In those instances, organizations may address law firm data security at a high level during the initial engagement phase and follow up with a more detailed process as time permits. Such basic information might include the law firm's data security policy and information about the law firm's cybersecurity insurance coverage.

Alternatively, or in addition, organizations can mitigate risk by disclosing the organization's data to the law firm via a secure site already vetted for data security and controlled by the organization. For example, suppose an organization is sued in a preliminary injunction action in a rural state court and needs to retain counsel immediately. The case involves trade secrets, including the secret formula for the organization's largest selling product. The best lawyer for the matter is a solo practitioner with a very basic computer setup who relies upon a local cloud storage provider for most data storage. The organization does not have time to investigate the data security practices of either the solo practitioner or the cloud service provider before substantial work must be done. Instead of transmitting highly sensitive documents to outside counsel, the organization could instead use a third-party hosting platform maintained by a tier-one provider whose data security practices previously have been investigated rigorously by the organization.

C. Who Engages Outside Counsel about Its Data Security Practices

Who at the organization engages in the conversation with outside counsel about law firm data security will depend on a variety of factors. In some instances, in-house counsel leads the conversation. If a specific business unit is responsible for the law firm relationship, the conversation might be led by the business unit. For example, where engagement of outside counsel is managed by the procurement department, then the procurement department may take the lead. Some organizations look to their IT function to manage law firm data security. Regardless who takes the lead in the conversation, it is advisable for the leader to get input from each stakeholder within the organization so that their needs are met. In larger organizations, it may be beneficial and efficient to form interdisciplinary teams to manage communications with counsel. For example, some larger or more heavily regulated organizations have established formal information risk management, data security, or cybersecurity functions.

Consideration should be given to segmenting outside counsel into groups by the nature and volume of the organization's information shared with each group of law firms. For example, consider an organization in the health care services business. It uses three regional law firms in Group A to handle disputes with patients and medical insurance providers. It uses five law firms in Group B to handle its commercial real estate needs. The organization's procurement department engages the law firms in Group B for the real estate matters. The information provided to the law firms in Group A is subject to far more extensive and detailed regulation than the information provided to the law firms in Group B. In these circumstances, it is advisable for in-house counsel with knowledge of the applicable data privacy regulations to take the lead on communications with law firm Group A, whereas it may be reasonable to rely upon the procurement function to take the lead on communications with law firm Group B, with appropriate input from the legal and IT functions.

Where communications are handled by the procurement or IT functions, they will sometimes use the same questionnaires and communications for law firms as they do for other types of vendors.[9]

---

[9] The term "vendor" is used here to refer broadly to providers of goods and services to the organization and not narrowly to providers of services to the legal function.

In-house counsel may wish to review those communications. Law firms are different from other vendors in many respects, and consideration should be given to whether the same information should be sought from both outside counsel and other, non-law-firm vendors. As set out elsewhere in this paper, there are numerous data security considerations that are unique to law firms, and there are data security issues that are important to non-law-firm providers but do not apply to law firms. Corporate counsel should review "one size fits all" vendor questionnaires that are sent to law firm and non-law-firm vendors to confirm that all important issues are addressed. Deference should be given to questions from the model questionnaire set out in Appendix 2 of this *Commentary*.

The organization should also consider the impact of privacy rules that limit to whom within the organization particular information may be disclosed. Such privacy rules may affect who communicates with a law firm about the information subject to such rules.

D. The Organization's Point of Communication at Outside Counsel

The organization also should consider with whom at the law firm they communicate about data security issues. Law firms follow a variety of approaches to managing their data security function. In some instances, communications are handled at the law firm by the relationship partner. Sometimes the law firm will designate someone within the IT organization to respond. In other instances, law firms that have an in-house "general counsel" function may designate lawyers from the general counsel function to respond. Some larger law firms may designate a multidisciplinary team to respond.

Should in-house counsel leave it to the law firm to decide who should handle communications? Not necessarily. In-house counsel has an interest in making sure that it is getting the information it needs and that the information appears to be complete and reliable. In making that determination, in-house counsel should consider the nature and volume of the organization's information shared with counsel. Law firms should welcome a dialogue with their existing and prospective clients about how best to collaborate on securing collective data.

E. Data Security Questionnaires

1. Questionnaires and Their Alternatives

Data security questionnaires are used widely by organizations to create the foundation for discussions with outside counsel about the law firm's data security. While this *Commentary* advocates for the use of the Model Questionnaire in Appendix 2, there may be other ways to gather information. For example, in some situations, such as urgent matters described above, in-person or short "email interviews" may be conducted in lieu of a lengthier questionnaire process.

2. Documentation Requests

Each organization should consider which documents the law firm should be required to disclose. Which documents to request will depend upon nature of the organization's business, the nature of

the work performed by the law firm, and the types of documents and information provided by the organization to the law firm. At a minimum, the organization should expect the law firm to be able to make available for review the firm's data security policy, a statement of its cybersecurity insurance coverage, and validation of the security assessments the firm has performed with any subcontractors that will hold the organization's data and information.[10] It is in the best interests of both the organization and the law firm to share information by screen share rather than requiring the law firm to send copies of data security documentation to the organization. Keeping the law firm's information secure within the firm's own systems helps maintain the confidentiality of the firm's data security practices, which ultimately benefits both the firm and the organization whose information the firm holds. Moreover, an organization may not want to assume additional risk to itself by retaining sensitive data security documents of other organizations.[11]

3. Questionnaire Format

A wide variety of practices are currently used for presenting questionnaires to law firms. Some larger organizations use web-based forms to collect the information and automatically populate database tools that synthesize the information on the organization's end. Other organizations use forms created in a word processing program such as Microsoft Word or Google Docs or spreadsheet programs such as Microsoft Excel.[12] Still other organizations use third-party hosting systems or tools to elicit information.[13] Whichever approach the organization decides to use, the form needs to be sufficiently flexible to permit the law firm to make needed disclosures. Organizations should recognize that law firm network architecture and security processes may vary widely. If the organization decides to use a heavily formatted form to present its questionnaire—for the valid purpose of receiving uniformly formatted responses—the organization should also provide a space for the law firm to provide additional information in free-text form. Organizations also should recognize that law firms will often need to obtain input from multiple people within the firm to respond to the different

---

[10] An organization's first instinct might be to also request the law firm's data breach response plan. Each organization should consider whether such a request is in its best interest. Data breach response plans can reveal confidential aspects of the law firm's data security architecture. It is in all parties' interests to minimize the dissemination of such key information. Therefore, organizations should strongly consider relying upon the law firm's representation that it has a data breach response plan.

[11] If the organization decides to obtain copies of the law firm's data security documentation, it should return or securely destroy the materials promptly upon completion of its review to minimize the risk of unintended disclosure of sensitive law firm information that could jeopardize the security of the organization's own information in the hands of the firm. Law firms may include confidentiality clauses in their nondisclosure agreements (NDAs) to address proper handling, including retention and destruction of any data collected in relation to audits/assessments.

[12] Macro-enabled forms, such as spreadsheets, are often blocked by law firm security systems as a risk-control measure. The organization should consider providing flexibility to disable macros to reduce security risk to both parties' systems.

[13] If using a third-party system or tool, the organization should carefully vet the vendor and only use vendors with which the organization would trust its own information. Law firms may include "right to audit" clauses if an organization chooses to use a third party to store assessment data.

questions. Therefore, the organization should permit the law firm to export the questionnaire into a format the firm can work on "in draft."

4. Processing Questionnaire Responses and Documentation

The organization should have a reliable process for reviewing questionnaires and following up. The organization should involve personnel with sufficient technical expertise to identify issues that are significant to the organization. Smaller organizations that do not have in-house security functions should consider engaging an outside IT consultant to assist in evaluating the responses. If the questionnaire is worded with care and precision, insufficient answers (e.g. incomplete or nonresponsive replies) should be obvious on their face. Organizations should consider documenting both their review process and the conclusions reached at the end of the process. Organizations should be entitled to accept their outside counsels' responses as accurate. The attorney-client relationship is governed by stringent ethical rules not found in most other businesses, including enhanced obligations of disclosure and candor. In addition, outside counsel have strong incentives to preserve their good reputations.

5. Addressing Unsatisfactory Responses

If an answer from the law firm does not satisfy the organization's requirements, the organization should initiate a dialogue with outside counsel to gain a more detailed understanding of counsel's data security processes and practices. The organization should request additional information about the responses of concern. Sometimes counsel's response may be based upon a misunderstanding. The organization may determine that counsel has security processes and practices that mitigate the risks indicated by the answers of concern. Dialogue will also inform the organization's understanding of the materiality of the deficiency and may suggest alternatives to protect organization data. The organization should consider requiring outside counsel to alter its data security practices only in the case of material deficiencies that threaten information of significant sensitivity.

F. Frequency of Review

The frequency with which the organization reviews outside counsel's data security practices should depend upon several factors, including: the nature of the organization's business, the degree of regulation applicable to information shared with counsel, and the nature of the organizational documents and information provided to the law firm. Generally, the more extensive and sensitive the information provided, the more frequent the review should be. Organizations should recognize that reviews consume organizational resources. It is appropriate for organizations to balance the benefit of more frequent reviews against the cost of internal resources required to conduct and follow up on the review. Organizations also should recognize that these reviews impose burdens upon law firms that increase the firm's cost of doing business. Organizations and law firms might consider a hybrid approach under which the organization does a comprehensive review every three to five years, with partial updates annually between full reviews. There may be a few questions from the Model Questionnaire that the organization wants to address annually with its law firm(s).

G. Audit Requests

Audits of a law firm's data security practices can provide additional protections to an organization. Audits can also provide advantages to law firms. Law firms that take security seriously may see the audit process as an opportunity to collaborate closely and build relationships with an organization that is an established or prospective client.[14] But audit requirements should not be imposed by organizations reflexively. Organizations should first consider the goal of the audit and ask whether the organization's goals might be achieved in a different and less expensive way. For example, if the goal of the audit is to test data breach response processes, would a request for evidence of a tabletop exercise be more effective?

Organizations also should consider limiting the audit to the portions of the law firm's activities that involve the organization's most sensitive information. For example, if the organization only transacts business with a law firm by email or secure file transfer, it may be unnecessary to audit the law firm's website or application development process. If the audit is conducted by the law firm itself, organizations should consider how much value the audit provides. Third-party audits are of greater value to the law firm and the organization but may entail considerable cost. Ultimately, organizations and law firms should work together to create a certification program that will enable firms to satisfy data security requirements for multiple institutional clients, without the need for costly audits.

H. Privilege and the Organization's Communications with Outside Counsel

Ordinarily, the attorney-client privilege covers confidential communications between an attorney and a client with respect to obtaining legal advice from the attorney.[15] There is an issue as to whether communications about the law firm's data security practices are for the purposes of legal advice that the firm will give to the organization. It is likely to be argued that the information relates to nonlegal, technical, and business advice. A party opposing application of the privilege may also argue that the law firm is not a disinterested counselor in that the firm is seeking to be engaged to represent the organization and therefore cannot give impartial, disinterested advice as to the adequacy of its own data security practices. Whether communications between the law firm and the organization will be considered privileged will depend on the facts and circumstances applicable to each specific communication. Therefore, the organization may want to approach its communications with the law firm, including due diligence, with the knowledge that the communications may not be privileged and manage its communications accordingly.

---

[14] Providing a law firm with opportunities to discuss its client's data security needs may enhance the law firm's development of more secure solutions, which benefits both the organization and the law firm.

[15] *See* United States v. Upjohn, 449 U.S. 383, 390 (1981) ("[T]he privilege exists to protect not only the giving of professional advice to those who can act on it but also the giving of information to the lawyer to enable him to give sound and informed advice.").

I. Outside Counsel Data Security and the Engagement Letter

An organization should include in its engagement letter with outside counsel the data security requirements that will apply to the law firm. Data security requirements should address issues both during the engagement and after the engagement's conclusion. Model clauses to include in the engagement letter are provided in Appendix 1 to this paper.

APPENDIX 1—MODEL CLAUSES FOR AN ENGAGEMENT LETTER

INFORMATION SECURITY GUIDANCE ADDENDUM TO RETAINED COUNSEL AGREEMENT

This Information Security Addendum is incorporated, effective _____, 20__, into the Retained Counsel Agreement dated (the "Agreement") [INSERT DATE] between [INSERT FIRM NAME] ("Retained Counsel") and [INSERT ORGANIZATION NAME] ("Organization"). Guidance will be updated as necessary to reflect changing technology and new security threats. In addition to the terms set forth in the Agreement, Retained Counsel agrees to the following provisions:

1) Retained Counsel has and will maintain and document a comprehensive Information Security Program that complies with all applicable laws and regulations and is reasonably designed to identify, protect against, detect, respond to, and recover from threats to nonpublic information obtained by or provided to Retained Counsel that was created, compiled, modified, or received by Organization or its agents, whether that information belongs to Organization or to a third party ("Organization Information"), when that information is created or collected, in transit, being processed, at rest in storage, or destroyed.

2) Retained Counsel will use Organization Information only for the purposes for which Organization provides it, as described in the Agreement. Retained Counsel will not distribute, share, or provide Organization Information to any other party, except as authorized in connection with the representation, without the express permission of Organization, except as required to comply with a regulatory or legal process;

3) Retained Counsel has designated one or more specifically named employees responsible for the administration of its Information Security Program and will provide the names and titles of the individual(s) and their direct contact information to Organization;

4) Retained Counsel will regularly identify, assess, and mitigate the risks to the security, privacy, and confidentiality of Organization Information in Retained Counsel's operations and evaluate the effectiveness of the safeguards controlling against these risks.

5) Retained Counsel will regularly monitor its Information Security Program and assess the program at least once per year and be prepared to inform the Organization of any results upon request.

6) Retained Counsel will restrict access to Organization Information to those employees, agents, or subcontractors having a need to know the information to perform their jobs regarding Retained Counsel's representation of Organization, including but not limited to individuals involved with Information Technology maintenance, security, and forensic investigation.

7) Retained Counsel will maintain an Incident Response Plan that identifies, analyses, and, if needed, corrects an information security incident to prevent a future incident reoccurrence, which it will review and update at least annually.

8) Retained Counsel will, at its own expense, provide notice to Organization of any occurrence that could compromise or threaten the confidentiality, integrity, or availability of Organizational Information or the receipt of a complaint regarding the privacy or security practices of the law firm (a "Security Incident"), if that Security Incident exposes Organizational Information (a "Breach") within 72 hours of discovery, along with any information reasonably requested by Organization to understand or remediate the Breach, to the extent allowed by law. Information to be provided will include, but will not be limited to, the name and contact information of an employee of Retained Counsel who will serve as Retained Counsel's primary security contact, who will cooperate fully and assist Organization in and understanding the nature, root cause, and resolution of the Breach. The notice called for in this section will be given to:

[ADD ORGANIZATION CONTACT NAME and an alternate designee]

9) Retained Counsel will, at its own expense, take reasonable steps to remedy any Breach and minimize risk of future Security Incidents or Breaches in a timely manner and in accordance with all applicable laws and regulations. Retained Counsel will reimburse Organization for reasonable costs incurred by Organization in responding to, and mitigating damages caused by, any Security Incident or Breach attributable to Retained Counsel, including all costs of notice and/or remediation deemed necessary by Organization to comply with applicable laws. Organization will have the right, at its option, to solely provide and/or control any notice(s) to Organization customers, employees, or others impacted or potentially impacted by such Security Incident or Breach. Retained Counsel will not provide any notices or discuss any Security Incident or Breach with any other party without Organization's prior written consent, except as required by law, by other contractual agreements like this one, and as needed to investigate and remediate the Security Incident or Breach. Retained Counsel shall be able to notify its clients of the existence of a security incident and/or breach, although no identifying information regarding the Organization shall be provided.

10) Upon reasonable notice, Retained Counsel will allow Organization to review, assess, and inspect Retained Counsel's Information Security Program upon request and upon execution of appropriate Nondisclosure Agreements. Organization may conduct an annual review of Retained Counsel's comprehensive Information Security Program by providing to Retained Counsel a questionnaire to be completed by Retained Counsel and returned to Organization.

11) Retained Counsel will, at Organization's request, destroy or return all Organization Information in its possession and certify to Organization in writing that Retained Counsel has done so, unless necessary to require with Retained Counsel's legal obligations and/or any disputes with Organization within the applicable statute of limitations. If Retained Counsel destroys Organization Information rather than returning it, Retained Counsel will use destruction

methods that comply with all applicable state and federal laws and regulations. This obligation to return or destroy information will not, to the extent reasonable, apply to Confidential Information that is stored in backup or other disaster recovery systems, archives, or other storage systems that make it impractical to destroy the information. If Retained Counsel continues to hold Confidential Information after Organization requests return or destruction of the information, its obligations under this Agreement will continue to apply for so long as it continues to hold such information.

12) Retained Counsel shall not use or collect any Organization-supplied information and/or information accumulated about Organization during the representation (e.g., analytics, statistics, etc.) unless such information is anonymized and/or Organization is given reasonable notice of its use or collection.

13) Retained Counsel will obtain Organization's written consent before using any third party to provide services to Organization or involving Organization Information if that third party's handling of Organization's data is significantly different than already agreed/approved systems. Retained Counsel will require all third parties providing services regarding Retained Counsel's representation of the Organization to agree, in writing, to provide safeguards and breach notice for Organization Information equivalent to those as set forth in this Addendum. Specifically, Retained Counsel has confirmed that any records, data, information, and/or analytics that a third party creates regarding Retained Counsel's representation of the Organization shall be owned entirely by the Organization. This obligation does not apply to general purpose vendors used by Retained Counsel to provide general services to the entire law firm, provided Retained Counsel has reviewed and approved the information security controls of such vendor and has bound them by contract to protect Organization Information.

14) Retained Counsel agrees to carry out a background check on its non-attorney employees with access to the Organization's information, including a review of their references, employment eligibility, education, and criminal background to help minimize risk to the security of Organization Information or Organization employees and further agrees to ensure the credibility and reliability of its employees with access to the Organization's information. Retained Counsel will at the request of the Organization provide a report of its background check without revealing the identity of its employees.

15) Retained Counsel and Organization will safeguard all information and items provided to each other in order to allow other party to access Information, including but not limited to, other party's computer networks, premises, service providers, clients, keycards, codes, usernames, passwords, keys, badges, etc., as well as information that, if disclosed, would compromise the security of Organization or Retained Counsel Information, such as the designs of other party's networks, information controls, or design of its computer systems.

16) Retained Counsel will store, to the extent possible, all media that encode or contain Organization Information, including hard drives, flash drives, or other media, in a secure, protected

media storage area that is physically and environmentally controlled and protected, with appropriate physical security to prevent unauthorized access.

17) Retained Counsel has implemented or will implement the following safeguards for systems that process, store, or transmit Organization Information as agreed upon with Organization:

- Identity and Access Management that includes but is not limited to the use of complex passwords that comport with the latest guidance from the NIST.
- Encryption of particularly sensitive Organization Information (PII, PHI, etc.) in transit (e.g., via email, FTP, internet, etc.);
- Encryption of portable media, laptops, desktops, smartphones, mobile devices, and any new technologies that store Organization Information;
- Multi-factor authentication for remote access to Retained Counsel's networks;
- Training of all employees, agents, and subcontractors with current or potential access to Organization Information upon hire and at least annually thereafter, regarding their obligations to implement Retained Counsel's Information Security Program;
- Disciplinary measures, up to and including termination of employment or engagement, for employees who violate Retained Counsel's Information Security Program;
- Measures to prevent former employees, agents, and contractors from accessing Organization Information after the termination of their employment or engagement by Retained Counsel;
- Appropriately configured and updated firewall, antivirus, and anti-malware software;
- Prompt addition of vendor-recommended security patches and updates to systems and other applications;
- Intrusion detection and prevention systems with appropriate logging and alerts to monitor access controls and assure data integrity and confidentiality;
- Separation of Duties;
- Infrastructure and Physical Security; and
- Disaster Recovery Planning.

[INSERT NAME OF RETAINED COUNSEL]

By: _____

Name: _____

Title: _____

Date: _____

[INSERT NAME OF ORGANIZATION]

By: _____

Name: _____

Title: _____

APPENDIX 2—SAMPLE LAW FIRM QUESTIONNAIRE

GLOSSARY

Breach: A Security Incident that exposes Organization Information.

Incident Response Plan: A documented plan for responding to and recovering from a Security Incident.

Information Security Program: A set of policies and processes designed to identify, protect against, detect, respond to, and recover from threats to digital and non-digital information when information is created or collected, in transit, being processed, at rest in storage, or destroyed.

Organization Information: Any nonpublic information obtained by or provided to Retained Counsel that was created, compiled, modified, or received by Organization or its agents, whether that information belongs to Organization or to a third party.

Security Incident: Any occurrence that could compromise or threaten the confidentiality, integrity, or availability of information maintained by a law firm or its third-party vendors or the receipt of a complaint regarding the privacy or security practices of the law firm.

QUESTIONNAIRE

	Rating[16]	Evidence Required?[17]	Name of Document
1. General Security			
Question 1.1.			
Do you have a documented Information Security Program? If so, please be prepared to provide it.		Yes	
Sample response: Yes, our firm maintains an Information Security Policy and Health Insurance Portability and Accountability Act (HIPAA) Policy.			
Comments: All law firms should have an Information Security Program. If the firm handles information for covered entities under HIPAA, it should also maintain a HIPAA Policy. Other policies (e.g., Payment Card Industry (PCI) compliance) may be needed depending on the law firm's practice areas and client base.			
Question 1.2:			
Are the policies and processes in the Information Security Program cross-referenced to and based on applicable laws, regulations, industry standards, business standards, or operational standards (e.g. National Institute of Standards and Technology (NIST), Center for Internet Security (CIS), HITRUST, International Organization for Standards (ISO), etc.)? If so, please list which ones.			
Sample response: Our firm's Information Security Policy is consistent with industry standards and is mapped to NIST.			
Comments: Many firms use the NIST Cybersecurity Framework; other acceptable standards may include ISO27001.			
Question 1.3			
Who must comply with the policies in the Information Security Program (partners, employees, service providers, contractors, etc.)?			
Sample response: All users with network access must comply with the policies in our Information Security Program.			

[16] Rank scale: 1 = unacceptable; 2-3 = questionable, may want to ask further questions; 4-5 = reasonable.

[17] Yes indicates evidence should be prepared to be shared via screen-share or on-site visit following an executed NDA.

	Rating[16]	Evidence Required?[17]	Name of Document
Comments: Law firms must ensure that service providers and consultants comply with appropriate aspects of the Information Security Program. No "exceptions" should be given for attorneys unless they are reviewed by the Chief Information Officer (CIO), Chief Information Security Officer (CISO), or appropriate management.			
Question 1.4:			
What security certifications and attestations do you have? **Sample response:**			
Comments: The need for these certifications may vary depending on the law firm's size, work, and client base, and some may be cost prohibitive for smaller firms. Organizations should consider whether it is sufficient for a firm to meet the standards of ISO27001 without the certification process. Further, consider asking what specific functions/services are covered by the certification; ISO27001 and Service Organization Control (SOC) are scoped at the discretion of the organization being assessed. Various consultants can review these reports to determine if they cover areas crucial to in-house counsel.			
Question 1.5:			
Will your certifications and attestations remain in place for the duration of the contract? **Sample response:** Yes, all certifications are anticipated to remain in place.			
Comments: This question is to ensure that any certifications that exist as of the day the questionnaire is completed do not expire, thereby exposing the organization to unnecessary risk.			
Question 1.6			
Do you have accredited third parties assess your security controls? If so, who performs them and how frequently? **Sample response:** Our firm has an annual security assessment performed by [accredited third party] that assesses all internal and external controls firmwide. Additionally, our firm meets quarterly with a third-party security consultant to assess any new software, policies, procedures, or other material changes that have been implemented in the Information Technology (IT) environment that may affect security.			
Comments: Most law firms should consider regular third-party security assessments that test both internal and external controls. It is particularly important to assess the security implications of new or modified software and hardware. Firms should also rotate their assessment companies regularly.			

	Rating[16]	Evidence Required?[17]	Name of Document
Question 1.7			
What is the scope of the assessment(s) performed?			
Sample response: See prior response.			
Comments: While it is a best practice for assessments to be firmwide and assess all controls, organizations should determine what constitutes their largest risk and ensure the law firm is addressing those areas.			
Question 1.8:			
Will you provide the organization with the most recent and future versions of the applicable assessments?		Yes	
Sample response: Subject to execution of an appropriate nondisclosure agreement (NDA), the firm will provide this material upon request.			
Comments: Because audit reports contain information that could, if revealed, compromise the security of a firm, firms may ask organizations to execute NDAs before the reports are shared or may elect to provide information about the report verbally rather than in writing.			
Question 1.9:			
Do you perform information security risk management assessments on any companies that will be handling organization data for this representation?			
Sample response: Yes.			
Comments:			
Question 1.10:			
Do you have a document retention and destruction policy? If so, please be prepared to provide a copy.		Yes	
Sample response: Yes, we have a document retention/destruction policy. Subject to execution of an appropriate NDA, the firm will provide this material upon request.			

	Rating[16]	Evidence Required?[17]	Name of Document
Comments: Because document retention policies contain sensitive information that may compromise the security of the firm, an organization may be asked to execute an NDA before the firm shares this information. Most organizations want to ensure that any document retention policy provides for the secure destruction of organization data at the end of an engagement. In today's environment, a law firm should not hold organization data indefinitely, but firms do have ethical and loss-control requirements that may limit their ability to destroy data as soon as the engagement ends.			
Question 1.11:			
Please provide an organization chart for your Information Technology and Information Security departments or teams that includes the percentage of time each member devotes to information security activities.		Yes	
Sample response: The firm will provide this material.			
Comments: For a larger law firm, you should expect to see a separate CISO who ideally does not report to the CIO. For smaller firms, this area may be outsourced entirely to a third-party service provider.			
Question 1.12:			
Please describe the policies and processes you have in place to ensure that you are complying with all applicable privacy laws and regulations.			
Sample response: We understand our ethical and legal duties to properly protect personal data under various U.S. and international laws and regulations. We provide our attorneys with training and education in this area.			
Comments:			
2. Risk Assessment			
2.1 Cybersecurity Considerations			
Question 2.1.1:			
Will Organization Information be segregated from other firm data at all times during the engagement? If so, describe how.			
Sample response: Yes. We can maintain security controls on all Organization Information so that only your legal team has access to Organization Information in the course of the engagement.			

	Rating[16]	Evidence Required?[17]	Name of Document
Comments: This may not be possible for many law firms, particularly smaller law firms with less sophisticated information management systems. Firms should discuss, among other things, segregation processing, document review hosting, production, storage, and archiving.			
Question 2.1.2:			
Do you have a policy for business continuity? Please be prepared to provide a copy of the policy.		Yes	
Sample response: Yes, our firm has a policy for business continuity. The policy is updated annually.			
Comments: It is not unusual for firms to refuse to provide a copy of the policy for security reasons. If this is the case, consider asking for a redacted copy, a table of contents, or a remote viewing session via WebEx or similar technology. Alternatively, ask for specifics regarding topics, implementation date, review dates, and whether the policy is approved by management.			
Question 2.1.3:			
Do you have a policy for disaster recovery? Please be prepared to provide a copy of the policy.		Yes	
Sample response: Yes, our firm has a policy for disaster recovery. The policy is updated annually.			
Comments: See prior response.			
Question 2.1.4:			
Do you have a secondary site for disaster recovery purposes? If so, how far away is the disaster recovery site from the current servers that will house Organization Information?			
Sample response: Our law firm maintains a disaster recovery site more than 100 miles away from our normal servers.			
Comments: Most law firms should have an offsite disaster recovery site. Although a number of factors go into the appropriate distance from servers (e.g., physical access to the site, whether a third-party service provider is handling data, redundancy options, whether or not the law firm is in an area with a high likelihood of natural disasters, etc.) distances between 25-100 miles are considered sufficient for most businesses.			
Question 2.1.5:			
What is the current Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for your disaster recovery solution? When was the last disaster recovery test performed?			

	Rating[16]	Evidence Required?[17]	Name of Document
Sample response: Our RTOs and RPOs vary based on system and function. As examples, the RTO for our email system is 2 hours and for our financial systems is 8 hours to full resumption of activity. Our last test of disaster recovery was on [xx/xx/xxxx].			
Comments:			
Question 2.1.6:			
Do you remain up to date with system, network, and software security patches?			
Sample response: Yes.			
Comments: All law firms must answer this question in the affirmative.			
Question 2.1.7:			
If the answer to 2.16 is yes, please describe your patching process.			
Sample response: Our firm provides monthly system and security patches, with additional patches being provided on an as-needed basis if a threat develops. All patches are tested before implementation.			
Comments: Firms should discuss, among other things, the types of patches and the frequency of implementation. Because security patches are sometimes incompatible with law firm software, firms may purposely not patch vulnerable systems in order to maintain functionality.			
Question 2.1.8:			
Do you remain up to date with system, network, and software security patches? In the event of notification of a zero-day vulnerability, how long will it take for firms to apply and implement necessary security patches? Describe the process.			
Sample response: Our response will depend on the vulnerability and the systems affected. We promptly investigate and remediate known vulnerabilities.			
Comments: Firms should recognize that there is not a "one-size-fits all" solution. This sets a standard for the organization to measure firms against if a security issue arises.			

	Rating[16]	Evidence Required?[17]	Name of Document
Question 2.1.9:			
Do you perform an annual risk assessment?			
Sample response: Yes.			
Comments:			
2.2 Event Reporting			
Question 2.2.1			
Do you have an Incident Response Plan that covers incidents affecting both physical and electronic files?			
Sample response: Yes, we have an Incident Response Plan that covers incidents affecting both physical and electronic files.			
Comments: If firms do not provide a copy of the policy, organizations should ask for specifics regarding topics, roles and responsibilities, implementation date, review dates, and whether the Incident Response Plan has been approved by management.			
Question 2.2.2:			
Do you have a client notification plan in the event of Security Incidents or Breaches? If so, describe when the plan is put into action or be prepared to provide documentation.			
Sample response: Client notification is an element of our Incident Response Plan. Clients are notified within 48 hours of proper investigation of a Breach if their unencrypted data is affected.			
Comments: While many organizations would like firms to provide evidence of any Breach or Security Incident, this would be onerous for many law firms. Requiring notification when there is a Breach involving unencrypted Organization Information, regardless of whether it contains Personally Identifiable Information (PII)/Protected Health Information (PHI)/Payment Card Industry (PCI) presents a reasonable compromise.			
Question 2.2.3:			
Does your Incident Response Plan include appropriate contacts (including law enforcement)?			
Sample response: Yes.			
Comments:			

	Rating[16]	Evidence Required?[17]	Name of Document
Question 2.2.4:			
Please describe your process for notifying organization management of a Security Incident.			
Sample response: This varies by engagement but typically is done via relationship partner with consultation from our Office of the General Counsel (OGC) and IT security teams.			
Comments:			
Question 2.2.5:			
Have you created remedial plans to address deficiencies in your audits? If so, please be prepared to provide documentation to support.		Yes	
Sample response: Yes, we have created such remedial plans, which include an action log with owners and due dates.			
Comments: Firms may not provide this information, because it is typically regarded as proprietary and confidential.			
Question 2.2.6:			
Do you have the ability to track and manage incident investigations? If so, describe your process.			
Sample response: Yes, as part of our Incident Response Plan, we track and manage incident investigations and document any findings.			
Comments:			
2.3 Service Provider Due Diligence			
Question 2.3.1			
Do you anticipate using third-party service providers to store Organization Information, including but not limited to cloud storage, or any third-party tools not hosted in your environment to process Organization Information? If so, please describe the service providers and their services or tools and indicate why you are using them.			

	Rating[16]	Evidence Required?[17]	Name of Document
Sample response: We use third-party service providers to store and process Organization Information for document production [vendor x], litigation management [vendor y], and other purposes [vendor z].			
Comments: Subcontractors and service providers can be a weak link. Organizations should ensure that firms know which service providers will be used with the representation and their current cybersecurity posture, and make sure these service providers are being audited on a regular basis.			
Question 2.3.2:			
For any service providers described in 2.3.1, do you maintain an inventory of Organization Information stored (other than temporary storage under 90 days) with these service providers?			
Sample response: Yes, we maintain a list of this information.			
Comments:			
Question 2.3.3:			
Have you performed security assessments on the service providers identified in 2.3.1? If so, please describe any steps you have taken to address identified security vulnerabilities.			
Sample response: Yes, we perform annual security assessments on the listed service providers. Material security vulnerabilities are identified, and service providers are required to remediate the vulnerabilities within a reasonable period of time.			
Comments: Consider whether the amount and type of data being stored is worth this additional cost.			
Question 2.3.4:			
For any service providers described in 2.3.1, have these service providers experienced a Security Incident within the last two years? If so, please describe.			
Sample response: We know of no such incidents.			
Comments:			

	Rating[16]	Evidence Required?[17]	Name of Document
Question 2.3.5:			
Are there other subcontractors and/or suppliers who may have access to Organization Information? If so, please list those subcontractors and suppliers and describe the process for sharing/managing information for each.			
Sample response: In addition to the third-party service providers listed above, other subcontractors and suppliers like couriers and delivery services may have limited or transient access to Organization Information. The firm assesses information security practices when determining which of these subcontractors and suppliers to contract with, and it takes steps that are reasonable under the circumstances to prevent any inadvertent disclosure of Organization Information to these subcontractors and suppliers.			
Comments:			
Question 2.3.6:			
Does the firm have an ongoing service provider governance/risk management program? If so, please describe it.			
Sample response: Yes. As noted above and below, we evaluate and select subcontractors and suppliers based in part on their information security practices, and we expect them to return or destroy Organization Information obtained during an engagement, to maintain Organization Information as confidential during the engagement, and to maintain an appropriate Information Security Program. Wherever possible, we enforce these requirements by contract.			
Comments:			
Question 2.3.7:			
In your service provider agreements, do you require your service providers to (1) return or destroy all Organization Information at the end of an engagement; (2) maintain the confidentiality of Organization Information; (3) maintain an appropriate Information Security Program; and (4) have a plan to transition Organization Information in the event the provider or the firm are replaced?			
Sample response: Yes.			

	Rating[16]	Evidence Required?[17]	Name of Document
Comments: Add additional terms as necessary.			
Question 2.3.8:			
Do you outsource any of your systems, services, or infrastructure to vendors outside of the U.S.? If so, please provide the locations and percentage of the work performed outside of the U.S., as well as a description of how the outsourced systems, services, employees, or infrastructure are vetted.			
Sample response: No, no systems, services, or infrastructure are outsourced outside of the U.S.			
Comments: Storing data or accessing data from foreign locations may require the organization and the firm to analyze their liability for cyber incidents under foreign regulations.			
2.4 Representations and Warranties			
Question 2.4.1			
Do you, and will you continue to, comply with any information security requirements included in your agreement with the organization?			
Sample response: Yes.			
Comments:			
2.5 Confidentiality			
Question 2.5.1			
Will Organization Information be appropriately protected from unauthorized access or disclosure? Describe all standards and systems currently in place to provide protected environments.			
Sample response: Yes. The firm has in place an Information Security Program that will protect Organization Information (including any Protected Health Information (PHI), Personally Identifiable Information (PII), Nonpublic Personal Information (NPI), or Payment Card Industry (PCI)) from unauthorized access and disclosure and maintain it in compliance with all applicable laws and regulations.			

	Rating[16]	Evidence Required?[17]	Name of Document
Comments: Consider whether Organization Information for the engagement(s) will include PHI, PII, NPI, or PCI information that may require additional protections (encryption, monitoring, role-based restricted access, etc.)			
Question 2.5.2			
If you have any data that may subject to the European Union (EU) General Data Protection Regulation (GDPR), do you have a protocol for handling this data in compliance with the aforementioned authority? If so, please describe.			
Sample response: We have mapped where data subject to EU regulations is stored for each client, and we comply with all GDPR requirements for storing and processing that data. At a client's request, we will execute an EU data processing agreement.			
Comments: If the firm has access to personal information regulated by the GDPR, the firm must comply with the GDPR. This may include appointing a Data Protection Officer or contracting with a third-party service provider for these services. Firms with international clients or U.S.-based clients that have an international reach (e.g., e-commerce) should apprise themselves of these regulations.			
Question 2.5.3			
If you have any data that may be subject to other non-U.S. data protection regulations, do you have a protocol for handling this data in compliance with the aforementioned authority? If so, please describe.			
Sample response:			
Comments: This answer will depend on the data to which the law firm has access.			
2.6 Termination			
Question 2.6.1			
Do you have a transition plan to facilitate the orderly winding up and transfer of data and services back to the Organization or to another law firm? If so, please describe.			
Sample response: Yes. Our departure procedures outline departure steps to be executed for both personnel and Organization Information.			
Comments:			

	Rating[16]	Evidence Required?[17]	Name of Document
2.7 Insurance			
Question 2.7.1			
Do you have cyber liability insurance with an insurance company having a minimum credit rating of A– from S&P or an equivalent rating agency? If so, please provide evidence of coverage.		Yes	
Sample response: Yes.			
Comments:			
Question 2.7.2			
With regard to the coverage referenced in 2.7.1, please describe the coverages and sublimits that you maintain.			
Sample response:			
Comments: Depending on the scope of services, the organization may not need this level of detail from a firm.			
Question 2.7.3			
Will you add the organization as an additional insured to the coverage referenced in 2.7.1?			
Sample response: We cannot.			
Comments: Some policies will not permit this, will not permit it for a reasonable price, or do not have additional insured endorsements with appropriate limits on the firm's exposure.			
3. Asset Security			
3.1 Inventory of Authorized and Unauthorized Devices			
Question 3.1.1:			
Do you use an automated asset inventory discovery tool to build and maintain an asset inventory of systems connected to your public and private networks (yes or no)?			
Sample response: Yes.			
Comments:			

	Rating[16]	Evidence Required?[17]	Name of Document
Question 3.1.2:			
Does the asset inventory include the following elements: (yes or no)? ● Network address ● Machine name ● Asset purpose ● Asset owner ● Associated department ● Asset location			
Sample response: Yes.			
Comments:			
Question 3.1.3:			
Upon discovery of an unauthorized device, how long does it take your IT staff to remove the device from the network, disable it, or eliminate access to the network (in minutes)?			
Sample response: Unauthorized devices cannot connect to our private network and may access our public Wi-Fi network only if the user can supply the appropriate password.			
Comments:			
Question 3.1.4:			
When IT equipment is retired, do you sanitize or securely destroy all Organization Information on the equipment? If so, what standards do you use, and do you require written certification of destruction if you use a third-party service provider?			
Sample response: Yes. Equipment is sanitized or destroyed using Department of Defense destruction methods. We require written certification of destruction when we use a third-party service provider.			
Comments:			
3.2 Inventory of Authorized and Unauthorized Software			
Question 3.2.1:			
Do you perform regular scanning and generate alerts when unapproved software is installed on a computer?			

	Rating[16]	Evidence Required?[17]	Name of Document
Sample response: Yes.			
Comments:			
Question 3.2.2:			
Do you deploy software inventory tools for all servers and workstations?			
Sample response: Yes.			
Comments:			
Question 3.2.3:			
Do you have a change control/review process for software patches and updates? If so, please describe.			
Sample response: Yes. This is covered in our change control procedures, with weekly review meetings for approvals.			
Comments:			
Question 3.2.4:			
If application development is performed in-house (including interfaces, add-ons, modules, plug-ins, etc.), then describe your software development security procedures.			
Sample response:			
Comments: Organizations should also consider whether the firm's in-house application development indirectly involves third parties.			
3.3 Continuous Vulnerability Assessment and Remediation			
Question 3.3.1:			
Do you perform INTERNAL vulnerability scanning and/or penetration testing annually? If so, please provide the date of your last test.			
Sample response: Yes. [xx/xx/xxxx].			
Comments: Ensure that the date is within last 12 months or that the next test date is in the not too distant future.			

	Rating[16]	Evidence Required?[17]	Name of Document
Question 3.3.2:			
Do you perform EXTERNAL vulnerability scanning and/or penetration testing annually? If so, please provide the date of your last test.			
Sample response: Yes. [xx/xx/xxxx].			
Comments: Ensure that the date is within last 12 months or that the next test date is in the not too distant future.			
3.4 Physical Security			
Question 3.4.1:			
Do you have a physical security policy that includes all data centers and office locations? If so, please be prepared to provide.		Yes	
Sample response: Yes.			
Comments: Pay particular attention to visitor policies and video monitoring.			
Question 3.4.2:			
Do you have policies or programs in place to support the ongoing management of environmental controls (i.e. HVAC, fire detection and suppression, fuel/generator, etc.) for your offices and facilities? If so, please describe.			
Sample response: Yes. [Describe specifics.]			
Comments: Primary focus here would be on data-center environment.			
Question 3.4.3:			
Are there secure facilities and processes at each location for disposing of confidential materials (e.g., shredders, locked bins, etc.)? Please describe.			
Sample response: Yes. [Describe specifics.]			
Comments:			
Question 3.4.4:			
Is access to your facility controlled by the use of an electronic access control system (e.g., badge reader, biometric scanner)?			

	Rating[16]	Evidence Required?[17]	Name of Document
Sample response: Yes.			
Comments:			
Question 3.4.5:			
Do you physically maintain your own data centers? Whether yes or no, please provide details about who maintains them and where they are geographically located.			
Sample response:			
Comments: The exact location may be confidential, so consider if confirmation of high-level details will be acceptable.			
3.5 Malware Defenses			
Question 3.5.1:			
Is there an anti-malware policy or program that includes work-stations, servers, and mobile devices?			
Sample response: Yes.			
Comments:			
Question 3.5.2:			
What is the percentage of systems with anti-malware systems deployed, enabled, and up to date?			
Sample response: Approximately 90 percent.			
Comments:			
3.6 Secure Configurations for Network Devices such as Firewalls, Routers, and Switches			
Question 3.6.1:			
Have you defined secure configurations for each type of net-work device in writing?			
Sample response: Yes.			
Comments:			

	Rating[16]	Evidence Required?[17]	Name of Document
4. Communications and Network Security			
Question 4.1:			
Do you encrypt Organization Information at rest and in transit? If so, please describe how.			
Sample response: Yes. All workstations and servers are encrypted with 256-bit encryption.			
Comments: This is especially important if PHI/PII/PCI will be involved in the representation.			
Question 4.2:			
Do you have network security mechanisms in place (e.g., firewalls, intrusion-detection/intrusion-prevention systems (IDS/IPS), etc.)? If so, please describe.			
Sample response: Yes. We have firewalls at our perimeter and at key points within network for segmentation.			
Comments:			
Question 4.3:			
Do you monitor audit logs for your network? If so, please describe your policies and processes, and include in your description how often the logs are reviewed.			
Sample response: Yes. We use a log aggregator with key alarms set for notification to our security team.			
Comments:			
Question 4.4:			
If a system fails to log properly, how long does it take for an alert about the failure to be sent?			
Sample response: Varies per system; key systems report within 60 minutes.			
Comments:			

	Rating[16]	Evidence Required?[17]	Name of Document
Question 4.5:			
Do you have a corporate wireless network or a guest wireless network? If you have a guest network, is it segregated from the corporate network? Is Wi-Fi Protected Access 2 (WPA2) encryption and enterprise authentication implemented for the corporate wireless network?			
Sample response: Yes for all.			
Comments:			
Question 4.6:			
What information security policies and processes are in place that are specific to access from portable devices and mobile devices?			
Sample response: Our mobile devices are covered in our encryption policy (all require encryption).			
Comments:			
Question 4.7:			
Does your email system support Transport Layer Security (TLS) for encryption?			
Sample response: Yes.			
Comments:			
Question 4.8:			
Do you use secure configuration standards for network and server infrastructure?			
Sample response: Yes.			
Comments:			
Question 4.9:			
Do you restrict access to websites that can be used to exfiltrate confidential data (e.g. Gmail, Yahoo!)? If so, please describe the restrictions.			

	Rating[16]	Evidence Required?[17]	Name of Document
Sample response: Yes. Webmail is blocked.			
Comments:			
Question 4.10:			
Do you utilize intrusion-detection systems (IDS) or intrusion-prevention systems (IPS) on your network? If so, please describe them, and include in your description whether they work within your network or at its perimeter.			
Sample response: Yes, we utilize IDS on the perimeter of our network.			
Comments: Perimeter detection should be deployed. Best practice is to also have internal detection that looks for abnormalities within the environment, as well as malware.			
Question 4.11:			
Do you utilize a data loss prevention (DLP) solution, and do you have a written policy prohibiting data exfiltration?			
Sample response: Yes.			
Comments:			
5. Identity and Access Management			
Question 5.1:			
Are protections in place for remote access, including authentication mechanisms, encryption algorithms, and account management process? If so, please be prepared to describe them.		Yes	
Sample response: Yes. All listed procedures are in place.			
Comments:			
Question 5.2:			
Do you screen all partners, employees, service providers, and contractors, including a criminal background check, prior to hiring? If so, please be prepared to describe your screening policies and procedures.		Yes	

	Rating[16]	Evidence Required?[17]	Name of Document
Sample response: Yes, all the listed personnel are screened, and the screening of all but contractors includes a criminal background check. Individual employees of certain contractors may be screened if they have access to sensitive information.			
Comments:			
Question 5.3:			
Are access controls in place that cover adding users, setting their permissions, monitoring their activities, changing their access, and deleting users? If so, please be prepared to describe these controls.		Yes	
Sample response: Yes, all the listed controls are in place.			
Comments: Sound access control requires firms to establish role-based access based on the principle of least privilege, to segregate key duties, to review user access with reasonable frequency, and to promptly adjust user access in the event of role changes or terminations.			
6. Security Operations			
Question 6.1:			
Are new employees required to sign agreements relating to confidentiality and information security upon hire?			
Sample response: Yes.			
Comments: Law firms should have agreements that address both confidentiality and information security.			
Question 6.2:			
Is there a security awareness training program? If so, please describe it, and include in your description which employees must participate and how often.			
Sample response: Yes, we train all new employees with access to sensitive data at the time they are hired, and we also have an annual mandatory security training and updates that are circulated by email.			
Comments: Ideally, law firms should have regular modules and training (e.g., quarterly or monthly). Training upon hire and annual training should be the minimum.			

	Rating[16]	Evidence Required?[17]	Name of Document
Question 6.3:			
Does your security awareness training program include specialized content for employees with access to sensitive data (e.g., Accounting, Human Resources (HR)) or privileged accounts (e.g., IT)?			
Sample response: Yes, additional training is given to employees with access to sensitive data and those with privileged accounts.			
Comments:			