American Bar Association (ABA)
Cybersecurity Legal Task Force
Vendor Contracting Project: Cybersecurity Checklist[1]
Second Edition (2021)

The views contained herein do not necessarily reflect the views of each participant or the official policy of their respective agencies, private sector organizations, the United States Government, the American Bar Association, or the ABA Cybersecurity Legal Task Force. The views expressed herein represent the opinion of the authors. They have not been approved by the House of Delegates or the Board of Governors of the American Bar Association and, accordingly, should not be construed as representing the position of the Association or any of its entities.

ABA Cybersecurity Legal Task Force

The ABA Cybersecurity Legal Task Force was created in 2012 at the recommendation of then-ABA President Laurel Bellows. The Task Force's goal is to examine how to help lawyers protect their practices and their clients' confidential information and intellectual property during cyber events and position the ABA to contribute to the national cyber dialogue. The Task Force is comprised of representatives from over 25 ABA entities interested in the cyber domain and leaders in the private sector responsible for cybersecurity. To learn more, visit www.ambar.org/cyber.

Introduction

This Cybersecurity Checklist is directed to solo and small firm attorneys who interact with vendors offering them or their client's products or services that involve access to their sensitive data or internal systems. Keep in mind, however, that access to internal systems is not always open and obvious, as Target learned in the 2013 data breach stemming from its HVAC vendor. In these days of increasing cybersecurity risks, the mantra "know your supplier" cannot be overstated. This Checklist highlights the ways practitioners who are not steeped in the nuances of data privacy and

---

[1] This Checklist (Second Edition) was prepared by ABA members William R. Denny (*Wilmington, Delaware*) and Claudia Rast (*Ann Arbor, Michigan*), with valuable input from representatives and affiliates of the ABA Cybersecurity Legal Task Force [Allison Ahroni, (*New York City, New York*), Michael Aisenberg (*McLean, Virginia*), Norman Dupont (*Costa Mesa, California*), Pamela Esterman (*New York City, New York*), Christopher Frascella (*Washington, District of Columbia*), Sally Heuker (*Washington, District of Columbia*), Eric Hibbard (*Sunnyvale, California*), Maureen Kelly (*Washington, District of Columbia*), Aaron Schildhaus (*Washington, District of Columbia*), Alan Wernick (*Chicago, Illinois*), and Stephen Wu (*San Jose, California*)]. It builds on the first edition developed in 2016 by Cheryl M. Burtzel (*Austin, Texas)*, Candace M. Jones (*New York, New York)*, Lisa R. Lifshitz (*Toronto, Ontario, Canada*), and Lucy L. Thomson (*Washington, D.C.*).

data security can minimize cybersecurity risks in their contractual transactions with third party vendors. The Checklist frames the issues solo and small firm attorneys should consider in a context that is consistent with common principles for managing cybersecurity risk and addresses typical transactions from the due diligence aspect, beginning with vendor selection and moving to contracting and vendor management. Cybersecurity agreement provisions are not "one-size-fits-all" and should be informed by the relative risks presented by the transaction, such as the sensitivity and value of the data, the nature of the firm or client's business, and available risk mitigation strategies.

The Checklist begins with an executive summary that includes links to deeper dives into particular topics. For convenience, the Checklist uses the terms "**vendor**" or "**supplier**" to refer broadly to any third-party supplier of goods or services that involve cyber-related risk because they either directly connect to internal systems or involve the processing of personal or other sensitive data and uses the terms "**customer,**" "**client,**" or "**you**" to refer broadly to the party procuring or receiving the goods or services. The term "**agreement**" is used to refer to a product purchase agreement, license agreement, service agreement, or other agreement however styled to reflect the nature of the arrangement between the vendor and customer.

Introduction 1
Executive Summary 4
1. Cybersecurity Strategy – Understanding the Transactional Landscape 11
2. Risk Assessment – Cybersecurity Considerations for the Transaction 12
A. Due Diligence 13
B. Due Diligence Questionnaires 14
C. Relevant Ethics Rules 16
D. Data Security Planning 17
3. Contract Provisions – Setting Expectations, Mitigating Risk, and Allocating Liability 25
A. Definitions 25
B. Understanding the Product or Service. 26
C. Representations and Warranties. 26
D. Data Ownership and Access and Use Rights. 26
E. Confidentiality. 29
F. Security Program. 31
G. Privacy. 33
H. Audit of Vendor Performance 35
I. Cyber Incident Reporting. 36
J. Remedies. 36
K. Termination 36
L. Insurance. 38
M. Limitation of Liability and Indemnification. 40
N. Business Continuity and Resiliency 41

Executive Summary

1. Cybersecurity Strategy – Understanding the Landscape of the Transaction

Management of vendor relationships is critical to effective cybersecurity because many breaches happen through vendors. Take for example the December 2020 news of the SolarWinds breach. SolarWinds is an IT monitoring and management company that provides software tools for network systems operators. Though little-known before the breach, SolarWinds counted 425 of the Fortune 500 among its customers and multiple federal government agencies.[2] Also revealed in December 2020, but with less media coverage was the breach of Accellion's file transfer tool, FTA, which impacted law firms Jones Day and Goodwin Proctor, among others.[3] [4] Many businesses may not even realize how many vendor relationships they have, or what access vendors have to their systems and data. Businesses often rely heavily on technology solutions to monitor or protect their networks without understanding the risks posed by these suppliers.

Law firms are not immune from cybersecurity incidents, even small or solo firms. The ABA's *Tech Report 2020* details how law firms continue to suffer data breaches,[5] and are often targeted because they obtain, store, and use highly sensitive client information. 29% of the law firm respondents reported experiencing a security breach over the last year (up 3% from 2019),[6] including lost or stolen devices, hacker activity, and website exploitation.[7] Because customers and regulators increasingly demand that businesses effectively manage third-party risk, addressing this risk efficiently and comprehensively is critical to a law firm's success.

"29% of the law firm respondents reported experiencing a security breach over the last year (up 3% from 2019), including lost or stolen devices, hacker activity, and website exploitation."

2. Risk Assessment– Cybersecurity Considerations for the Transaction

Before entering into a vendor relationship, a due diligence risk assessment must be conducted to address the risks presented by the transaction, including cyber risks. Customers want to ensure that what they obtain from vendors at least maintains the level of cybersecurity controls required by applicable law, relevant security frameworks, and internal policies and practices. Vendors want to

---

2 The New York Times, https://www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security-pentagon.html?searchResultPosition=1 (published Dec. 14, 2020, updated Dec. 15, 2020).

3 MarketWatch, https://www.marketwatch.com/story/lower-profile-accellion-hack-hit-dozens-of-high-profile-targets-including-kroger-csx-harvard-01615154005 (published Mar. 7, 2021).

4 Lawsuits mount for vendor linked to Jones Day, Goodwin Procter data breaches, Reuters (Feb. 24, 2021) available at https://www.reuters.com/article/accellion-lawsuits-idUSL1N2KV3D5.

5 ABA Tech Report 2020, https://www.lawtechnologytoday.org/2020/10/techreport-2020-cybersecurity/?utm_medium=email&utm_source=salesforce_303064&sc_sid=03660239&utm_campaign=YOURABA&promo=YOURABA&utm_content=&additional4=&additional5=&sfmc_j=303064&sfmc_s=45074674&sfmc_l=2776&sfmc_jb=26&sfmc_mid=100027443&sfmc_u=9012336.

6 *Id.*

7 *Id.*

assess both their own and their customers' security postures to promote sales, ensure customers can meet vendor-imposed security obligations, and mitigate their legal risks.

Customers dealing with vendors might balance the benefits of using customized due diligence questionnaires with the potentially significant burden such questionnaires might impose on vendors. Vendors might ask what type of customers are being served, what products are being provided, what customers will do with the products, what data they will access, and what laws will apply. The due-diligence dance between a vendor and prospective customer has become increasingly complex. It is not enough to require a representation and warranty of "compliance with applicable and relevant laws or industry standards." The dynamic and evolving nature of cybersecurity vulnerabilities defies being tied simply to current law or a particular generic guidance document. This Checklist identifies various resources and tools for assembling due diligence questionnaires.

A. Due Diligence

When evaluating any potential vendor, you must exercise due diligence, including the use of qualified information security personnel. To the extent potential cybersecurity weaknesses in a potential vendor's system are identified (e.g., weak passwords or password reset management, lack of multi-factor authentication), you (informed by these experts) will need to weigh these risks against the transaction's benefits and consider appropriate mitigation. This initial assessment and the plan for any agreed remediation should inform the agreement. After completing your due diligence, you may also need to reassess your or your client's overall risk profile to account for any risks arising from the vendor relationship that your firm or the client will need to manage. Of course, all parties will need to assess risk as their respective environments change or whenever additional products or services are implemented. Cyber threats evolve, and risk and its inherent vulnerabilities are not static. This is not a one and done environment, but a constant arena of change.

"Cyber threats evolve, and risk and its inherent vulnerabilities are not static."

B. Due Diligence Questionnaires

Due diligence of the vendor often includes the request that a potential vendor complete a due diligence questionnaire. There are a number of standardized questionnaires that a customer can adopt or modify, and some vendors, especially the larger ones, may have their own set of answers to standard due diligence questions or risk assessments that they will offer to the customer in the place of answering multiple non-standard questionnaires. Law firms should consider maintaining their own set of responses to standard due diligence questions to provide to clients upon request.

C. Relevant Ethics Rules

Lawyers have ethical duties to take reasonable security measures to protect confidential client information. They also have an obligation to be technologically competent, or if not, to seek assistance from someone who is. A significant element of legal representation involves both understanding the information security risks to confidential client information and safeguarding

these confidences competently and acting responsibly if an unauthorized disclosure occurs.[8] Section 2.C. of the Checklist details relevant ethics rules. An additional resource for understanding these issues is the *ABA Cybersecurity Handbook (2nd)*.[9]

D. Data Security Planning

Section 2.B. of this Checklist discusses concrete examples of how to shape and develop standards and defensible cybersecurity practices.[10] It is important to consider company or client-specific circumstances during the planning phase. High-profile breaches illustrate the additional legal complications attached to consumer personal data[11] and other sensitive data, highlighting the risks to a company's reputation and brand and other tangible and intangible consequences.

Law firms are inherent targets due to the high-profile clients they represent and the abundance of confidential data and communications they tend to store. Thus, data security planning is critical for all firms, particularly smaller firms that may have access to fewer technology resources. The ever-changing landscape of risks and attack methods amplify the threat, especially as those lawyers who have been working remotely since the onset of COVID-19 restrictions in March/April 2020 are now deciding to continue to work remotely. The ubiquity of the Internet of Things (IoT), legal outsourcing, the use of mobile devices, Bring Your Own Device (BYOD) policies, cloud computing and home WiFi expand the potential number of vulnerable entry points for cybercriminals. Methods of cyber-attacks are also proliferating and evolving.

"Law firms are inherent targets due to the high-profile clients they represent and the abundance of confidential data and communications they tend to store."

3. Contract Provisions – Setting Expectations, Mitigating Risk and Allocating Liability

Section 3 of the Checklist provides sample provisions and other resources regarding terms likely to reflect information security or privacy considerations. It does not cover agreement provisions that do not directly implicate data security and privacy. Keep in mind that the agreement between you or your client and its selected vendor should contemplate the entire vendor lifecycle. Contract provisions, including those that address cybersecurity and privacy must be customized to address the risks.

---

8 ABA Formal Opinion 483 (Oct. 17, 2018).

9 ABA Cybersecurity Handbook, (Jill Rhodes, Robert S. Litt, ed., 2d Ed. 2018).

10 Fontaine, D. and Stark, J.R. Guest post: Three cybersecurity lessons from Yahoo's legal department woes. The D&O Diary (March 30, 2017) available at http://www.dandodiary.com/2017/03/articles/cyber-liability/guest-post-three-cybersecurity-lessons-yahoos-legal-department-woes/.

11 Capital One Fined $80 Million in Data Breach, US News & World Report (August 7, 2020) available at https://www.usnews.com/news/business/articles/2020-08-06/capital-one-fined-80-million-in-data-breach.

A. Definitions

The agreement should define key terms related to information security and privacy. The Glossary attached as Appendix C is available as a resource. However, definitions should be specific to the particular agreement.

B. Understanding the Product or Service

The agreement should describe how the product or service implicates information security. For example, will this be an on-site or third party hosted solution? What connectivity will be required with internal systems? A detailed description of the security and privacy-related aspects of the product or service can provide a roadmap for ensuring that security and privacy-related risks are addressed in other relevant provisions of the contract. You should also consider your firm's or client's direct responsibilities, whether stated explicitly or imposed implicitly by the product or service's limitations. For example, a vendor-hosted solution may provide the tools for securing the site and protecting data, but the responsibility may shift to you or your client to configure those tools properly.

C. Representations and Warranties

Section 3 of the Checklist includes sample representations and warranties.

D. Data Ownership and Access and Use Rights:

Section 3 also reviews data ownership, which is a big deal, particularly in the legal context. If you own it, you can monetize it, and data can be digital gold. Also, ownership of data gives rise to legal and contractual obligations to safeguard data and to be responsible for the rights of data subjects. Lawyers have ethical obligations, as well, in processing data owned by the client.

E. Confidentiality

This section on confidentiality discusses how the failure to appropriately address confidentiality requirements can expose the organization to significant liabilities. Encryption, combined with the appropriate key management, is one mechanism frequently used to implement confidentiality protections. The customer and all vendors with access to the confidential information should use these protections when the sensitive data are both in transit (communications and transfers) and at rest (stored).[12]

F. Security Program

Information security involves the implementation of security controls to protect a business's digital assets. In the context of vendor contracts, this involves protection of both the vendor's computer systems network and software and your client's electronic data, records, and systems to which the

[12] NIST Special Publication 800-175B Rev. 1, Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms, provides specific guidance on acceptable encryption and key management.

vendor has access. Measures to design the security of information systems and data are generally grouped into the following three categories: (1) physical security controls, designed to protect the tangible items that comprise the physical system, (2) technical security controls, involving the use of software and data safeguards incorporated into computer hardware and related devices, and (3) administrative controls, consisting of written policies, procedures, standards, and guidelines to guide conduct, prevent unauthorized access, and provide an acceptable level of protection for computing resources and data.

While most state data security laws require that a business implement and maintain reasonable security of personal information, including information in the hands of your vendors, some laws, such as the Massachusetts data security regulations,[13] are more prescriptive and require that the business maintain a Written Information Security Program (WISP). Multiple laws applying to a business's cybersecurity practices create obvious challenges to compliance. Therefore, instead of trying to reconcile all of the laws, regulations and guidelines describing the required level of security, it is most practical to pick one framework (such as NIST Cybersecurity Framework, ISO 27001 series, CIS Critical Security Controls), actively manage it, and audit the results. As discussed, in the agreement, you can add a provision that calls for implementation of a specific framework or, in higher risk scenarios, identify more detailed, specific cybersecurity controls that must be implemented.

G. Privacy

The terms "privacy" and "security" are often used interchangeably, however, privacy and security provisions are generally distinct. Privacy envelopes a type of data that relates to a person. To adequately address privacy in a contract, you need to know what type of data is collected, why it is collected, what is done with it, who processes it, where is it transferred, *etc*. Security addresses how data is kept confidential and secure.[14] The agreement will need separate provisions addressing both privacy and security. For example, you or your client will want to ensure that the vendor abides by all applicable data privacy laws in connection with its processing of personal data, such as addressing how the data may be accessed, used, and shared, and the vendor's obligations in the event it determines there has been unauthorized access to the data.

H. Audit of Vendor Performance

Contractual provisions in the agreement addressing routine monitoring of a vendor's obligations under a service agreement are standard, but especially critical when that vendor is handling personal or confidential data such as privileged data. Such provisions often include compliance certifications that the customer can request annually, such as requiring the vendor to have "reported all known material breaches of security, suspected fraud, or other irregularities, or reportable incidents that may constitute violations of law, breaches of this agreement, or vendor's ethics or corporate social responsibility policies." You might also consider an ongoing requirement the

---

[13] Mass. Standards for the Protection of Personal Info., 201 CMR 17.00 et seq. By specifically requiring businesses to implement a risk-based, process-oriented, "comprehensive, written information security program" in accordance with a detailed list of requirements, the Massachusetts regulations created one of the most comprehensive sets of general data security obligations imposed on businesses by a state.

[14] It is important to note that all "data" is not always or necessarily personal data. It may be confidential business data, but still critical to protect.

vendor will be responsible for identifying and becoming familiar with any changes in laws that are applicable to the vendor's delivery or performance of its services.

I. Cyber Incident Reporting

Include a provision on reporting obligations in the event of a cyber incident. The vendor should have some form of written "security" plan that outlines in detail what steps it will take when a cyber incident occurs. Different jurisdictions have different notice requirements in the event of a breach involving personal information and some regulated industries are also obligated to report breaches, so receiving timely notice from the vendor is vital. In addition to these legal requirements, many customers, including law firm clients, contractually obligate companies to disclose cyber incidents. Sample language for an agreement is included in this portion of Section 3.

J. Remedies

The agreement should address what remedies are available if the vendor does not meet its cyber obligations. Remedies should be appropriate for the nature of the failed performance, and actionable. For example, a framework to provide a timely response, including escalation procedures, commensurate with the severity of a defect or vulnerability, may be as important to mitigate loss as a damages provision.

K. Termination.

Often lost in negotiations is what happens to customer data when the agreement with the vendor ends. As noted in the data ownership section, your firm or client will want to consider language in the agreement to address the potential for off-boarding or later transferring the data back to the customer or to a different vendor or alternatively securely destroying the data when the existing vendor agreement is terminated. If the vendor is to destroy the data, the timing of the destruction should be discussed, and the customer may want to request that the vendor certify that the data has been securely destroyed. In some instances, vendors may need to maintain the data for a period of time to meet applicable regulatory requirements.

L. Cyber Insurance.

In addition to assessing whether you or your client should maintain cyber insurance to address and mitigate internal and outsourcing risks, also consider whether you want to contractually obligate the vendor to carry cyber insurance. As with any type of insurance, a cyber insurance policy will often not cover all losses, so it is critical to understand the applicable deductibles, coverage limits, and what risks are excluded.

M. Limitation of Liability and Indemnification

This section analyzes contract-based caps on liability often advocated by vendors and potential responses to those caps. Many vendors try to limit their liability to the amount of their fee, despite that potential harm to the customer from failure of the vendor to protect the security or privacy of confidential information could far exceed that amount. Vendors also often limit their liability by

limiting damages to direct damages only while disclaiming consequential damages. Such a limitation could easily preclude any recovery for a customer's costs and liability as a result of a vendor's data breach.

One effective way for customers to mitigate their risk of loss is to require indemnification for all direct losses and third-party claims arising out of a security breach, and to carve this indemnification obligation out of the limitation of liability clause. In other words, the indemnification liability should not be capped by the amount of fees paid or limited with respect to the type of damage suffered by the customer.

N. Business Continuity and Resiliency

Any vendor deemed "critical" to you or your client (*i.e.,* a vendor whose sudden shut down would have a significant adverse impact upon your client's business or its customers) should be required to provide a copy of its disaster recovery or business continuity plan. These plans are becoming increasingly common among vendors and should not present a sticking point in contract negotiation. If it is—beware. In addition, you should require the vendor to provide its latest disaster recovery test results to confirm that the vendor has taken appropriate steps to continue operations (*i.e.,* to continue to provide the services that your client has contracted to receive) in the event a disruption event occurs to the vendor's operations.

The Cybersecurity Checklist also includes a series of appendices that provide additional tools for you to use in developing the developing appropriate cybersecurity obligations and managing performance of those obligations through contract performance. Those appendices are as follows:

Appendix A – Resources for Developing a Strategy to Identify and Manage Cybersecurity Risk

Appendix B – Federal Financial Regulator Guidance—Third-Party Providers

Appendix C – Glossary

Appendix D – NIST Key Areas in a Security Program

Appendix E – Sample Provision Covering Personal Information

Appendix F – Data Breach Disclosure Laws

Appendix G – Resources for Vendor Management Practices

Appendix H – Resources for Establishing a Written Cybersecurity Governance Framework

Appendix I - Certificates and Attestations

Appendix J – Contract Provisions: Termination

1. Cybersecurity Strategy – Understanding the Transactional Landscape

According to a 2018 study, more than 58% of companies have experienced a data breach caused by a vendor or other third party,[15] and an estimated 28% involved small businesses.[16] These numbers are likely to increase. Studies show that the deployment of a remote workforce increases not only the attack landscape as hundreds if not thousands of workers are dispersed across the country, but also the response times and ultimate costs of mitigating and restoring breached systems.[17] All law firms should establish and maintain a documented strategy for identifying and managing cybersecurity risks. This strategy should be informed by relevant laws and regulations, the customer's contractual commitments to its customers, applicable industry standards, business and operational requirements, and the firm's risk self-assessment.[18] [19] A law firm's business and risk strategies should account for third party interactions, particularly as a customer or client representative, and transaction terms should address the firm or client's cybersecurity strategy for the vendor. A list of possible considerations for a cybersecurity strategy is contained in **Appendix A.** Applicable law may mandate specific terms for vendor agreements. A list of such laws can be found in **Appendix B,** with some state laws listed in **Appendix E.1**.[20]

"All law firms should establish and maintain a documented strategy for identifying and managing cybersecurity risks."

---

15 *Opus & Ponemon Institute Announce Results of 2018 Third-Party Data Risk Study*, BUSINESSWIRE (Nov. 15, 2018), https://www.businesswire.com/news/home/20181115005665/en/Opus-Ponemon-Institute-Announce-Results-2018-Third-Party.

16 2020 Data Breach Investigations Report, Verizon (Sept. 7, 2020) at 79, https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf (last accessed Sept. 7, 2020). (While differences between small and medium-sized businesses (SMBs) and large organizations remain, the movement toward the cloud and its myriad web-based tools, along with the continued rise of social attacks, has narrowed the dividing line between the two. As SMBs have adjusted their business models, the criminals have adapted their actions in order to keep in step and select the quickest and easiest path to their victims.").

17 Bluefin, Key Takeaways from IBM and Ponemon's 2020 Cost of a Data Breach Report available at https://www.bluefin.com/bluefin-news/key-takeaways-ibm-ponemons-2020-cost-data-breach-report/, "According to Ponemon's survey, businesses are acutely aware of the threat [of COVID-19], with 78% of respondents reporting that remote work would increase the time it would take to identify and contain a data breach. The longer it takes to contain a breach, the most expensive it becomes, and 70% of survey respondents acknowledged that remote work would indeed increase the overall cost." (Last accessed Dec. 16, 2020).

18 *See* industry-specific laws with security and privacy requirements, such as the Gramm-Leach-Bliley Act (GLBA) (financial services), HIPAA, and the Health Information Technology for Economic and Clinical Health Act (HITECH). *See also* **Appendix B** for examples of U.S. federal regulator guidance on managing outsourcing of third-party risk.

19 States have enacted laws that require organizations doing business in the state to take reasonable measures to protect and secure data in electronic form containing personal information. All U.S. states have breach notification laws triggered by loss of personally identifiable or other sensitive information. Organizations with global business operations must comply with applicable country-specific laws and may be subject to rules of intergovernmental organizations, *e.g.*, European Union, Canada, the Association of Southeast Asian Nations, Asia-Pacific Economic Cooperation, etc. Additional guidance can be expected over time.

As a solo and small firm lawyer, vendor selection should be guided by your or your client's requirements for relevant and secure information systems. These requirements should anticipate access controls that your firm or your client will implement and maintain in its information security plan. Clients should have an informed and realistic view of their environment and business needs so they can reasonably assess the impacts of introducing a vendor relationship and make appropriate business judgments consistent with their risk tolerance and applicable legal and contractual requirements. Based on the nature of the goods or service and the parties' relationship, new vendors may introduce, or increase risk. Your client should clearly understand the vendor's service delivery model and approach, including the proposed use of third parties who may have access to or impact the client's systems and data. Your customer should also plan adequate resources to implement and maintain appropriate vendor management practices. A list of resources for vendor management practices can be found in **Appendix G**.

It is also important to understand how you or your client's requirements could affect the vendor's operations—e.g., supplying a client in regulated industries may impose additional requirements. For example, if your client plans to use a cloud service to host its data, the cloud provider will need to know what types and categories of data it will host, particularly if the provider's servers are located outside of the domestic US or the client is subject to industry specific cybersecurity requirements such as a government contractor.

Understanding the transactional landscape requires the active involvement of individuals at your firm's or client's organization who understand the business objectives, the business process (particularly the participants and information involved), the information systems, and the organization's risk tolerance and risk management practices. Those responsible for the business activities of the product or service will drive transaction planning, with help from those who implement, manage, and oversee the effectiveness of the cybersecurity strategy. Firms and client organizations with established written cybersecurity governance frameworks should be better equipped to plan for and implement new or changed vendor-customer relationships in the ordinary course of business. A list of resources for establishing a written cybersecurity governance framework can be found in **Appendix H**.

2. Risk Assessment – Cybersecurity Considerations for the Transaction

A risk assessment should identify the relative importance of functions, activities, products, and services.[21] Firms and their clients should also evaluate the inherent cybersecurity risk presented by the people, processes, technology, and data supporting those things, and assess the existence and effectiveness of controls to protect against the risks. This aids the development of remediation plans to reduce risks and vulnerabilities to a reasonable and appropriate level.

[21] Risk assessments can inform decision-makers and support the risk management process by identifying: (i) relevant threats to the organization or threats directed through third party entities; (ii) vulnerabilities both internal and external to the organization; (iii) the impact (*i.e.*, harm) to the organization and individuals that may occur given the potential for threats exploiting vulnerabilities; and (iv) likelihood that harm will occur. There are many risk assessment frameworks and guidance documents available, including industry-focused guidance. *See* the *Framework for Improving Critical Infrastructure Cybersecurity*, National Institute of Standards and Technology, February 12, 2014.

A. Due Diligence

After assessing the potential risks in a transaction and the firm or its client's risk management strategy, then due diligence begins. Due diligence activities start with conducting a security assessment of the vendor, evaluating the vendor's ability to manage its IT infrastructure and operations consistent with cybersecurity objectives, and identifying past breaches and vulnerabilities in the vendor's systems. A security assessment of the vendor may be a direct assessment by the customer or its agent, review of vendor self-assessment or third-party assessment reports, or some combination of those activities. Qualified information security personnel should assist the customer to identify relevant areas of assessment and to evaluate the information provided by prospective vendors. A security assessment should consider, among other items, the extent to which the vendor:[22]

- Has adopted appropriate security policies and procedures, including written policies as necessary to create a "culture of security," and enforce its security procedures, particularly those most likely to prevent the most common types of data breaches;

- Has created appropriate incident response and business continuity or disaster recovery plans and tests and updates them regularly;

- Maintains a program to manage compliance with applicable laws and regulations, including those on data breach, data disposal, privacy and confidentiality of personal information and other protected data, as well as laws or regulations that restrict use of certain information without appropriate consent; and

- Addresses information security in a manner that enables the customer to demonstrate its compliance with applicable laws and regulations, considering controls that the vendor may provide the customer.

The customer should ask the following questions when assessing the vendor's program to maintain its IT infrastructure and operations consistent with cybersecurity objectives, including the customer's requirements:

- To what extent does the vendor implement and use software and hardware with security and privacy built into the design of the product?

- To what extent does the vendor assess the secure development practices of third parties supplying custom and critical applications?

- How does the vendor monitor its systems for known vulnerabilities and respond to newly-reported vulnerabilities?

[22] A complete security assessment guide is outside the scope of the Checklist. Parties should consult employees and advisors with appropriate security expertise.

- Does the vendor have a procedure to monitor vulnerabilities identified in authoritative sources and other threat intelligence?

- Does the organization adhere to practices of scanning software for vulnerabilities before it is installed and for avoiding implementation and use of software and hardware for purposes for which they were not designed?

- Where and when does the vendor encrypt data in its possession or control?

- Does it send any data over unencrypted channels?

Keep in mind, too, that to your client, you are also a vendor, and these same concerns and questions apply to your firm's security practices.

The vendor should be required to identify incidents or breaches and vulnerabilities in its IT systems (including systems provided to it or hosted by third parties) and its plans for recovery or remediation. The information requested from the vendor should be reasonable under the circumstances and tailored to the type of product or service the vendor will provide. Customers should implement closer scrutiny when the vendor will have access to sensitive customer/client data or personal information, provide a product that affects the security of an organization broadly, or will be a key part of the customer's critical infrastructure. If a vendor is not willing to provide the requested information, consider what assurances the customer should request about how the vendor manages vulnerabilities and incidents, generally. In this context, the parties may also have an interest in knowing about their counterparties' experience in matters involving law enforcement or regulatory authorities as well as communication plans and infrastructure in place to communicate if/when an incident occurs.

B. Due Diligence Questionnaires

Customers may consider using standardized questionnaires or accepting standardized questionnaire responses from the vendor. The following are tools for assembling standardized due diligence questionnaires that customers can adopt or modify:

- Standardized Information Gathering questionnaire (behind paywall)[23]:Guidance to those selecting potential Cloud Service Provider (CSPs) vendors, gathering information regarding how security risks are managed across 18 domains within a CSP's environment, including information technology, resiliency, cyber security, data security and privacy. Using a single standard like this streamlines CSP vendor assessment.

- National Credit Union Administration Guidance:[24] Guidance to credit unions for assessing third-party risk; explanations and additional information follow checklist.

[23] https://sharedassessments.org/sig/

[24] https://www.ncua.gov/files/letters-credit-unions/LCU2008-09ENC.pdf

- Federal Deposit Insurance Corporation Guidance:[25] General framework for boards of directors and senior management to provide appropriate oversight and risk management of significant vendor relationships. Management should consider the principles addressed and ensure that appropriate procedures are in place, considering the complexity and risk potential for each of its third-party relationships.

- Federal Financial Institutions Examination Council Handbooks:[26] High-level guidance for financial institutions doing due diligence on service provider's RFP response as well as the provider itself.

- NIST Cybersecurity Framework:[27] This framework, updated in 2018, now includes provisions for assessing the cybersecurity risk posed by vendors, and considerations for vendor risk management.

- NIST Key Practices in Cyber Supply Chain Risk Management: Observations from Industry.[28] This publication is based on an analysis of interviews with 24 companies and a number of standards and industry best practice documents.

- NIST Integrating Cybersecurity and Enterprise Risk Management (ERM).[29] Published October 2020, this document provides additional guidance regarding cyber supply chain risk management.

- NIST SP 800-30, Rev. 1, Guide for Conducting Risk Assessments, updated December 14, 2020.[30] This guideline focuses on conducting risk assessments of federal information systems and organizations, and on identifying specific risk factors that should be monitored on an ongoing basis to avoid exceeding organizational risk tolerance.

Vendors should be prepared when their customers and potential customers request responses to questionnaires. A vendor may already have certifications or assessments relating to its cybersecurity or privacy programs. These certifications or assessments can serve as useful information about the information security measures that the vendor has implemented and may make due diligence more efficient. A list of certificates and attestations are available in **Appendix I**.

Receipt of a vendor's risk assessment certification does not mean your job is over: as the saying goes, trust, but verify. The greater the number (transactions per day) and depth (how many users) of digital interactions and the greater the sensitivity of the data, the greater the risks for something

25 https://www.fdic.gov/news/financial-institution-letters/2008/fil08044a.html
26 https://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services/risk-management/service-provider-selection/due-diligence.aspx.
27 https://www.nist.gov/cyberframework.
28 https://csrc.nist.gov/publications/detail/nistir/8276/draft.
29 https://csrc.nist.gov/publications/detail/nistir/8286/final.
30 https://www.nist.gov/privacy-framework/nist-sp-800-30 (although the NIST page references the January 16, 2020, update, the download button still brings up the September 2012 version).

to go wrong. Whether you are representing your own interests or those of your client, it is worth the time to take any vendor's certification and respond with a request for specific responses to the issues or concerns that may be unique to the business.

The due diligence questionnaire (and the vendor's responses) will also help to inform you when a cyber incident occurs.[31] Having a due diligence questionnaire in which your organization has inserted its own responses will also serve as a starting point when clients start asking for due diligence information.

C. Relevant Ethics Rules

"Lawyers must take competent and reasonable measures to safeguard client information."

Lawyers must take competent and reasonable measures to safeguard client information. These duties provide minimum compliance standards, and safeguards should be included in a comprehensive security program. You should consider the following ABA Model Rules in assessing risks posed by vendors in the cyber world.

Model Rule 1.1 covers the general duty of competence, requiring "competent representation to a client."[32] This requires "the legal knowledge, skill, thoroughness, and preparation reasonably necessary for the representation,"[33] including in selecting and using technology, including cybersecurity. Attorneys who lack such must either learn it or consult with qualified people who have the requisite expertise. To maintain competence, a lawyer should keep abreast of the benefits and risks associated with relevant technology.[34] A lawyer also has the ethical duty "to take special security precautions to protect against the inadvertent or unauthorized disclosure of client information."[35]

Model Rule 1.4 requires appropriate communications with clients "about the means by which the client's objectives are to be accomplished," including technology use. It requires keeping the client informed, sometimes obtaining 'informed consent,'[36] and notifying a client of actual or suspected unauthorized access to or disclosure of their material confidential information, e.g., theft of or a ransomware attack on the client's information. The lawyer should also inform the client of the extent to which information was accessed or that the extent is unclear. The notice must be sufficient to allow a client to decide how to respond. ABA Formal Opinion 483 separately discusses whether and when to disclose the breach to law enforcement.[37]

---

31 See Chapter 14, Best Practices for Incident Response in ABA Cybersecurity Handbook, (Jill Rhodes, Robert S. Litt, ed., 2d Ed. 2018) for more details on incidence response and remediation measures.

32 Model Rules of Prof'l Conduct R. 1.1.

33 *Id.*

34 *Id.* at cmt 8.

35 ABA Formal Opinion 477R (May 22, 2017). Following the lead from Model Rule 1.1, and Opinion 477R, the ABA issued Formal Opinion 483 *infra* at note 36, which focused on "an attorney's ethical obligations when a data breach exposes client confidential information."

36 Model Rules of Prof'l Conduct R. 1.4.

37 ABA Formal Opinion 483 (October 17, 2018).

Model Rule 1.6 relates to confidentiality, requiring protection of "information relating to the representation of a client…"[38] Disclosure of covered information generally requires express or implied client consent. The rule provides, "A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client,"[39] and comments with factors for determining the reasonableness of the lawyer's efforts.[40] [41]

Model Rule 1.15 requires lawyers to segregate and protect client and third-party money and property held by the lawyer.[42] Some bars have extended this rule to electronic data.

Model Rule 5.3 requires lawyers to employ reasonable safeguards, like due diligence, contractual requirements, supervision, and monitoring, to ensure that non-lawyers provide services in compliance with a lawyer's ethical duties, including confidentiality.[43]

D. Data Security Planning

Given the ethical rules and business prudence, you should adopt a data security plan. This goes beyond mere measures like firewalls and passwords and adopts a, "fact-specific approach to business security obligations that requires a 'process' to assess risks, identify and implement appropriate security measures responsive to those risks, verify that the measures are effectively implemented and ensure that they are continually updated in response to new developments."[44] A data breach occurs when "material client confidential information is misappropriated, destroyed or otherwise compromised or where a lawyer's ability to perform the legal services for which the lawyer is hired is significantly impaired by the episode."[45]

---

38 Model Rules of Prof'l Conduct R. 1.6.

39 *Id.* At R. 1.6(c).

40 Model Rules of Prof'l Conduct R. 1.6, cmt 18. Factors include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).

41 At least one state, California, has already tried to further clarify "reasonable efforts." California's then-Attorney General Kamala Harris stated in California's 2016 Data Breach Report that "[the Center for Internet Security's Top 20 Critical Security Controls] are the priority actions that should be taken as the starting point of a comprehensive program to provide reasonable security." The report went on to state that "[t]he failure to implement all the Controls that apply to an organization's environment **constitutes a lack of reasonable security**." (Emphasis added.) See California's 2016 Data Breach Report, available at https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf. CSC 20 is located at https://www.cisecurity.org/controls/cis-controls-list/. In addition, California state law requires a business to disclose to any resident a data breach involving unencrypted personal data [California Civ. Code s. 1798.82(a)]. New York and Oregon have passed similar but not identical policies. Bailey Sanchez, The evolution of the 'reasonable security' standard in the US context, IAPP (Jun. 4, 2020), https://iapp.org/news/a/the-evolution-of-reasonable-security-derived-from-ftc-orders-and-state-legal-developments/

42 Model Rules of Prof'l Conduct R. 1.15.

43 Model Rules of Prof'l Conduct R. 5.3.

44 *Id.*, quoting ABA Cybersecurity Handbook, *supra* note 9, at 73.

45 ABA Formal Opinion 477R, *supra* note 35.

Lawyers must employ reasonable efforts to monitor for a breach of their technology resources connected to the internet, external data sources, and external vendors providing services relating to data and its use.[46] There is no ethical violation if a potential breach or breach is not immediately detected. A violation occurs if there is failure to take reasonable efforts to prevent and detect a breach, and a breach results. In the event of a breach, a lawyer must act promptly and reasonably to ensure the intrusion has been stopped and to determine any data intrusion and loss, addressing confidentiality obligations and mitigating damages.[47] A key step is developing an incident response plan tailored to the size of the firm and the data and systems needing protection. It should designate an incident response manager, procedures for initial reporting of an incident, confirming the incident, escalation as appropriate, and post incident investigation. After a breach, a lawyer should also evaluate how to avoid a reoccurrence.[48]

i. For Small Firms

Solo and small firms should establish standards and protocols for use of office technology, such as cybersecurity training, and procedures for securing data and infrastructure. Existing frameworks can provide useful guidance; a list is available in **Appendix A**. An incident response plan is key to being able to address a data breach in a coordinated manner.

ii. Understanding Cybersecurity Risk

Numerous data breaches, both of small and high-profile firms,[49] have compromised sensitive and proprietary information, [50] and provided access to a whole law firm's network. A breach can

---

46 *Id.*

47 ABA Formal Opinion 483, *supra* note 37.

48 *Id.*

49 The 2016 "Panama Papers" email hack resulted in 2.6TB of data leaked. The data were sent to over 100 media outlets, resulting in a searchable database of over 214,000 offshore accounts, exposing world leaders, executives, celebrities, and more; Iceland's Prime Minister resigned, the firm closed offices and resigned as the registered agent for over 1,000 companies, and the Department of Justice launched a criminal investigation. *See* The Massive Panama Papers Leak Explained, Computerworld (April 5, 2016) http://www.computerworld.com/article/3052218/security/the-massive-panama-papers-data-leak-explained.html; Elida Moreno & Enrique Pretel, *Panama Law Firm Says Data Hack Was External, Files Complaint*, REUTERS (April 5, 2016) http://www.reuters.com/article/us-panama-tax-fonseca-idUSKCN0X3020; ICIJ releases database revealing thousands of offshore companies, https://panamapapers.icij.org/blog/20160509-offshore-database-release.html; Jane McCallion, Aaron Lee, Clare Hopping, Caroline Preece, *Panama Papers: Emma Watson named in leaked documents*, ITPRO (November 5, 2016), http://www.itpro.co.uk/data-leakage/26293/panama-papers-emma-watson-named-in-leaked-documents. Another more recent high-profile breach occurred in May 2020 to media and entertainment firm, Grubman Shire Meiselas & Sacks, available at https://variety.com/2020/digital/news/entertainment-law-firm-hacked-data-breach-lady-gaga-madonna-bruce-springsteen-1234602737/#! (last visited Dec. 16, 2020).

50 In 2016, three Chinese nationals were indicted for securities and wire fraud for hacking into prominent international law firms and trading on confidential, non-public information obtained from the e-mails of partners who worked on high-profile M&A transactions. *See* FBI Alert Warns of Criminals Seeking Access to Law Firm Networks (March 11, 2016), https://bol.bna.com/fbi-alert-warns-of-criminals-seeking-access-to-law-firm-networks/; *U.S. v. Iat Hong, et. al.,* 16 Cr 360 (S.D. N.Y. 2016).

destroy attorney-client privilege and protective orders preserving the secrecy of sensitive data,[51] and result in devastating consequences to data subjects, potentially subjecting them to identity theft, fraud, negative publicity, and even financial ruin. The reputational harm to a firm alone may result in lost business and ethics violations. [52]

a. New Technologies Create Unprecedented Challenges

Seeking efficiencies from new technologies, most lawyers and law firms use e-mail extensively, have smart phones, and work on laptops and tablets; courtrooms are relying on state-of-the-art computer devices; and how and where data are stored and processed varies significantly. Some firms are using cloud computing for storing and processing client and firm records, and some have implemented "bring your own device/technology" (BYOD) policies. With new technology comes new risk. And of course, with most businesses continuing to operate remotely throughout 2020 and into 2021, the risks posed by the business use of personal devices, home WiFi security (or not), and dispersed IT operations.

1) Internet of Things (IoT) in the Workplace.

Even solo and small firms may often utilize IoT devices such as security cameras, wireless locks, motion sensors, automated lighting and window shades, and climate control. The risks posed by IoT devices are many and varied. Because they are generally small, easy to manufacture and relatively inexpensive, manufacturers are loath to incorporate security into the design of the device because it will only drive up the price and they might lose their competitive advantage. The recent regulatory movement is aimed at leveling the playing field by requiring the incorporation of security into the design of the device, but success in that effort is not yet verified. For now, be cautious about any IoT device that will want to automatically connect to your IT network—be it at home or at your business location.

2) Legal Outsourcing.

It is common practice for law firms to outsource various administrative, accounting, and other services.[53] Law firms and legal departments are now also increasingly practicing legal process

---

51 See FRCP 26(c)(7), allows a court to issue an order that "a trade secret or other confidential research, development, or commercial information not be revealed or be revealed only in a designated way."

52 Chapter 4 provides an in-depth discussion of the responsibilities of lawyers to protect sensitive and confidential information.

53 Deloitte Consulting LLP, 2016 Global Outsourcing Survey - Outsourcing accelerates forward (June 2016), *available at* https://www2.deloitte.com/content/dam/Deloitte/fi/Documents/technology/2016%20GOS%20Exec%20Summary_Nordic.pdf.

outsourcing.[54] Even small firms retain and spend large dollars on e-discovery services and forensic investigations is used to hire outside vendors.

To hackers, law firms are "business partners" of major corporate clients, with troves of proprietary data, providing a pathway into companies of strategic interest.[55] Similarly, it can be said that a law firm is only as secure as its weakest business partner. It is important to assess the security practices of all business partners—even those with sterling credentials.

3) Mobile Devices

With the ubiquity of mobile devices, security concerns continue to mount. While these devices are essential to our productivity, they by design present numerous risks. They are often lost or stolen, and the data on them may be accessed easily; many use weak or no passwords. Experts have identified three relevant "attack surfaces:"

- *the device itself*: the device may be stolen, its data may be stolen, and various sensors such as the camera and microphone may be surreptitiously activated.[56] In addition, the device itself may be a tool of espionage. For example, on December 10, 2020, the FCC began the process to revoke the authorization of China Telecom to operate in the U.S. due to "significant concerns" that its devices will intercept communications.[57]

- *the operating system*: the operating system (OS) may be faulty, preboot Trojans (malware that affects preboot operations) may "jailbreak" its precautions, [58] or it may permit weak passwords.

- *the external service providers*: provider failures cover failure of IT management, malicious application injection, and data theft. Hackers can also insert malware into Apps so when users download them hackers can access sensitive information, launch man-in-the-middle attacks), and inject new messages between parties. The Federal Trade Commission (FTC) has brought several cases against companies for marketing mobile devices and software with security vulnerabilities or that exposed personal data without consumers' knowledge.[59]

---

54 Chambers and Partners, Legal Process Outsourcing – Global Wide, *available at* http://www.chambersandpartners.com/15649/1783/editorial/2/1; Top 3 Trends to Watch in Legal Outsourcing (2016); The Huffington Post, *available at* http://www.huffingtonpost.com/robert-gogel/top-3-trends-to-watch-in_b_10856942.html .

55 Intelligence Center Report, APT1, *Ibid.*

56 Often mobile device users do not realize that when accepting certain application policies during loading, these include the right to turn on a camera and/or microphone.

57 David Shepardson, FCC begins process of halting China Telecom U.S. operations, Reuters (Dec. 10, 2020), https://www.reuters.com/article/usa-china-tech/fcc-begins-process-of-halting-china-telecom-u-s-operations-idUKKBN28K2ER.

58 Installing software on a phone to "break open" the phone's OS security and allow a user to modify anything it protects. This is a well-known form of privilege escalation that usurps OS isolation assumptions.

59 FTC Mobile Technology Issues, *available at* https://www.ftc.gov/news-events/media-resources/mobile-technology.

Over the last decade, more than one-third of data breaches resulted from the theft or loss of portable media containing unencrypted personal information.[60] Widely publicized breaches illustrate the sheer magnitude of the exposure of personal records and the potential damage to millions.[61] [62] The consequences are particularly serious if the mobile devices are used to communicate with legal clients or to view, process, or store confidential client data or information. The small firm lawyer should attempt to prevent breaches with encryption, enforcing procedures banning the transport of sensitive data on moveable media, carefully tracking the devices and monitoring and management of applications, and having the highest standards and requirements for commercial couriers.

4) BYOD Policies

Studies show BYOD policies may not always be cheaper in the end for organizations seeking to reduce costs and accommodate a new generation of lawyers, and they carry significant responsibilities from both an information governance and technical perspective.[63] There are several key steps a law firm should take to protect confidential data. First, where possible, use mobile device management, which provides a centralized way to manage mobile devices remotely, including, significantly, the ability to lock or erase a lost device remotely, and check its geographic location. Second, only known users, known devices, and vetted app providers should be permitted on the network, and not phones that have been jailbroken or rooted. Finally, phones and tablets used to create, transmit, or store sensitive data, should have centralized password management with acceptable password policies, and all user data should be encrypted. Such management software is readily available from many vendors.

5) Cloud Computing and Wi-Fi

Because of the increased flexibility and efficiency afforded by on-demand computing resources, law firms are using cloud services for processing and storing confidential client data and records. Cloud computing can introduce risk by outsourcing the administration and physical control of sensitive data to a third-party, and maintenance of the data on shared computing platforms. These risks should be carefully evaluated and addressed when using the cloud to store client data.[64] In all instances, cloud service providers should be considered public repositories. Law firm and client

---

60 DataLossdb, Data Loss Statistics, *available at* http://datalossdb.org/statistics.

61 *Id.* TriCare-SAIC (4,600,000 records breached); Bank of New York Mellon (4,500,000 records); Sutter Physicians Service and Foundation of California (4,200,000 medical records breached); Educational Credit Management Co. (3,300,000 records breached); and Jacobi Medical Center NY (1,700,000 medical records breached).

62 Mark Iandolo, Horizon Healthcare Services settles data breach case for $1.1 million, Legal Newsline (March 1, 2017), *available at* http://legalnewsline.com/stories/511085361-horizon-healthcare-services-settles-data-breach-case-for-1-1-million.

63 Stephen Wu, *A Legal Guide to Enterprise Mobile Device Management: Managing Bring Your Own Device (BYOD) and Employer-Issued Device Programs* (ABA). This book examines the legal and practical implications of this trend and highlights future challenges for organizations in both the U.S. and internationally. NIST Spec. Pub. 800-124 Rev. 2 (Draft), Guidelines for Managing the Security of Mobile Devices in the Enterprise (March 2020), *available at* https://csrc.nist.gov/publications/detail/sp/800-124/rev-2/draft.

64 See, NIST Spec. Pub. 800-144, *Guidelines for Security and Privacy in Public Cloud Computing, available at* http://dx.doi.org/10.6028/NIST.SP.800-144.

"Law firm and client data should be encrypted both in transit (as it is uploaded and downloaded) and at rest (while it is stored)."

data should be encrypted both in transit (as it is uploaded and downloaded) and at rest (while it is stored). There are many options for cloud service providers, and it often falls to counsel to review the provider agreement, so it's best to review the risk issues highlighted in this Checklist. There are good online resources for comparing options as well.[65]

Wireless communication also creates opportunities for hackers to intercept sensitive data, like passwords. Public WiFi and private home locations rarely have security features necessary to protect confidential client data, and hackers can use proxy servers to create fake hotspots and intercept or redirect confidential communications. Thus, data encryption is critical. Another common tool that is available to both individuals and enterprises is a Virtual Private Network ("VPN"), which provides a secure "tunnel" to transmit and receive data.[66]

iii. Information Security

a. Protecting the Confidentiality, Integrity, and Availability of Data

Most breaches are preventable. Just as people and entities protect their physical assets, information security must be an integral part of any technology solution. Standards, guidance, and compliance tools for developing and implementing security plans are available.[67] Building strong information security programs that focus on protecting information confidentiality, integrity, and availability,[68] is not only good business practice, but also helps avoid the costs of data breaches, potential liability, negative press, embarrassment, and loss of trust.[69]

---

65 Top Cloud Providers in 2020, available at https://www.zdnet.com/article/the-top-cloud-providers-of-2020-aws-microsoft-azure-google-cloud-hybrid-saas/, last visited Dec. 16, 2020.

66 The Best VPN Service for 2020, available at https://www.pcmag.com/picks/the-best-vpn-services?test_uuid=001OQhoHLBxsrrMgWU3gQF&test_variant=a (last visited Dec. 16. 2020).

67 The various NIST and other governmental standards and guidelines are excellent resources and provide much more detail on accepted best practices. *See, e.g., Security and Privacy Controls for Information Systems and Organizations*, NIST Spec. Pub. 800-53, Rev. 5 (Sept. 2020, updated as of 12/2-20), *available* at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf. The various IT Security associations provide other resources. See e.g., www.sans.org. The ISO/IEC Information Security Management System (ISMS) family of standards are based on the governing principle that an organization should design, implement, and maintain a coherent set of processes and systems to manage risks to its information assets, thereby ensuring acceptable levels of information security, available at http://www.iso.org.

68 Supra at Protecting the Confidentiality, Integrity, and Availability of Data p. 26

69 The high costs of responding to data breaches in terms of expenditures for detection, escalation, notification and response, along with legal, investigative and administrative expenses, customer defections, opportunity loss, reputation management, and costs associated with customer support such as information hotlines and credit monitoring subscriptions, have been well-documented. For access to the Ninth Annual Cost of Cybercrime Study released by Accenture and Ponemon, *see* Bissell, Lasalle, & Dal Cin, Ninth Annual Cost of Cybercrime Study, https://www.acenture.com/us-en/insights/security/cost-cybercrime-study, March 6, 2019. As the notification requirements in the data breach laws become more stringent, increasing numbers of individuals who must be notified, and the liability imposed by courts and administrative agencies for data breaches increase significantly, these costs are likely to continue to rise.

1) Confidentiality:

The largest data breaches—spanning sectors—illustrate the heightened risk to millions of individuals when large datasets of sensitive personal information are compromised.[70] Database access vulnerabilities are well-documented and include using default and weak passwords, failing to patch known vulnerabilities, misconfigurations, and granting excessive privileges. Specific security measures to protect confidentiality are available.[71]

2) Integrity

It is critical to protect information against corruption, tampering, or other alteration, including safeguarding the accuracy and completeness of information, to prevent potentially devastating impacts on key information systems. [72]

3) Availability

Recently, attacks designed to restrict website and service availability have become more prevalent. These occur primarily with distributed denial of device (DDoS) attacks are used to overwhelm a single targeted system, [73] computer viruses that delete user data, or ransomware.

b. Who is responsible for Information Security?

Businesses, including law firms, should implement proactive measures at the highest level which flow down through the rest of the organization. Without managerial "buy in," there will be no incentive for the rest of staff to adopt appropriate technology and follow good security practices.

---

70 Capital One, the names of 106 million people who had applied for credit were exposed (2019); Facebook, use of third party apps exposed 540 million accounts (2019); First American, 885 million records with financial information (2019); Equifax, the credit agency breach involved the compromise of 143 million records (2017), Marriott Hotels, the breach affected 500 million people (2018), Yahoo, 1.5 billion user accounts compromised (2013 and 2014); e-Bay, 145 million records breached (2014); Target Stores, 110 million (2013); Anthem BlueCross BlueShield, 69-80 million (2015); Home Depot, 56 million (2014); and Office of Personnel Management (OPM), 22.5 million security clearance records, 5 million fingerprints (2015).

71 DHS National Cybersecurity and Infrastructure Security Agency, Insider Threat Mitigation Guide (November 2020), *available at* https://www.cisa.gov/sites/default/files/publications/Insider%20Threat%20Mitigation%20Guide_Final_508.pdf.
Specific security measures that should be taken to protect personal data include: (1) Inventory your databases; (2) Classify systems with sensitive data; (3) Scan for vulnerabilities and misconfigurations, keep up-to-date with security patches, enforce strong passwords, and audit configurations and settings; (4) Identify privileged users (DBAs); (5) Validate access to sensitive data; assign restricted permissions on tables with sensitive information; (6) Prioritize and fix what you can; (7) Monitor database activity; and (8) Encrypt data in-transit and at-rest using network-level encryption and column-level encryption.

72 The Honorable James R. Clapper, Director of National Intelligence, Statement for the Record to the Senate Armed Services Committee, Worldwide Threat Assessment of the U.S. Intelligence Community (Feb.9, 2016), pages 1-2, *available at* https://www.intelligence.senate.gov/sites/default/files/wwt2016.pdf.

73 Malware disguised as legitimate software that will enable a cyber-criminal to gain access to a user's system and spy on them, steal sensitive data, and gain backdoor access.

c. Embracing a Risk Management Framework

1) Security by Design

"…security must be incorporated into the architecture and design of the organization's information systems and supporting IT assets, also known as* security-by-design*."

To properly support an organization's risk management framework, security must be incorporated into the architecture and design of the organization's information systems and supporting IT assets, also known as *security-by-design*.

Information security results from the systematic assessment of the threats and risks present in an information system. Risk assessments are undertaken to identify gaps and deficiencies in a cybersecurity program due to operational changes, new compliance requirements, an altered threat environment, or changes in the system architecture and technologies deployed. Risk analysis should be an ongoing process including regular record review to track access to confidential records and detect security incidents, periodic evaluation of the effectiveness of security measures put in place, and regular reevaluation of potential risks to sensitive and confidential information. Resources including a common vocabulary and a scalable framework are available with the NIST Framework.[74]

The risk management process includes the following:

- Evaluating the likelihood and impact of potential risks to sensitive and confidential information;
- Implementing appropriate security measures to address the identified risks;
- Documenting the chosen security measures and, where required, the rationale for adopting them; and
- Maintaining continuous, reasonable, and appropriate security protections.

This process informs decision-makers and supports risk response by identifying:

- relevant threats to firms or threats directed through outside organizations against them;
- vulnerabilities both internal and external to the law firm;
- impact to the firm and its clients that may occur given the potential for threats exploiting vulnerabilities; and
- likelihood that harm will occur.

---

[74] NIST *Framework for Improving Critical Infrastructure Cybersecurity, ver. 1.1* (April 16, 2018), *available at* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. Additional NIST resources to implement the framework can be found at https://www.nist.gov/cyberframework.

Then, appropriate security controls can be selected, implemented, and continuously monitored to reduce risks and vulnerabilities to a reasonable and appropriate level. Security-by-design includes constant monitoring of systems, security status, and risks to protect against the broad range of serious threats to information systems.[75]

Continuous monitoring is designed to provide meaningful, actionable intelligence and reporting, rather than mere data collection. Robust continuous monitoring will provide the information necessary to make cost-effective, risk-based decisions.[76] Cybersecurity situational awareness informs firms of threats, vulnerability, and the compliance posture of the system, and provides information about incidents needing investigation, enabling a highly proactive security posture.

3. Contract Provisions – Setting Expectations, Mitigating Risk, and Allocating Liability

A. Definitions.

First in reviewing a vendor contact is defining key terms related to information security, e.g., "confidential information," "cyber incident" or "security" incident," and "data breach."[77.] In reviewing a vendor's definitions, consider whether the vendor defines malware or similar concepts like "harmful code" which cover, in addition to viruses, other undisclosed functionality (e.g., backdoors, self-help tools, remote access, and ransomware). In defining vulnerability,[78] consider features or functionality that by design could also be vulnerabilities—like SolarWinds' remote monitoring feature that subsequently allowed hackers to get an "inside" view of various federal agencies' computer systems.

---

75 The SANS CIS Critical Security Controls: Guidelines provide guidance to maximize the impact of government and private sector security efforts, and identify critical priority controls, most of which can be continuously monitored. Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines, v. 7.1, *available at* https://www.sans.org/critical-security-controls/ (the website provides a wealth of valuable information about the leading information security methodologies and how they relate to each other).

76 NIST Spec. Pub. 800-37, Rev. 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* (Jan. 16, 2020), *available at* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf.

77 Consider the distinction between "incident" and "breach" illustrated by The Health Insurance Portability and Accountability Act of 1996 (HIPAA) definitions. HIPAA regulations define "security incidents" as "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system." 45 CFR § 164.304. The breach notification rule in HITECH defines breach as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under [the HIPAA Privacy Rule] which compromises the security or privacy of the protected health information . . . ." (See the definition of "breach" at 45 CFR § 164.402.) "Incident" is broader in that it covers attempts as well as actual compromises.

78 The NIST *Glossary of Key Information Security Terms* (Rev. 2 May 2013) presents a few definitions of "vulnerability," including these: "Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source" and "A weakness in a system, application, or network that is subject to exploitation or misuse." (Internal citations omitted.)

B. Understanding the Product or Service.

How does the nature of the product or service implicate information security? Consider you or your client's responsibilities in the transaction, such as what responsibility might your client have regarding the configuration of the vendor's services. A common source of cyber risk occurs with the misconfiguration of a vendor's product or service.

Customers should also consider what steps will be taken to monitor the role of third parties to the vendor. The customer might review the vendor's vendor management program or insist on direct access to the downstream vendor for review and monitoring as well as being identified as a third-party beneficiary of subcontracts. The approach taken should be commensurate with the significance of the third party's role.

i. How will the contracting parties interact, share, and manage information? For what reasons will the vendor have direct access to the customer's systems, e.g., maintenance and support?

ii. Does the vendor need, or will it be given permission to use, the customer's information, technology, and intellectual property? If so, will the vendor be authorized to allow its affiliates, subcontractors, and suppliers to have access, and subject to what conditions? What legal assurance will the customer have that the vendor manages any downstream sharing effectively?

iii. What records, data, information, and analytics will the vendor create during the term of the contract and who will own them? Who will have access to those records? Does the vendor intend to make any secondary usage of such? Where will those records be located? On what terms and through what channels will the customer or its representatives have access to those records?

iv. Where will products be manufactured, or services performed? Location considerations may include continuity and infrastructure risk, political risk, and security risk. Also consider third parties critical to the vendor's products and services. If the customer operates subject to regulatory restrictions on foreign service providers, for example, those restrictions should be addressed with respect to the vendor's subcontractors and suppliers. If data will flow across borders, consider need for a Data Transfer Agreement to comply with foreign privacy laws.

C. Representations and Warranties.

The sample representations and warranties below are representative of the issues you should address on behalf of your client. As always, each party needs to consider in its particular circumstances what is acceptable.

i. No recent security incidents/breaches not disclosed to the customer.

This representation implies that the vendor has provided relevant information during the vendor selection and due diligence process. Use of "incident" or "breach" will be informed by their definitions and may be qualified with an appropriate materiality standard.

ii. No claims threatened or pending, or events or circumstances known to the vendor likely to give rise to claims because of any security incident or vulnerability.

iii. No regulatory actions threatened or pending, or events or circumstances (noncompliance) known to the vendor likely to give rise to regulatory action because of any security incident or vulnerability.

iv. No processing, storage, or transmission of customer's information by third parties not disclosed to customer.

Alternate example: *Vendor's information storage and handling procedures comply with relevant sector-specific laws as applicable.*

This will be complicated if the vendor uses cloud services for processing or storage. The vendor will have to consider the cloud provider's operations.

v. Vendor has all licenses and certifications required by applicable law to provide the product/ perform the service.

Consider licenses and/or certifications that may be required for handling the customer's information, if any. See **Appendix I for further information on this topic.**

vi. Vendor has all rights necessary to provide the product, software, and data and other information, and perform the service as contemplated by the contract. If vendor licenses any software, data, or other content necessary to perform a service for customer, vendor's licenses authorize vendor to use the licensed material to perform the service for third parties.

Information about the maturity of the vendor's business procedures to manage its products and third-party content could indicate its maturity in other aspects of its business, including cybersecurity.

vii. Vendor has a data or information security program in place as required by the agreement [cross-reference the relevant section].

Alternate example: *Vendor has identified no deficiencies in its information security program when measured against [contract requirements – appropriate internal cross-reference] that have not been disclosed to the customer and accepted or are*

the subject of an appropriate plan of action and milestones to remediate in a manner acceptable to customer.

viii. Vendor employs personnel qualified to maintain the information security program.

If the vendor outsources information security activities, the customer should receive notice if the vendor changes providers and is entitled to validation that the new provider is the same or better.

ix. Vendor handles information collected from customer (or customer's customers) consistent with the practices for information handling described in policies and procedures, including its privacy policy and other terms posted on its website or otherwise published to users.

x. Vendor's responses to customer's information security due diligence questionnaire are true and complete as of the date made and as of the date of the agreement.

As with any representation about the veracity of information, the parties should consider how to address the time lapse between when responses are provided and when the representation is made. The customer should also consider a corresponding undertaking by the vendor to update the information security questionnaire or otherwise provide similar information periodically during the term of the agreement.

If the customer identifies deficiencies in any part of the vendor's responses, they should be accounted for either by acceptance (which may entail additional controls established by the customer) or with an undertaking by the vendor to remediate against an agreed plan of action and milestones. The latter should be documented in the agreement. The parties should be mindful of limiting information in the agreement's text about deficiencies and remediation, e.g., referencing a plan of action and milestones that bears indicia of acceptance, but not attaching or restating the plan directly in the agreement, can help limit specific vulnerability details to those who need to know them.

D. Data Ownership and Access and Use Rights.

Data can be digital gold. If you own it, you can monetize it. If your client transmits its data directly to the vendor or the vendor collects data on the client's behalf, what rights does the vendor have in the data? Do the vendor's rights in the data reflect the pricing discount it is willing to give your client? Will the vendor be able to access or use the data for its own commercial purposes? These questions require a careful consideration of circumstances under which the vendor will require access to the data to keep it secure or to perform its duties. Given lawyers' ethical, legal, and contractual obligations to safeguard data, you will likely want to take care to maintain ownership of data and limit the vendor's rights. In some instances, more specific laws may apply. For example, in the California Consumer Privacy Act (CCPA),[79] a "Service Provider" vendor must limit the use of personal information "on behalf of the business that provided the personal

[79] Cal. Civ. Code § 1798.140.

information," and is specifically prohibited from building or modifying consumer profiles to use in providing services to other businesses or correcting or augmenting data acquired from another source.

E. Confidentiality.

Parties should consider the nature of the information to be exchanged or collected and relevant data protection laws, including lawyer's obligations with respect to protect client information. It may be necessary or appropriate to supplement a general confidentiality provision with a data privacy provision to cover more detailed requirements.

i. Mutual. Do both parties have confidential information of the other? Do all provisions apply equally and reasonably to both parties?

ii. Scope. Define confidential information in the possession or control of each party, where "control" encompasses information entrusted by the receiving party to any third party. The parties also should address scope of confidentiality applicable to data generated by the performance of the agreement.

iii. PII. Will the vendor collect, store, process, or transmit PII? From what jurisdiction(s) does the PII originate and where will it be stored? For a sample provision covering PII see **Appendix E**.

iv. Permitted uses of confidential information. Generally, confidential information should be used only as necessary to perform the service, furnish the product, and administer the agreement. If other uses are permitted, under what conditions and how will those other uses be monitored?[80] The parties also should address the use of data created by the performance of the agreement.

v. Storage & Communication. Restrictions on location, notice of storage in any location not previously disclosed; and *encryption.*

vi. Sharing with affiliates and downstream vendors/subcontractors. Under what circumstances and subject to what conditions? How does the vendor track and manage information provided to its subcontractors and service providers and flow-down requirements in customer contracts and other applicable law? How will the vendor provide assurance of compliance by downstream recipients? The same

[80] Note that under certain laws, such as the California Consumer Privacy Act, the failure to limit the vendor's use of data to performance of the contract could impact the parties' rights and obligations. *See* subsection (G)(i) below.

questions apply with respect to vendor confidential information given to the customer.

vii. Customer-supplied information and "record information," i.e., information accumulated about customers or as a byproduct of the customer relationship –

viii. Return/destruction obligation at the end of contract term and at other times at the disclosing party's request. No vendor should be allowed to retain PII forever, especially after the contract has ended (in some jurisdictions the perpetual retention of PII after it is no longer required violates applicable privacy laws). Requests made other than at the end of the term or following a breach should be conditioned so that the disclosing party cannot use the provision to impair the performance of the recipient or deprive the recipient of the benefit of the contract.

ix. Exceptions to return – Will the disclosing party agree to exceptions, such as for information stored in secure back-up in a manner that makes destruction of specific customer information impractical or commercially unreasonable? Is the information subject to a litigation records hold? If laws or regulations require the vendor to maintain the records? Many laws and regulations require entities to destroy, dispose of, or otherwise make personal information and business records unreadable or undecipherable.

x. Incident management. If an incident or breach occurs, then steps to manage confidential information should be taken. (*See below*, Section 3(I), Cyber Incident Reporting).

a. *Duration of confidentiality obligation* – indefinite (if a party is in possession or control of the other party's confidential information). If a confidentiality obligation is defined, the disclosing party must take steps to confirm that the recipient returns or destroys the information before the obligation expires. Failure to do so would be equivalent to permitting unrestricted use and disclosure at the end of the confidentiality period. (*See below*, Section 3(J), Remedies.)

xi. Encryption. One part of protecting confidential information that is provided to the vendor is encryption. Encryption is the process of converting data into an unintelligible form, decipherable with a typically secret key. The reverse is called decryption. Encryption may be used to perform confidentiality, data integrity, authentication, authorization, and non-repudiation. Data at-rest encryption protects data stored or recorded on computers and storage devices; vendors should employ it to protect their own sensitive data as well as data provided to them. Data in-motion encryption protects the confidentiality of data as they move between networks or devices. Sender and recipient agree to establish a unique key to be used for each

communication session. NIST provides extensive background on managing keys. See **Appendix C**.

F. Security Program.

You or your client should seek to contractually obligate the vendor to establish and maintain a comprehensive security program commensurate with the consequences and risk of loss, misuse, and unauthorized access to or modification of information. As noted previously, security programs are not "one-size-fits-all." Regulators for various sectors and at different levels of government have published guidance on security plans, including NIST.[81] (*See also* Appendix D, NIST Key Areas in a Security Program.)

The level of specificity for security controls in any contract will depend on factors such as the nature of the transaction, the level of sensitivity of the data being protected, the specificity of applicable legal requirements, the likelihood and magnitude of the risks to data, the size and sophistication of the parties, the parties' information technology infrastructure and capabilities, the cost of security controls, and the available resources to protect data. As a baseline, most likely you will want to establish a general requirement for the vendor to implement and maintain administrative, physical, and technical safeguards to protect customer data. For instance, you may want to tailor the following sample clause to your transaction:

When providing the Services to [Customer], [Vendor] will maintain a written information security program of reasonable and appropriate administrative, physical, and technical safeguards to:

- Ensure the confidentiality, integrity, and availability of Customer Data stored within, or transmitted to or form, vendor's information processing facilities;

- Protect against reasonably anticipated (i) threats or hazards to the security or integrity of the Customer Data or the Services, and (ii) unauthorized access to, or uses or disclosures of, Customer Data; and

- Ensure compliance with all applicable laws by [Vendor's] Vendor's officers, members, employees, contractors, subcontractors, and agents, including but not limited to laws relating to the security or privacy of Customer Data.

This general provision covers all three of the main areas of information security controls – administrative, physical, and technical safeguards. Information security professionals often define information security as protecting the "confidentiality, integrity, and availability" of data. This general provision covers all three objectives. This provision is also consistent with many of the

[81] See, e.g., *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*, NIST SP 800-171, rev 2 (Feb. 2020), *available at* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf. *See also*, ABA Cybersecurity Handbook, *Supra* note 9, at Appendix E.

security requirements in cybersecurity laws such as HIPAA. Finally, the provision calls for compliance with applicable laws, which may require additional controls.

For higher risk transactions, this general provision is helpful but may be insufficient. Customer clients may want to impose specific security compliance requirements that go beyond the general requirements in the provision above. While the general language above arguably encompasses specific security controls helpful for any high-risk transaction, customer clients will often believe that a specific contract provision is important to make expectations clear and establish a minimum set of specific controls. For example, you may want to consider addressing the following specific subject matter for security program obligations:

i. Physical controls and administrative, management, technical, and logical controls.

ii. Vulnerability management – monitoring for threats,[82] and response and remediation procedures.

iii. Software management – program for assessing risk associated with vendor or third-party applications. Does vendor follow secure development practices for internally-developed software? Does vendor assess secure development practices of third parties supplying custom and critical applications?

iv. Infrastructure maintenance – regular patching and other maintenance activities to protect systems and keep the infrastructure operating at committed service levels. Are maintenance activities prioritized to consider information security risk as well as operational risk/performance?

v. Personnel – qualifications of employees with cybersecurity responsibilities and systems/data access; policies and training; and an insider threat program including monitoring and enforcement, background investigations, segregation of duties, and least permissions/privilege protocols for systems/information access.

vi. Compliance with specific law or regulatory requirements.[83]

vii. Threat assessment/intelligence monitoring – vendor procedures to monitor dynamic threat environment.

The customer should also consider its own activity to monitor third-party intelligence about vendor products and services used by customer.

---

82 DoD Vulnerability Disclosure Policy, hackerone, https://hackerone.com/deptofdefense?type=team (last updated Jan. 28, 2021).

83 E.g., HIPAA/HITECH if handling personal health information, GLBA 501(b) if handling information for financial institutions, and PCI DSS for handling credit card information, and international laws and regulations as applicable for non-U.S. operations and non-U.S. customers.

viii. Change management – change management procedures for relevant vendor systems; notification of changes that could affect security assessments.

You should coordinate any needed specific security controls with your firm or client and their supporting information security professionals.

Frequently, contract drafters collect these specific security controls and place them in a security or data protection exhibit or appendix to a contract. The provisions that should appear in an exhibit or appendix will depend on the transaction. Nonetheless, you may find that controls in the common security frameworks mentioned above (NIST Cybersecurity Framework, ISO 27001 series, and CIS Critical Security Controls) may assist you and your client in determining which requirements to add to an exhibit or appendix.

G. Privacy.

A customer should review a vendor contract to determine if it complies with one of the two currently applicable laws regulating the privacy of specific consumer information. More laws and regulations are likely soon, and you should ask potential vendors about compliance with other laws as well.

i. California Consumer Protection Act ("CCPA") of 2018 and the California Privacy Rights Act of 2020

CCPA became effective January 1, 2020 and expanded by a ballot initiative entitled the "California Privacy Rights Act" ("CPRA") on November 3, 2020. Although the CPRA will not enter into force until January 2023, many its provisions will have a "look back" to January 1, 2022.[84]

There are a variety of actors under the CCPA, including "service providers,"[85] "third parties,"[86] and "consumers."[87] When drafting and negotiating contracts, if these California laws are applicable, it is important to understand their definitions and the relationship between the roles that define their obligations.[88]

---

84 These provisions are (1) extension of the employee exception and business-to-business exception to Jan. 1, 2023; (2) establishment of a Consumer Privacy Fund; (3) direction for the California attorney general "to adopt regulations and the mechanisms to transfer regulatory authority" to the state's new enforcement agency, the California Privacy Protection Agency ("CPPA"); (4) creation of the CPPA, "vested with full administrative power, authority and jurisdiction to implement and enforce the CCPA, as amended by the CPRA"; and (5) funding for the CPPA, which is expected to be approximately $10 million.

85 See California Consumer Privacy Act, §1798.140(v).

86 *Id.* At §1798.140(w).

87 *Id.* At §1798.140(g).

88 For example, if your "business" client does not qualify as a "third party," your business client will benefit from certain liability protection by adding restrictive language in its contract with the service provider. The business would also need to obtain a certification that the recipient service provider both understands and will comply with these restrictions. A sample clause might be drafted as follows: *[Company] is a Business and [Vendor] is a Service Provider for purposes of the CCPA. [Vendor] shall not: (a) sell the Personal Information; (b) retain, use or disclose the Personal Information for any purpose other than for the specific purpose of performing the Services; (c) retain, use, or disclose the Personal Information for a commercial purpose other than providing the Services; or (d) retain, use, or disclose the Personal Information outside*

ii. General Data Protection Regulation (GDPR)

It has become increasingly common for law firms or their clients to be involved in transactions with international customers or their vendors. In these instances, you must look outside the U.S. domestic privacy framework. For example, when personal data from a person located in the EU is coming *from* the EU *to* the US,[89] the GDPR requires data controllers[90] (also called data exporters or those who initiate and collect personal data from individuals in the EU[91]) to vet data processors[92] (also called data importers or those who perform some type of processing on the personal data), and, once vetted, implement a contract that provides sufficient guarantees to protect the rights of data subjects. There should be an appropriate mechanism for legally transmitting the data outside of its home country, such as through implementation of what the EU calls "model clauses" or "standard contractual clauses" ("SCCs"). US entities previously relied on the Privacy Shield mechanism in conjunction with the SCC's.[93] This accepted process was thrown into disarray on July 16, 2020, when the Court of Justice for the European Union invalidated the Privacy Shield as an acceptable mechanism for the cross-border transfer of personal data.[94] If you or your client are contemplating any transaction that involves the collection of personal data from individuals in the EU for transport outside of the EU for processing, seek expert advice.[95]

"If you or your client are contemplating any transaction that involves the collection of personal data from individuals in the EU for transport outside of the EU for processing, seek expert advice."

of the direct business relationship between [Vendor] and [Company]. [Vendor] certifies that it understands these restrictions and will comply with them. Merely including this clause is insufficient: due diligence is necessary to map out each element of the personal data and role of the participating service provider.

89 *See* the UK Data Protection Act 2018 for those individuals located in the United Kingdom. The Data Protection Act complements the GDPR and was enacted in anticipation of Brexit. *See also* the Personal Information Protection and Electronic Documents Act when addressing the personal data of individuals in Canada.

90 Those who "control" the collection of personal data from natural persons or data subjects.

91 This is often misunderstood and described as EU "residents" or EU "citizens." It is neither. The Regulation is drafted to apply to "the processing of personal data of data subjects who are in the Union . . . ." Regulation (EU) 2016/679 (GDPR) Ch. 1, Art. 3, Section 2.

92 Those who "process" the personal data that has been collected.

93 https://www.privacyshield.gov/welcome last visited 11/21/2020.

94 Case C-311/18 *Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems* (Schrems II). The main questions before the Court were whether the EU-US Privacy Shield and the standard contractual clauses (SCCs) remain valid mechanisms for international data transfers from the EU to the US under current US law.

95 In November 2020, the European Data Protection Board issued guidance on how to address cross border transfers of personal data from the EU to the US and also published draft SCCs for comment. *See* https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries.

H. Audit of Vendor Performance

Monitoring and assessment provisions should be included and require appropriate remediation activities and mechanisms to exit the relationship if issues identified cannot be adequately addressed.

i. Performance relative to agreed service level commitments, key performance, and risk indicators.

ii. Vendor entitlements to customer information and systems to align with customer's current risk tolerance, *i.e.*, customer may remove vendor entitlements as necessary to maintain customer security – even if vendor performance is impaired. The contract should address notice and adjustment to changed conditions for access to information and systems.

iii. Audit, whether customer audit, vendor self-assessment and certification, or third-party audit, of internal controls, reporting, contract performance, security/technical, etc. Security audits may occur periodically and be event-driven. Audit provisions may provide that the results of third-party audits be made available to customer (*e.g.*, upon request or according to an agreed upon schedule), together with evidence of remediation of risks identified and explanation of any risks accepted (*i.e.*, disclosed to customer and not remediated). Consider the level of audit detail accessible to customer (*e.g.*, conclusions versus entire report), as well as expectations regarding severity of risks that must be remediated versus risks the vendor may accept.

iv. Representations – relevant to:

1) assess the vendor's capability to make investments in operations that enable continuous monitoring and on-going attention to the changing environment/threat landscape;

2) evaluate risk of loss of service if vendor fails; and

3) evaluate risk of loss of information if vendor fails and customer is unable to recover information from vendor or its downstream service providers.

v. Vendor personnel background investigation – conducted by customer or vendor. Consider legal constraints on individual background investigations.

vi. Access to vendor information, systems, and operations for audit/assessment by customer's regulators. If the customer is a regulated entity, are the vendor's

activities subject to regulatory examination or oversight, including access to work papers, drafts, and other materials?

I. Cyber Incident Reporting.

The agreement should contain clear language requiring the vendor to notify the customer immediately upon the discovery of a breach of security affecting the accessibility, confidentiality, or integrity of client-provided information. Sample language is below:

> "*If vendor discovers or is notified of a breach or potential breach of security relating to the security protocol as defined by the parties, then vendor will immediately investigate and (i) if it is determined that a breach resulting in a security incident occurred, vendor shall immediately notify the customer contract executive of such incident, and (ii) shall exert commercially reasonable efforts to attempt to remedy the effects of the breach or to thwart a potential breach*."

J. Remedies.

Remedies considerations include damages, specific performance, and limitations and disclaimers. Consider whether you or your client is responsible for to the costs associated with the investigation and mitigation of the vulnerabilities related to the vendor's product or service, including the costs for unscheduled upgrades, or if they are compensable as damages. Also consider if liquidated damages are an appropriate or effective remedy for some elements of loss arising from cybersecurity incidents.

You should also consider whether specific performance of cybersecurity covenants is an available or enforceable remedy. Are the parties able to agree on it as a remedy, and would such an agreement be enforceable even with a recital about the unique and unquantifiable risks posed by unwanted disclosure? Finally, consider incidental and consequential damage disclaimers as they relate to security breaches—what costs arising from response and recovery are direct damages and what costs are incidental/indirect or consequential?

K. Termination

The best time to address termination is at the drafting phase. When disputes arise, it is often the vendor—and not your client—who holds the advantage. The vendor will be holding valuable client data or unfinished products or services and getting it back into your client's possession can be tricky.

This issue often arises when a vendor will host customer data in an application or other solution. At some point, you may want to re-compete this effort or bring the data back in-house. The agreement should specify, at a minimum, that the vendor has an obligation to assist the customer in the transition of the data back to the customer or to another vendor. The more details that can be included about the vendor's data transfer responsibilities and who pays for such efforts will avoid unnecessary disputes at the end of a contract.

The right to terminate the agreement should also be addressed. Consider what acts, omissions, or conditions give either party the right to terminate. Should breach of certain cybersecurity obligations be defined as "material" for purposes of establishing the right to terminate? Will termination be an effective remedy – as a practical matter? Is either party permitted to terminate under circumstances other than default (e.g., upon reasonable notice and without penalty), e.g. if a regulator formally terminates or alters the arrangement; if the vendor can't adequately respond to a cyber threat; if the parties disagree about a vulnerability or remediation plan; or for convenience, if the customer doesn't believe it has received adequate assurance of the fulfilment of cybersecurity obligations?

Transition Plans serve to facilitate orderly winding up and transfer of data and/or services back to the customer or to an alternate vendor. Include a provision in the agreement obligating the vendor to provide termination assistance following the expiration or termination of the agreement. A sample provision is included in **Appendix J**.

Consider any hardware, third-party software, data, record information, space leases, IP, and other assets or support that will be required for continued operation and should be assigned or transferred at the expiration or termination.

Offboarding/Turnover obligations include verification/certification of return or destruction of customer data and information, return/deactivation of credentials controlled by vendor, cooperation with orderly removal of vendor personnel access to customer (physical and logical access), and transition assistance. Ensure that the agreement requires the vendor to oversee its affiliates' and subcontractors' compliance with the above. Examples are provided in **Appendix J.**

"…many regulations view lost or stolen media containing certain sensitive data as a breach."

Properly handling stored media (e.g., hard drives, back-up drives, flash drives, etc.) is an important element of most security frameworks. Lost or stolen media has been such a visible source of data breaches that many regulations view lost or stolen media containing certain sensitive data as a breach. Thus, common asset management transactions like media disposal and transfers must be handled carefully to avoid breach scenarios. Media transfers occur when the organization (or a part of it) loses control of the media. If the receiving party is not authorized to access any sensitive data that may be recorded on the media, the media must be sanitized prior to transfer. Also consider measures to protect the IT asset when it is transported by a third party. Media disposal is the final element in the lifecycle of an IT asset. Since many IT assets contain some form of storage media, it is important to consider what may have been stored on this media prior to taking any action. Vendor repairs or maintenance could also result in a type of media disposal. Finally, sanitization is the process or method of rendering access to target data on storage media infeasible for a given level of effort.[96] Methods of sanitization include clearing (overwriting storage space on the media through the interface or through appropriate firmware command), purging (degaussing, cryptographic erase, and executing appropriate firmware commands), and destruction (disintegrating, incinerating, melting,

[96] ISO/IEC 27040 and NIST SP 800-88r1.

pulverizing, or shredding). The agreement should provide for mandatory sanitizing measures when storage media are transferred, become obsolete, are no longer usable, or are not needed by an information system. The residual magnetic, optical, electrical, or other representation of data should also be sanitized. Storage devices or storage media that contain sensitive data must be sanitized prior to disposal. Proof of sanitization can occur through an audit log trail or a certificate of sanitization; organizations should retain this evidence.

L. Insurance.

One benefit of requiring your or your client's vendor to have cybersecurity insurance in that insurance companies often conduct their own due diligence before deciding to insure companies and often offer services in the event of a cyber incident. This can provide you further assurances that the vendor has adequate security in place to guard against cyber incidents.

Cyber insurance is crucial to risk management, especially when routinely handling sensitive or regulated data and customer data or networks. Cyber insurance can provide coverage for costs associated with data restoration, incident response, business disruption and liability. The ABA Center for Professional Responsibility has published guidance in this area.[97] Insurance is not, however, a substitute for due diligence and contract and performance management.

Evaluating cyber insurance programs includes evaluating cyber risks in a way that actively predicts, identifies, assesses, treats, and responds to cyber incidents,[98] as part of an effective risk management approach based on a robust security framework.[99] It is helpful to translate the cyber risks into business terms to highlight the business consequences of cyber incidents. Address risks through avoidance; threat removal; changing the likelihood or consequences of the risk; retaining the risk; or risk-sharing.

In evaluating whether a vendor's proffered policy is sufficient, you should consider the potential business impacts from a cyber incident. These impacts can include: loss of sales, lost profit, cost of crisis management, costs of forensic investigations, lawsuits and indemnification, cost of notifications to business partners and customers, regulatory investigations, fines, attorneys and consultants, public relation professionals, and remedial measures as well as reputational damage, impact or damages to business executives, management, staff and related personnel or leakage of trade secrets and other infringement of intellectual property rights. Knowing risks and their consequences allows a policy to align with an organization's security risk management strategy and risk acceptance criteria. Include in your coverage the following losses categories:

---

97 ABA Protecting Against Cyber Threats: A Lawyer's Guide to Choosing a Cyber Liability Insurance Policy (ABA Standing Committee on Lawyers' Professional Liability, 2nd ed., 2020).

98 A cyber incident occurs when a cyber risk becomes a reality and leads to the probable loss of confidentiality, integrity or availability of data or other assets.

99 *See* ISO/IEC 27001, NIST SP 800-53, COBIT, NIST Cybersecurity Framework, etc.

a. *Liability:* indemnification of losses to other parties (e.g., damages affecting individuals or other organizations resulting from data breach, etc.).

b. *Incident response costs:* customer or employee notification; customer or employee protection; forensic expert; incident management operations; and staff and personnel costs.

c. *Cyber extortion costs:* response to ransomware and similar threats. Some jurisdictions do not allow this coverage.

d. *Business interruption:* loss of income or profit and increased operating expenses resulting from a cyber incident.

e. *Fines and penalties:* civil penalties, and regulatory penalties and fines resulting from an investigation or enforcement action by a regulator or other compensation awarded by a legal system. Some jurisdictions do not allow this coverage. Fines and penalties can also result from a failure to meet contractual obligations.

f. *Systems damage:* Post-incident repair and restoration costs to systems, data, and software applications not otherwise covered.

Be sure to examine policy exclusions, which commonly include some or all the following:

a. First- and third-party bodily injury and property damage from a cyber incident.

b. *Terrorism*. Clearly define "Act of Terrorism" or "Cyber Terrorism" and limit exclusions to apply only where the U.S. Government officially declares an incident as an act of terrorism or cyber terrorism.

c. *Acts of war and other hostile acts.* There is no generally recognized definition of cyber war. It is generally linked to nation-state actors or level of disruptive or destructive impact, whether war is declared or not. Limit nation-state exclusions to those recognized by the U.S. Government or United Nations.

d. *Insider threats.* If excluded, request an exception to apply at least to the company's highest-ranking directors and officers, and ensure the exclusion

applies only after a court of law has made a non-appealable finding of intentionality.

e. *Territorial limits.* Some coverage is limited only to incidents that occur in the U.S. Additional coverage may be needed depending on where data is stored.

f. Loss of intellectual property, e.g., patents, copyrights, or trade secrets.

g. Theft or loss of confidential information where the information is not directly owned by the insured.

h. *Acts of God.* Review and negotiate to limit these exclusions as much as possible.

i. *Devices.* Some policies do not cover unencrypted or non-company-owned devices, or portable devices in general. Request removal of the exclusion.

j. Loss of reputation.

Note how much the insured vendor should pay before a claim can be made against the policy; any aggregate limit either as to the policy as a whole or for a single event per annum; waiting periods before business interruption coverage applies; and for how long business interruption coverage applies. Insurers can require a level of security as a precondition of coverage; such conditions are usually stated in the policy, and the insured must meet them during the validity of the contract.

M. Limitation of Liability and Indemnification.

Many vendors try to limit their liability in the agreement to the amount of or some multiple of their fee. This may be woefully inadequate to cover a customer's costs arising from a breach and firms should resist such limitations. Vendors may also try to limit indemnification to matters caused by their "gross negligence," while "negligence" is generally more favorable for the customer. They may also limit indemnification to third party claims. Ideally, indemnification should extend to both third party claims and the customer's costs to recover from the cyber incident. Consider "Choice of Law" provisions in their vendor contracts, as state law may dictate how much and to what extent a vendor may limit their liability by contract.

Consider the loss of information/violation of data protection provisions, i.e., costs associated with breach notification, investigation, remediation (*e.g.*, credit reporting, specific actions required by applicable regulators/governmental authorities, and contractual obligations such as payment processor contracts), and litigation expenses.

Be aware of disclaimers of liability for third-party material; most open-source licenses disclaim liability associated with any use of the licensed material. If the vendor also disclaims liability for third-party material, like software components, the customer will bear the risk of loss associated with the component.

If a limitation of liability is included, consider carve-outs or separate caps for indemnification of third-party claims, particularly those based on information loss or violation of data protection requirements, costs associated with security and data breaches, IP infringement, and costs to remediate vulnerabilities and incidents.

N. Business Continuity/Resiliency.

Consider what priority the vendor will give the customer in a contingency situation that impairs the vendor's performance. Knowing whether the customer is a critical customer should inform its business continuity/resiliency planning. Also consider prioritizing the products supplied and services performed by the vendor so that there are established expectations about where to direct limited resources. The agreement may point to a contingency plan and provide a process for periodic review and update.

Important considerations include disaster recovery (e.g. retention and back-up procedures, ability and time to failover to redundant systems, and security of back-up facilities); ownership/license of material to maintain operations; identification of key personnel and training for contingency situations; customer access to vendor's continuity plan and periodic testing results; vendor participation in customer continuity and/or incident planning; communication between parties during a contingency event and a mechanism to update or validate communication plans periodically; and *force majeure*.

Appendix A
Resources for Developing a Strategy to Identify and Manage Cybersecurity Risk

These links are mostly geared towards small businesses but are relevant for all firms.

1. American Bar Association Cybersecurity Legal Task Force

    a. General Resources: a variety of cybersecurity resources including the *ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals (2nd)*

    b. Small Firm Initiative: resources specific to small firms

2. Center of Internet Security (CIS): How to Build a Cybersecurity Compliance Plan. CIS is a non-profit security organization safeguarding cybersecurity and publishes consensus-based best security practices like the *CIS Controls and Secure Configuration Benchmarks.*

3. FCC

    a. Cyberplanner: helps small businesses create customized cybersecurity plans.

    b. Cybersecurity for Small Business: cybersecurity resources for small businesses.

4. FTC Cybersecurity Basics for Small Business: resources on a variety of small firm cybersecurity topics, developed in partnership with NIST, the U.S. Small Business Administration (SBA), and the Department of Homeland Security (DHS).

5. International Bar Association (IBA): best practices for small-medium law firms.

6. International Legal Technology Association LegalSEC Initiative: guidelines for risk-based information security programs.

7. International Organization of Standardization (ISO)

    a. ISO2700k Information Security: Informational site dedicated to the ISO/IEC 27000-series (ISO27k) standards for information risk and security management. ISO has a library of benchmarks, controls, and best practices.

    b. ISO 22301:2012 Business Continuity Management Standard. This site references the TC223 Societal Security Technical Committee's standards developed for protecting society if catastrophes, natural disasters, major terror attacks or shutdown of power grids occurs. Microsoft is the first hyper-scale cloud service provider to receive ISO22301 certification.

8. NIST

    a. Cybersecurity Framework: this voluntary framework includes standards, guidelines, and best practices to manage cybersecurity risk.

b. Small Business Cybersecurity Corner: cybersecurity basics, guidance by topic, and information about responding to a cyber incident, for small and medium businesses.

c. NISTIR 7261 Small Business Information Security: The Fundamentals: presents the cybersecurity fundamentals for small businesses in a format consistent with the Cybersecurity Framework

9. SBA Cybersecurity for Small Businesses: considerations and resources on topics including: Common Threats, Assess Your Business Risk, Cybersecurity Best Practices, and Training and Events.

10. U.S. Securities and Exchange Commission, Office of Compliance Inspections and Investigations: Cybersecurity and Resiliency Observations. Good for firms dealing with securities.

Appendix B
Laws Mandating Terms for Vendor Agreements

Below are examples where applicable law mandates specific or general terms for vendor agreements. Business Associate Agreements Required by HIPAA, U.S. Government Contract Provisions in supplier agreements, and post-Schrems II requirements for organizations handling personal data of individuals in the EU (even if the contracting parties are not).

U.S. federal regulator guidance on managing outsourcing or third-party risk:

1) FDIC:

-Guidance for Managing Third-Party Risk

-Consumer Compliance Examination Manual (June 2019)

-Supervisory Guidance on Model Risk Management

-FIL 19-2019: Technology Service Provider Contracts

-FIL 15-2018: FDIC Forum: Use of Technology in the Business of Banking

-FIL-13-2014: Technology Outsourcing Informational Tools for Community Bankers

-FIL-46-2012: Supervision of Technology Service providers and Outsourcing Technology Services

-FIL-44-2008: Third-Party Risk Guidance for Managing Third-Party Risk

-FIL-52-2006: Foreign-Based Third-Party Service Providers: Guidance on Managing Risks in these Outsourcing Relationships

-FIL-50-2001: Bank Technology Bulletin on Outsourcing

2) Group of 7 ("G7"), Fundamental Elements of Cybersecurity for the Financial Sector

3) Office of the Comptroller of the Currency, Risk Management Guidance, OCC-Bulletin-2013-29 (October 30, 2013)

4) Guidance on Managing Outsourcing Risk, Board of Governors, Federal Reserve System (December 5, 2013)

5) Office of the Comptroller of the Currency, Bulletin 2017-7| January 24, 2017: Third-Party Relationships: Supplemental Examination Procedures

6) Consumer Financial Protection Bureau

-Bulletin 2012-13, Service Providers (April 13, 2012)

-Bulletin 2016-02, Service Providers (October 31, 2016)

7) Federal Financial Institutions Examination Council

-Guidance on IT Service Providers (October 2012)

-Retail Payment Systems: Vendor and Third-Party Management

8) Securities and Exchange Commission

-Guidance Update No. 2015-02, Cybersecurity Guidance (April 2015)

9) Federal Reserve Bank of Minneapolis, Risk Management Considerations for Vendors

10) Federal Reserve Board of Governors, Guidance on Managing Outsourcing Risk

11) Securities Industry and Financial Markets Association

-Third Party Risk Management

-Summary Third Party Regulation Mapping Table (PDF)

-Third Party Regulation Mapping Matrix (XLS)

Financial Services Regulations:

- OCC Bulletin 2013-29
- Federal Reserve – Guidance on Managing Outsourcing Risk (12/5/13)
- Consumer Financial Protection Bureau (CFPB) Bulletin on Service Providers
- Committee on Payment and Settlement Systems (CPSS 115)
- Financial Conduct Authority (FCA) Outsourcing In Asset Mgmt. Industry
- Federal Financial Institutions Examination Council (FFIEC) – Supervision of Technology Service Providers (TSP) (10/2012)
- Regulatory Notice to Members 11-14 (Proposed Reg 3190) – 35/11
- NASD Notice to Members (NTM) 05-48
- Financial Intermediary Controls and Compliance Assessment Engagements (FICCA) Engagements by the Investment Company Institute (ICI)
- Investment Industry Regulatory Organization of Canada (IIROC) – Notice 14-0012

- International Organization of Securities Commissions, Public Document 187 – (IOSCOPD187)
- International Organization of Securities Commissions, Public Document 432 (IOSCOPD432)
- Gramm-Leach-Bliley Act (GLBA) / Reg S-P – Privacy of Customer Information
- Senior Management Arrangements, Systems and Controls (FRA-FCA)
- Outsourcing Working Group – Industry Response To FSA Dear CEO Letter On Outsourcing
- National Institute of Standards and Technology (NIST) Framework On Cybersecurity
- Federal Reserve SR 14-1/14-1A

Applicable to systems operated by the U.S. government or on its behalf by contractors is NIST 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations, updated as of Dec. 10, 2020.

This includes controls to evaluate, monitor, and mitigate risks related to suppliers and other third parties. Industries and organizations across the private sector widely accept and rely on NIST guidance. The NIST framework provides guidance on third-party risk management, generally referred to as supply chain risk management, to help organizations establish and implement controls to protect their information systems and the data within them. These controls aim to ensure that organizations properly vet the privacy and security implications of the third parties that develop, deploy, and maintain information system technologies, or otherwise supply and handle information assets. With respect to third-party risks, NIST 800-53 covers, among other things, the following:

- Supply chain risk management and plans
- External system service providers
- Risk assessments of third parties and outsourced service providers
- Incident handling, reporting, and response plans, as well as contingency plans
- Information sharing with external parties

Appendix C
Glossary

Term	Definition	Source
access control	The process of granting or denying specific requests to: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities (e.g., federal buildings, military establishments, border crossing entrances).	[NIST SP 800-12 Rev. 1]
advanced persistent threats (APT)	An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives.	[NIST SP 800-53 Rev. 5]
application-level encryption	The process of encrypting or decrypting data is completed by the application that has been used to generate or modify the data that is to be encrypted.	
business continuity (BC)	capability of the organization to continue delivery of products or services at acceptable predefined levels following disruptive incident.	[ISO 22300]
cloud computing	paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand. Note: Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.	[ISO/IEC 22123-1]
cross border data transfer	The transmission of personal information from one jurisdiction to another. Note: Many jurisdictions, most notably the European Union, place significant restrictions on such transfers. The EU requires that the receiving jurisdiction be judged to have "adequate" data protection practices.	[IAPP Glossary]

Term	Definition	Source
data at rest	Data stored on stable non-volatile storage.	[ISO/IEC 27040]
data controller	person or organization who determines the purposes for which and the manner in which any personal data are to be collected, processed and stored.	[ISO 10667-2]
data governance	development and enforcement of policies related to the management of data. Note: Six principles of information technology governance: responsibility; strategy; acquisition; performance; conformance; human behavior. These principles also apply to data.	
data subject	person or organization from whom or about whom data are collected for research.	[ISO 20252]
disaster recovery (DR)	ability of the information and communications technology (ICT) elements of an organization to support its critical business functions to an acceptable level within a predetermined period following a disaster.	[ISO/IEC 27031]
disposal	Disposal is a release outcome following the decision that media does not contain sensitive data. Note: This occurs either because the media never contained sensitive data or because Sanitization techniques were applied, and the media no longer contains sensitive data.	[NIST SP 800-88 Rev. 1]
due diligence	comprehensive, proactive process to identify the actual and potential negative social, environmental and economic impacts of an organization's decisions and activities over the entire life cycle of a project or organizational activity, with the aim of avoiding and mitigating negative impacts.	[ISO 26000]
encryption	Cryptographic transformation of data (called “plaintext”) into a form (called “ciphertext”) that conceals the data’s original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called “decryption,” which is a transformation that restores encrypted data to its original state.	[NIST SP 800-82 Rev. 2].
file-level encryption	The process of encrypting or decrypting data stored in individual files or directories is completed by the filesystem.	

Term	Definition	Source
full disk encryption (FDE)	technology that causes the whole disk to be encrypted using an encryption key.	
incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.	[NIST SP 800-53 Rev. 5]
incident response	action taken to protect and restore the normal operational conditions of information systems and the information stored in it when an attack or intrusion occurs.	[ISO/IEC 27039]
incident response plan	The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber-attacks against an organization's information system(s).	[NIST SP 800-34 Rev. 1]
information security	Preservation of confidentiality, integrity and availability of information. In addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved.	[ISO/IEC 27000:2018]
Internet of things (IoT)	infrastructure of interconnected objects, people, systems, and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react.	[ISO 19731]
jailbreak	modify system or electronic device to remove restrictions imposed by the manufacturer or operator.	
key management	administration and use of generation, registration, certification, deregistration, distribution, installation, storage, archiving, revocation, derivation and destruction of keying material in accordance with a security policy.	[ISO/IEC 11770-1]
malware	software designed with malicious intent containing features or capabilities that can potentially cause harm directly or indirectly to the user and/or the user's computer system.	[ISO/IEC 27032]
personal information (also personally identifiable information or PII)	any information that (a) can be used to establish a link between the information and the natural person to whom such information relates, or (b) is or can be directly or indirectly linked to a natural person	[ISO/IEC 29100]

Term	Definition	Source
	Note 1: The "natural person" in the definition is the PII principal. To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other party, to establish the link between the set of PII and the natural person. Note 2: This definition is included to define the term PII as used in this document. A public cloud PII processor is typically not in a position to know explicitly whether information it processes falls into any specified category unless this is made transparent by the cloud service customer.	
phishing	fraudulent process of attempting to acquire private or confidential information by masquerading as a trustworthy entity in an electronic communication. Note: Phishing can be accomplished by using social engineering or technical deception.	[ISO/IEC 27032]
risk management	The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time.	[NIST SP 800-53 Rev. 5]
security by design	A design process in software engineering that incorporates the necessary security elements as integral to the foundation of the software. It is guided by an iterative process that evaluates risk at every potential entry point.	
Trojan horse	Hidden code in a computer program that allows the unauthorized collection, falsification, or destruction of information. Note: A type of malware.	
vendor	As used in this Checklist, an entity that sells its goods or services to our focused group of lawyers and law firms or those law firm clients.	
vendor risk management	This describes the process by which you (either on behalf of yourself, your law firm or your client)—as a purchaser of a Vendor's goods or services—evaluate and manage the "risks"	

Term	Definition	Source
	associated with the relationship with the Vendor. What kind of data will be exchanged, processed, or managed by the Vendor? What representations, warranties, indemnities, insurance, is the Vendor willing to offer to secure its transaction? What foreign, federal, state, or local laws govern the transaction? What kind of damages, expenses, enforcement actions, etc. would result if the data were lost, stolen, or accessed without authorization? These are just a handful of the questions you might ask to evaluate and manage the risk associated with any given Vendor relationship.	
virtual private network (VPN)	restricted-use logical computer network that is constructed from the system resources of a physical network by using encryption and/or by tunneling links of the virtual network across the real network.	[ISO/IEC 18028-3]
virus	A type of programmed threat; a code fragment (not an independent program) that replicates by attaching to another program, and either damages information directly or causes denial of service. Note: A type of malware.	
zero-day event	First release of malware exploiting a previously undisclosed vulnerability.	

Appendix D
NIST Key Areas in a Security Program

In various guidance documents, NIST has identified key areas that must be addressed in a security program.[100] Examples include:

1) Access Control

   i. Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

   ii. Limit information system access to the types of transactions and functions that authorized users are permitted to execute

   iii. Examples: Establishing access controls and identity management protocols, including multi-factor authentication; Limits on privileged users

2) Awareness and Training

   i. Ensure that managers, systems administrators, and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of organizational information systems.

   ii. Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

3) Audit and Accountability

   i. Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.

---

[100] NIST Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, Spec Pub 800-171 (February 2020), *available at* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf . DoD requires its contractors to implement NIST 800-171 as a minimum baseline for adequate security on contractors' and DoD suppliers' internal systems that process unclassified controlled information. DFARS 252.204-7012. Effective November 30, 2020, DoD is using 2 new mandatory flow down clauses in its solicitations and contracts that require a contractor or subcontractor to have conducted a basic NIST 800-171 self-assessment in accordance with a DoD assessment guide, and to agree in advance that the Government may audit its NIST 800-171 implementation to be eligible for award. DFARS 252.204-7019, 7020. DoD also introduced a third new clause – DFARS 252.204-21 – to facilitate implementation of its new Cybersecurity Maturity Model Certification (CMMC) framework that will require all suppliers in DoD's supply chain to achieve prior to award and maintain throughout contract performance a third party certification that it has implemented the cybersecurity controls required at the CCMC maturity level DoD identifies in the solicitation. The program, which will be rolled out gradually over the next 5 years, incorporates all 110 NIST 800-171 controls into its required processes and practices and introduces additional processes and controls across the 5 levels. CMMC also adds three new areas or "domains" to the above list – Asset Management, Recovery and Situational Awareness. For more information on CMMC, including assessment guides for Levels 1 and 3, *see* https://www.acq.osd.mil/cmmc/draft.html.

ii. Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

4) Configuration Management

i. Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

ii. Establish and enforce security configuration settings for information technology products employed in organizational information systems

iii. Examples: Malicious activity scanning; Regular software patching

5) Identification and Authentication

i. Identify information system users, processes acting on behalf of users, or devices.

ii. Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

6) Incident Response

i. Establish an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.

ii. Track, document, and report incidents to appropriate officials and/or authorities both internal and external to the organization.

7) Maintenance

i. Perform maintenance on organizational information systems.

ii. Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

8) Media Protection

i. Protect (i.e., physically control and securely store) information system media containing CUI, both paper and digital.

ii. Limit access to CUI on information system media to authorized users.

iii. Sanitize or destroy information system media containing CUI before disposal or release for reuse.

9) Personnel

i. Screen individuals prior to authorizing access to information systems containing CUI.

ii. Ensure that CUI and information systems containing CUI are protected during and after personnel actions such as terminations and transfers.

10) Physical Protection

i. Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

ii. Protect and monitor the physical facility and support infrastructure for those information systems.

11) Risk Assessment

i. Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of CUI.

12) Security Assessment

i. Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application.

ii. Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems.

iii. Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

13) System and Communications Protection

i. Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.

ii. Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

14) System and Information Integrity

i. Identify, report, and correct information and information system flaws in a timely manner.

ii. Provide protection from malicious code at appropriate locations within organizational information systems.

iii. Monitor information system security alerts and advisories and take appropriate actions in response.

Appendix E
Sample Provisions Covering Personal Information

1. **Compliance with Data Protection Requirements and this Agreement.** Vendor will at all times comply with and treat Company Data in accordance with the requirements of this Agreement and the Data Protection Requirements. Vendor hereby represents and warrants that it will inform itself regarding, and comply with, all applicable Data Protection Requirements. Vendor will notify the Company if Vendor believes that the Company's instructions concerning Company Data, including, without limitation, the requirements of this Agreement, would cause Vendor to violate any Data Protection Requirement. In the event of such notification, the Company will then instruct Vendor on appropriate compensating controls by which to abide.

2. **Vendor Use of Company Data.** At no time shall Vendor acquire any ownership, license, rights, title or other interest in or to Company Data, all of which shall, as between the Company and Vendor, be and remain the proprietary and confidential information of the Company. Vendor shall not be entitled to use Company Data for its own purposes or for the purpose of any third party. In no event may Vendor: (a) use Company Data to market its Services or those of a third party; or (b) sell or rent Company Data to third parties.

3. **Restrictions on Subcontractors.** Before providing Company Data to any third party, including, without limitation, Vendor's affiliates or a potential subcontractor or service provider, Vendor must obtain written approval for such disclosure from an officer of the Company. The Company's consent to Vendor affiliates' or potential subcontractors' access to Company Data shall not be unreasonably withheld. If Vendor is permitted to disclose Company Data to such third party, such disclosure must be limited to the minimum Company Data necessary for the third party to fulfill its obligations to Vendor. Vendor agrees that if Company consents to Vendor's disclosure of Company Data to such third party, prior to making such disclosure, Vendor will enter into a written agreement with the third party that includes obligations that are at least as broad in scope and restrictive as those under this Agreement. Nonetheless, Vendor shall always remain accountable and responsible for all actions by such third parties with respect to the disclosed Company Data as if such third parties were a Party to this Agreement.

4. **Internal Vendor Security Program.** Vendor shall:

   A. develop, implement, maintain, monitor and comply with a comprehensive, written information security program that contains administrative, technical and physical safeguards to protect against anticipated threats or hazards to the security, confidentiality or integrity of, the unauthorized or accidental destruction, loss, alteration or use of, and the unauthorized access to or acquisition of Company Data and provide the Company with documentation of such safeguards, upon the reasonable request of the Company at any time;

   B. conduct a risk assessment to identify and assess reasonably foreseeable internal and external risks to the security, confidentiality and integrity of electronic, paper and other

records containing Company Data and to evaluate and improve, where necessary, the effectiveness of its safeguards for limiting those internal and external risks; and

C. ensure that its information security program is consistent with: (i) the Company's information security practices and requirements as may be issued to Vendor by the Company from time to time, including, without limitation, enhanced security provisions governing the use of Special Personally Identifiable Data in order to comply with applicable laws; (ii) the Data Protection Requirements; (iii) the PCI Standards, if Vendor has access to or otherwise handles Cardholder Data; and (iv) prevailing industry practices.

5. **Review of and Updates to Vendor Security Program.** Vendor shall review and, as appropriate, revise its information security program: (a) at least annually or whenever there is a material change in Vendor's business practices that may reasonably affect the security or integrity of Company Data; (b) in accordance with prevailing industry practices; and (c) as reasonably requested by the Company. If Vendor modifies its information security program following such a review, Vendor shall promptly notify the Company of the modifications and shall provide the modifications to the Company in writing upon the Company's request. Vendor may not alter or modify its information security program in such a way that will weaken or compromise the confidentiality and security of Company Data.

6. **Vendor Security Standards.** Vendor agrees that: (a) it will establish, maintain and comply with appropriate access controls consistent with then-current industry best practices which, as of the inception of the Agreement, includes, but is not limited to, limiting access to Company Data to the minimum number of Vendor employees and personnel who require such access in order to provide Services to Company; (b) its employees and personnel who will be provided access to, or otherwise come into contact with, Company Data will be required (including during the term of their employment or retention and thereafter) to protect such Company Data in accordance with the requirements of this Agreement; (c) its employees and personnel who will be provided access to, or otherwise come into contact with, Company Data will have the appropriate qualifications and references (which include, without limitation, a requirement that Vendor conduct drug and background checks of such employees and personnel prior to such employees or personnel accessing any Company Data to handle and to protect such Company Data in accordance with the requirements of this Agreement; and (d) Vendor will provide such employees and personnel with appropriate training regarding information security and the protection of personally identifiable data.

7. **Password Management and Authentication Controls**. Vendor must ensure that its systems which process Company Data employ strong password complexity rules. In particular, Vendor shall: (a) configure its passwords to expire every ninety (90) days or less; (b) enable system lockout after failed login attempts; (c) enable O/S screen saver locks after a period of

inactivity; (d) encrypt authentication credentials during storage and transmission; and (e) prohibit its users from sharing passwords.

8. **Extent and Content of Vendor Security Program.** Vendor shall maintain and enforce its information security program at each location from which Vendor provides Services. In addition, Vendor shall ensure that its information security program covers all networks, systems, servers, computers, notebooks, laptops, PDAs, mobile phones and other devices and media that process or handle Company Data or that provide access to Company Data, or the networks, systems, or information of the Company Entities. Moreover, Vendor shall ensure that its information security program includes, without limitation, industry standard password protections, firewalls and anti-virus and malware protections to protect Company Data stored on computer systems. Vendor further warrants that Company Data will not be commingled with data from other companies. Vendor shall regularly test and monitor Vendor security procedures and systems and shall conduct periodic reviews to ensure compliance with the requirements set forth herein. Vendor shall make the results of such reviews available to Company at Company's request.

9. **Annual External Security Assessment, Questionnaire, and Follow-up Questioning.** Vendor shall annually, at no additional cost or expense to the Company: (a) provide the Company with a copy of their Statement on Standards for Attestation Engagements (SSAE) No. 16 or equivalent external assessment report, which shall include an assessment report(s) for any third party supporting the Services; (b) complete the Company's standard information security questionnaire (at the Company's request), which shall include responses to any questions regarding Vendor's controls for any part of the Services performed by a third party by or on behalf of Vendor; and (c) make available an appropriate senior representative of Vendor's information security team to meet with the Company's information security team to discuss any questions or concerns the Company may have regarding Vendor's information security program.

10. **Encryption of Company Data.** Vendor shall encrypt, using industry standard encryption tools, all records and files containing Company Data that Vendor: (a) transmits or sends wirelessly or across public networks; (b) stores on laptops or storage media; (c) where technically feasible, stores on portable devices; and (d) stores on any device that is transported outside of the physical or logical controls of Vendor. Vendor shall safeguard the security and confidentiality of all encryption keys associated with encrypted Company Data.

11. **Disposal of Company Data.** If Vendor disposes of any paper, electronic or other record containing Company Data, Vendor shall do so by taking all reasonable steps (based on the sensitivity of the Company Data) to destroy the Company Data by: (a) shredding; (b) permanently erasing and deleting; (c) degaussing; or (d) otherwise modifying Company Data in such records to make it unreadable, unreconstructable, and indecipherable. All Special

Personally Identifiable Data must be disposed of in a manner described in clause (a), (b), or (c) of this Section.

12. **Vendor Access to Company Networks and/or Company Data Processed within Company.** If Vendor connects to the computing systems or networks of any Company Entities, Vendor agrees that: (a) Vendor will not access, and will not permit any other person or entity to access, the computing systems or networks of the Company Entities without the Company's prior written authorization and any such actual or attempted access shall be consistent with any such authorization; (b) all Vendor connectivity to the computing systems and networks of Company Entities and all attempts at same shall be only through the Company's security gateways/firewalls; and (c) Vendor will use latest available, most comprehensive virus and malware detection/scanning program prior to any attempt to access any of the computing systems or networks of any Company Entities. Vendor shall inform the Company in writing of the identity of Vendor employees and personnel who have access to the systems or networks of Company Entities. Vendor may change the Vendor employees and personnel who have access to the systems or networks of Company Entities; provided, that Vendor must give prior written notice to the Company and receive the Company's prior written approval for any such change.

13. **Vendor Access to Company Data Processed External to Company Controlled Environment.** If Vendor (a) provides Cloud or SaaS, or (b) provides outsourced software development services, or (c) [processes] Company Data external to a Company controlled environment, the following shall apply in addition to Section 14 above:

A. **Unauthorized Network Traffic.** Vendor must ensure that the Vendor networks that process Company Data employ industry best-practice safeguards and controls to monitor and block unauthorized network traffic.

B. **Malware Protection.** Where technically feasible, Vendor must deploy malware protection on all IT systems that access Company Data. Vendor must ensure malware protection technology has the latest and up-to-date manufacturer's signatures, definition files, software, and patches.

C. **Management of Cloud Service Users.** Vendor will provide a secure and timely management of on-boarding and off-boarding of cloud service users. Vendor will use standard APIs, such as Simple Cloud Identity Management.

D. **Authentication Requirements.** Vendor will use two-factor authentication and certificates to authenticate their remote administrators who manage their cloud services, or an alternative strong authentication method provided it has received prior approval from the Company.

E. **Authorization and Access Controls.** Vendor will maintain a policy and role-based access controls to log user access information for compliance, audit and incident

investigation purposes. Vendor will use standards such as OAUTH v2 to avoid becoming locked into one authorization method.

14. **Vendor System Checks and Remediation.** The Company may perform periodic security assessments of the computing systems and networks of the Company or Company Entities, which may include, without limitation, assessment of certain portions of the computing systems and networks of Vendor. Vendor agrees that should any such assessment reveal inadequate security by Vendor, Company, in addition to other remedies it may have, may suspend Vendor's access to the computing systems and networks of Company Entities until such inadequate security has been appropriately addressed, to the satisfaction of the Company. Such suspension will not be considered a breach of the Agreement by the Company.

15. **Third-Party Requests for Company Data.** If Vendor is requested or required (by oral questions, interrogatories, requests for information or documents in legal proceedings, subpoenas, civil investigative demands or other similar processes) to disclose any Company Data to a third party, Vendor shall immediately notify the Company of any such anticipated disclosure (except to the extent otherwise required by applicable law) and shall not disclose Company Data to the third party without providing the Company notice at least forty-eight (48) hours following such request or demand, so that the Company may, at its own expense, exercise such rights as it may have under law to prevent or limit such disclosure. Notwithstanding the foregoing, Vendor shall exercise commercially reasonable efforts to prevent and limit any such disclosure to only such Company Data as Vendor's legal counsel has determined is required to be produced and to otherwise preserve the confidentiality of Company Data, including, without limitation, by cooperating with the Company to obtain an appropriate protective order or other reliable assurance that confidential treatment will be accorded to Company Data.

16. **Maintenance of Vendor Records.** Vendor shall establish and maintain complete and accurate books, notices, accounting records and administrative records necessary to document the proper handling of Company Data under this Agreement, including, without limitation, accounts of all transactions involving Company Data, and shall retain such records pursuant to applicable law.

17. **Audits.** No more often than once per year (unless otherwise required by the Company's regulators) and upon reasonable notice to Vendor, Vendor shall permit Company, its auditors,

designated audit representatives, and regulators, including, without limitation, data protection regulators, at Company's sole expense (except as provided herein), to audit and inspect:

A. the facilities of Vendor and any third-party service providers of Vendor previously approved by the Company where Company Data is stored or maintained by, or on behalf of, Vendor;

B. any computerized or paper systems used to share, disseminate or otherwise handle Company Data;

C. Vendor's security practices and procedures, facilities, resources, plans and procedures; and

D. all books, notices, accounting records and administrative records required to be retained by Vendor hereunder.

18. **Post-Audit Recourse for Non-Compliance.** The audit and inspection rights shall be, at a minimum, for the purpose of verifying Vendor's compliance with this Agreement, all applicable Data Protection Requirements, and the PCI Standards. If any audit or inspection conducted pursuant to this Agreement reveals a material technical issue, security problem, or other non-compliance with this Agreement, any applicable Data Protection Requirements and/or the PCI Standards, then Vendor will pay the Company's costs for conducting such audit and/or inspection and will propose an appropriate written response, including, without limitation, a plan for the remediation of the problem, within the time reasonably requested by the Company. Upon the Company's approval of such plan, Vendor will remedy the problem according to the plan. The Company will not be responsible for any additional costs or fees related to such remedy.

19. **Vendor Assistance during Investigations.** Upon notice to Vendor, Vendor shall promptly assist and support the Company in the event of an investigation by any regulator, including, without limitation, a data protection regulator or similar authority, if and to the extent that such investigation relates to Company Data handled by Vendor. Such assistance and support shall be at the Company's sole expense, except where such investigation was required due to Vendor's acts or omissions, in which case such assistance and support shall be at Vendor's sole expense.

20. **Security Breach Notification and Response.** Vendor is responsible for any and all information security incidents involving Company Data that is handled by, or on behalf of, Vendor. Vendor shall notify the Company in writing immediately (and in any event within twenty-four (24) hours) whenever Vendor reasonably believes that there has been an unauthorized acquisition, destruction, modification, use, or disclosure of, or access to, Company Data ("Breach"). After providing such notice, Vendor will investigate the Breach, take all necessary steps to eliminate or contain the exposures that led to such Breach, document all

information collected as part of its investigation of the Breach, and keep Company advised of the status of such Breach and all matters related thereto. Vendor further agrees:

A. to provide, at Vendor's sole cost, reasonable assistance and cooperation requested by the Company and/or the Company's designated representatives, in the furtherance of any correction, remediation, or investigation of any such Breach and/or the mitigation of any damage, including, without limitation, any notification that the Company may determine appropriate to send to individuals impacted or potentially impacted by the Breach, and/or the provision of any credit monitoring or identity theft protection service that the Company deems appropriate to provide to such individuals;

B. that, unless required by law, Vendor shall not notify any individual or any third party (other than law enforcement) of any potential Breach involving Company Data without first consulting with, and obtaining the permission of, the Company;

C. that within thirty (30) days of identifying or being informed of a Breach, Vendor shall develop and execute a plan, subject to Company's approval, that reduces the likelihood of a recurrence of such Breach;

D. that the Company may, at its discretion, immediately terminate the Agreement without penalty if a Breach occurs; and

E. that, due to the unique nature of Company Data, the unauthorized disclosure or use of Company Data may cause irreparable harm to the Company, the extent of which will be difficult to ascertain and for which there will be no adequate remedy at law. Accordingly, Vendor agrees that the Company, in addition to any other available remedies, shall have the right to seek an immediate injunction and other equitable relief enjoining any Breach or threatened Breach without the necessity of posting any bond or other security.

21. **Disposal/Preservation of Company Data.** Vendor shall, as appropriate, regularly dispose of Company Data that is maintained by Vendor, but that is no longer necessary to provide the Services. Notwithstanding the foregoing, Vendor shall comply with the Company's written instructions to preserve Company Data in connection with any investigations, lawsuits or other disputes in which any Company Entities may be involved. Except to perform Termination Support, upon termination or expiration of the Agreement for any reason or upon Company's request, Vendor shall immediately cease handling Company Data or portion of Company Data specified by the Company, and shall return in a manner and format reasonably requested by the Company, or, if specifically directed by the Company, shall destroy any or all such Company Data in Vendor's possession, power or control, in whatever form, including, without limitation, all copies, fragments, excerpts, and any materials containing Company Data, whether or not such Company Data has been intermingled with Vendor's own information or materials. Upon the Company's instruction to destroy or return Company Data, all copies of Company Data shall be permanently removed from Vendor's, its agents', subcontractors' and third parties' systems, records, archives and backups and all subsequent use of such Company Data by

Vendor, its agents, subcontractors and third parties shall cease. Upon request, an officer of Vendor will certify to Company that all forms of the requested Company Data have been destroyed by Vendor.

Appendix F
Data Breach Disclosure Laws

State Laws on Breach Disclosure Obligations for Third-Party Custodians. This is a dynamic field and laws are subject to change; it may be helpful to confirm the status of these laws.

State	Obligations of Third-Party Custodians according to the Data Privacy Advisor	Legislation
Alabama	In Alabama, any third-party agent that experiences a breach of security must notify the covered entity as expeditiously as possible and without unreasonable delay, but no later than ten days after determining, or the entity reasonably believes, a breach occurred. The third party must cooperate with the covered entity to provide information necessary for the covered entity to comply with the notification requirements. Additionally, the parties may contractually agree to have the third-party agent handle notifications.	Alabama Code § 8-38-8
Alaska	If an Alaska entity maintains personal information on a state resident that it does not own or have the right to license, the entity must notify the owner or licensee of the information of any breach of the security of the data immediately following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The entity must also cooperate with the owner or licensee of the information as necessary to allow the owner or licensee to comply with its breach notification requirements.	Alaska Stat. Ann. § 45.48.070
Arizona	An Arizona covered entity that maintains unencrypted and unredacted computerized data that includes personal information it does not own or license must notify and cooperate with the owner or licensee of the information of any breach of the security of the system as soon as practicable.	Arizona Revised S. § 18-552
Arkansas	If an entity maintains personal information on a state resident, the entity must notify the owner or licensee of the information immediately following discovery of any breach of the security of the system if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.	Arkansas Code Ann. § 4-110-105(b)
California	Under California's general data breach notification statute, if an entity maintains computerized data about California residents that includes personal information the entity does not own, the entity must notify the owner or licensee of the information of any breach of the security of the data immediately following discovery if the personal information was or is reasonably believed to have been acquired by an unauthorized person.	California Civil Code § 1798.29, 1798.80, 1798.82, and 1798.84
Colorado	The Colorado statute requires a third-party service provider that maintains computerized personal information for a covered entity to notify the covered entity of a security breach in the most expedient time possible and without unreasonable delay, if the personal information was, or is likely to be misused. "Third party service provider" is defined as an entity that has been contracted to maintain, store, or process personal information on behalf of a covered entity.	Colorado Revised Statutes Ann. § 6-1-716(2)(b)) / (1)(i)

Connecticut	In Connecticut, a covered entity that maintains computerized data that includes personal information that it does not own or license must notify the owner or licensee of the information of any breach of the security of the data immediately following discovery if the personal information was, or is reasonably believed to have been, breached.	Connecticut General Statute Conn. Gen. Stat. Ann. § 36a-701b(c)
Delaware	In Delaware, on determining a breach of the security of the system, an entity that does not own or license the personal information must immediately: 1. Notify the information's owner or licensee. 2. Cooperate with the information's owner or licensee, including sharing information relevant to the breach. If a law enforcement agency determines that providing notice will impede a criminal investigation, notice may be delayed until the law enforcement agency determines it will no longer impede the investigation.	6 Del. C. § 12B-102(b),(c)
Florida	In Florida, a person or entity that maintains computerized data that includes personal information on behalf of another business entity must notify the entity for which the information is maintained of a breach of the security of the system as soon as practicable, but no more than ten days after the determination, if personal information was, or is reasonably believed to have been, acquired by an unauthorized person. A third-party agent must provide a covered entity with all information that the covered entity needs to comply with its notice obligations.	West Florida Statutes Annotated, § 501.171(6)(a)
Georgia	Any person or business that maintains computerized data on behalf of an information broker or data collector that includes individuals' personal information that the person or business does not own must notify the information broker or data collector of any breach of the security of the system within 24 hours following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.	West's Code of Georgia Annotated § 10-1-912(b)
Hawaii	Any business that is located in or conducts business in Hawaii and maintains or possesses records or data containing Hawaii residents' personal information that the business does not own or license, and any government agency that maintains or possesses Hawaii residents' personal information, must notify the owner or licensee of the information of any security breach immediately following discovery of the breach, consistent with the legitimate needs of law enforcement.	West Hawaii Revised Statutes Annotated § 487N-2(b)
Idaho	In Idaho, an entity that maintains computerized data with personal information that it does not own or license must notify and cooperate with the information's owner or licensee of any breach of the security of the system immediately following discovery of the breach, if any Idaho resident's personal information has or is reasonably likely to be misused.	Idaho Code § 28-51-105(2)
Illinois	The Illinois statute requires a data collector that maintains unencrypted computerized data that includes personal information it does not own or license to both: 1. Notify the information's owner or licensee immediately following discovery of any breach if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.	815 ILCS 530/10(b)

	2. Cooperate with the data owner or licensee with respect to breaches of personal information in the service provider's care including, at least: • informing the owner or licensee of the breach, including giving notice of the date or approximate date of the breach and the nature of the breach; and • informing the owner or licensee of any steps the data collector has taken or plans to take relating to the breach. The data collector is not required to either: • Disclose confidential business information or trade secrets. • Notify affected persons.	
Indiana	A covered entity in Indiana that maintains computerized data that includes personal information it does not own or license must notify the owner of the personal information if the entity discovers that personal information was or may have been acquired by an unauthorized person. Additionally, if a state agency maintains computerized data containing personal information on behalf of another and the state agency discovers an unauthorized acquisition, it must notify affected state residents.	Indiana Code § 24-4.9-3-2, 4-1-11-6, 4-1-11-5
Iowa	In Iowa, any person, business, or government entity that maintains or possesses personal information on behalf of another must notify the information's owner or licensor of any breach of security immediately following discovery of the breach if the breach included a consumer's personal information.	Iowa Code Annotated § 715C.2(2)
Kansas	The Kansas statute requires an individual or commercial entity that maintains computerized data that includes personal information it does not own or license to notify the information's owner or licensee following discovery of any breach if the personal information was, or is reasonably believed to have been, accessed and acquired by an unauthorized person.	Kansas Statutes Annotated § 50-7a02(b)
Kentucky	In Kentucky, an information holder that maintains computerized data that includes personally identifiable information that it does not own must notify the owner or licensee of the information of any breach of the security of the data as soon as reasonably practicable following discovery if the personally identifiable information was, or is reasonably believed to have been, acquired by an unauthorized person.	Kentucky Revised Statutes 365.732(3)
Louisiana	The Louisiana statute requires any person or agency that maintains computerized data that includes personal information it does not own to notify the information's owner or licensee following discovery of any breach if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Notice is subject to the same timing requirements as notices to affected persons.	Louisiana Statutes Annotated § 3074(D), (E
Maine	In Maine, a third-party entity that maintains, on behalf of another person, computerized data that includes personal information it does not own must notify the person maintaining personal information of a breach of the security of the system immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.	10 M.R.S.A. § 1348(2)
Maryland	A business that maintains computerized data that includes personal information of an individual residing in Maryland that it does not own or license, when it discovers or is notified of a breach, as soon as practicable, but not later than 45 days, to:	Maryland Code Annotated, Com. Law §

	• Notify the information's owner or licensee of the breach. • Share information about the breach with the information's owner or licensee. Third-party custodians are prohibited from charging the owner or licensee a fee for providing the information needed to notify individuals affected by a breach. The owner or licensee of the information is also prohibited from using any information related to the breach for any purpose other than: • Providing breach notification. • Protecting or securing personal information. • Providing notification to national information security organizations to alert and avert new or expanded breaches.	14-3504(c),(4)

Massachusetts	In Massachusetts, a covered entity that maintains or stores, but does not own or license, data that includes personal information and knows of or has reason to know of a breach or unauthorized acquisition or use of personal information must both:
	• Notify the information's owner or licensee as soon as practicable and without unreasonable delay.
	• Cooperate with the owner or licensor, including informing the owner or licensor of:
	  • the date or approximate date of the incident;
	  • the nature of the breach or unauthorized acquisition or use; and
	  • any steps the covered entity has taken or plans to take relating to the incident.
	The law expressly provides that a third-party custodian is not required to notify affected persons.
		M.G.L.ch. 93H § 3(a)

Michigan	**General Statute: MCL 445.72** A person, legal entity, or agency that maintains a database that includes data that it does not own or license that discovers a security breach must notify the information's owner or licensor of the security breach, unless the entity determines that the security breach has not or is not likely to cause a Michigan resident to suffer substantial loss or injury or identity theft. **Insurance Data Security Statute** Effective January 20, 2021, the insurance statute requires a licensee that maintains a database that includes data that the licensee does not own or license that discovers a security breach must notify the owner or licensor of the information of the cybersecurity event, unless the licensee determines that the cybersecurity event has not or is not likely to cause one or more Michigan residents to suffer substantial loss or injury or identity theft.	Michigan Compiled Laws Annotated, 445.72(2) HB 6491
Minnesota	Any Minnesota entity that maintains data that includes personal information that it does not own must notify the owner or licensee of the information immediately following discovery of any breach that resulted in or is reasonably believed to have resulted in acquisition of the personal information by an unauthorized person.	Minnesota Statute Ann. § 325E.61, subd. 1(b)

Mississippi	General Statute: Miss. Code Ann. § 75-24-29 In Mississippi, a person who maintains computerized data that includes personal information that it does not own or license must notify the information's owner or licensee of any breach of security as soon as practicable following its discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person for fraudulent purposes.	Miss. Code Ann. § 75-24-29(4)
Missouri	In Missouri, an individual or legal, commercial, or governmental entity that maintains or possesses records or data which contains personal information that it does not own or license must notify the information's owner or licensee immediately following a discovery of any breach of security, consistent with the legitimate needs of law enforcement (§ 407.1500(2)(2), RSMo). However, notification is not required if, after an appropriate investigation by the third-party custodian or after consultation with the relevant federal, state, or local law enforcement agencies, the custodian determines that a risk of identity theft or other fraud to any consumer is not reasonably likely to occur as a result of the breach. A written record of a determination not to provide notice to potentially affected persons must be maintained for five years.	§ 407.1500(2)(5), RSMo.
Montana	General Statute: Mont. Code Ann. § 30-14-1704 In Montana, a covered entity that maintains computerized data that includes personal information that it does not own or license must notify the information's owner or licensee of any breach of the security of the data system immediately following discovery if the personal information was or is reasonably believed to have been acquired by an unauthorized person. Insurance Information Statute: Mont. Code Ann. § 33-19-321 Any person to whom personal information is disclosed to perform an insurance function that maintains computerized data that includes personal information must notify the licensee or insurance-support organization of any breach of the security of the system immediately following discovery of the breach of the security of the system if the personal information was or is reasonably believed to have been acquired by an unauthorized person (Mont. Code Ann.	Montana Code Ann. § 30-14-1704(2) § 33-19-321(2)
Nebraska	In Nebraska, if an entity maintains computerized data that includes personal information that the entity does not own, the entity must notify the owner or licensee of the information of any breach of the security of the data immediately following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.	Nebraska Revised Statutes § 87-803(2)
Nevada	If a Nevada entity maintains computerized data that includes personal information that the entity does not own, it must notify the owner or licensee of the information of any breach of the security of the data immediately following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.	NRS 603A.220(2)
New Hampshire	In New Hampshire, if an entity maintains computerized data that contains personal information that the entity does not own, the entity must notify the information's owner or licensee immediately following the discovery of any breach of security if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.	New Hampshire RSA § 359-C:20(I)(c)

New Jersey	In New Jersey, any business or public entity that compiles or maintains computerized records containing personal information on behalf of a covered entity must notify the covered entity of any breach of security immediately following discovery if the personal information was, or is reasonably believed to have been, accessed by an unauthorized person. The covered entity must then notify its affected New Jersey customers (see Notice Requirements).	N.J.S.A. 56:8-163(b)
New Mexico	Any person who maintains or possesses computerized data containing New Mexico residents' personal identifying information they do not own must notify the owner or licensee of the breach in the most expedient time possible, but no later than 45 days after discovering the breach.	NMSA 1978, § 57-12C-6(C)
New York	An entity that maintains computerized data that it does not own must notify the owner or licensee of the information of any breach of the security of the system immediately following discovery if the private information was, or is reasonably believed to have been, accessed or acquired by an unauthorized person.	(N.Y. Gen. Bus. Law § 899-aa(3) and N.Y. State Tech. § 208(3)
North Carolina	In North Carolina, an entity that maintains or possesses records or data that includes personal information that it does not own or license must notify the owner or licensee of the information of any security breach immediately following discovery of the breach, consistent with the legitimate needs of law enforcement.	N.C.G.S. § 75-65(b)
North Dakota	In North Dakota, any person who maintains computerized data that includes personal information they do not own must notify the owner or licensee of the information of any data security breach immediately following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.	North Dakota Century Code Annotated § 51-30-03
Ohio	The Ohio breach notification statutes require an entity that maintains computerized data that includes personal information that it does not own must notify the owner or licensee of the information of any breach of the security of the system in an expeditious manner following discovery if, both: • The personal information was, or is reasonably believed to have been, accessed, and acquired by an unauthorized person. • The access and acquisition by the unauthorized person causes, or reasonably is believed will cause, a material risk of identity theft or other fraud to an Ohio resident.	Baldwin's Ohio Revised Code Annotated 1347.12(C) and 1349.19(C)
Oklahoma	General Statute: Okla. Stat. In Oklahoma, an entity that maintains computerized data that includes personal information that it does not own or license must notify the owner or licensee of the information of any breach of the security of a system as soon as practicable following discovery if the personal information was, or if the entity reasonably believes it was, accessed and acquired by an unauthorized person. State Agency Statute: Any covered entity that maintains computerized data that includes personal information that it does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following	Oklahoma Statutes Ann. tit. 24, § 163(C) Tit. 74, § 3113.1(B)

	discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.	
Oregon	An Oregon entity that maintains or otherwise possesses personal information on behalf of another entity must notify the other person of any breach of security as soon as practicable following discovery of the breach if an individual's personal information was included. Effective January 1, 2020, a vendor that discovers, or has reason to believe, a breach of security occurred must notify the covered entity as soon as practicable but not later than ten days after discovery. The Oregon statute defines "vendor" as a person who contracts with a covered entity to maintain, store, manage, process or otherwise access personal information for, or in connection with, providing services to or on behalf of the covered entity. If a vendor has a contract with another vendor that, in turn, has a contract with a covered entity, the vendor must notify the other vendor within the same timeframe as if notification was made to the covered entity. The vendor must also notify the Attorney General in writing or electronically, if the vendor was subject to a breach that involved the personal information of more than 250 customers or an indeterminate number of customers.	Oregon Revised Statutes § 646A.604(2)). S.B. 684
Pennsylvania	In Pennsylvania, a vendor that maintains computerized data that includes personal information that it does not own must notify the owner or licensee of the information of any breach of the security of the system immediately following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.	73 Pennsylvania Statutes § 2303(c)).
Rhode Island	In Rhode Island, any state agency or person that maintains computerized unencrypted data that includes personal information it does not own must directly notify the affected persons of the breach as set out in the sections above (see Notice Requirements, Reporting to Government or Regulatory Agencies, and Notice to Credit Reporting Agencies).	Rhode Island Gen. Laws § 11-49.3-4
South Carolina	General and State Agencies Statutes: S.C. Code Ann. §§ 39-1-90, 1-11-490 In South Carolina, a covered entity that maintains computerized or other data that includes personal identifying information that it does not own must notify the owner or licensee of the information of a breach of the security of the system immediately following discovery, if the personal identifying information was, or is reasonably believed to have been, acquired by an unauthorized person. Insurance Data Security Statute: An insurer licensee that provides insurance services to consumers through independent producers must notify the independent producer of record for all customers affected by a cybersecurity event involving nonpublic information in the possession, custody, or control of the licensee or its third-party service provider, as soon as practicable as directed by the Director of Insurance. The insurer is excused from this obligation if it does not have the current producer of record information for an individual consumer.	South Carolina Code Ann §§ 1-11-490(B) and 39-1-90(B) §§ 38-99-10 to 38-99-100 § 38-99-40(F)
South Dakota	The South Dakota statute does not directly address third-party obligations.	
Tennessee	An information holder in Tennessee that maintains computerized data that includes personal information it does not own must notify the owner or licensee	T.C.A. § 47-18-2107(c)

	of the information of any breach of the security of the system immediately, but no later than 45 days, following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.	
Texas	In Texas, an entity that maintains computerized data that includes sensitive personal information it does not own must notify the owner or license holder of the information of any breach of system security immediately after discovering the breach, if the sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person.	Tex. Bus. & Com. Code Ann. § 521.053(c)
Utah	A person in Utah who maintains computerized data that includes personal information that the person does not own or license shall notify and cooperate with the owner or licensee of the information of any breach of system security immediately following the person's discovery of the breach if misuse of the personal information occurs or is reasonably likely to occur. Cooperation includes sharing information relevant to the breach with the owner or licensee of the information.	Utah Code § 13-44-202(3)
Vermont	A Vermont entity that maintains or possesses computerized data containing personally identifiable information of a consumer it does not own must notify the owner or licensee of the information of any security breach immediately following the discovery, consistent with the legitimate needs of law enforcement.	9 Vermont Statutes Annotated § 2435(b)(2)
Virginia	General Statute: Va. Code Ann. § 18.2-186.6 In Virginia, a person or entity that maintains computerized data that includes personal information that it does not own must notify the owner or licensee of the information of any breach of the security of the system without unreasonable delay following discovery of the breach if the personal information was accessed and acquired by an unauthorized person or the individual or entity reasonably believes the personal information was accessed and acquired by an unauthorized person. Medical Information-Specific Statute: An entity that maintains computerized data that includes medical information that it does not own or license must notify the information's owner or licensee of any breach of the security of the system without unreasonable delay following discovery of the breach of the security of the system.	Va. Code Ann. § 18.2-186.6(D) § 32.1-127.1:05 § 32.1-127.1:05(D)
Washington	An entity that maintains data that includes personal information that it does not own must notify the owner or licensee of the information of any breach of the security of the system immediately following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.	Wash. Rev. Code Ann. §§ 19.255.010(2) and 42.56.590(2)
West Virginia	A West Virginia entity that maintains computerized data that includes personal information that it does not own must notify the owner or licensee of the information of any breach of the security of the system as soon as practicable following discovery if the personal information was, or the entity reasonably believes was, accessed and acquired by an unauthorized person.	West Virginia Code § 46A-2A-102(c))
Wisconsin	In Wisconsin, a covered entity, other than an individual, that stores but does not own personal information pertaining to a Wisconsin resident, who discovers that the personal information has been acquired by an unauthorized person, and has	Wis. Stat. § 134.98(2)(bm)

	not entered into a contract with the owner or licenser of the personal information, must notify the owner or licenser of the personal information of the acquisition as soon as practicable.	
Wyoming	A Wyoming entity that maintains computerized data that includes personal identifying information on behalf of another business entity must disclose to the owner or licensee of the information any breach of the security of the system as soon as practicable following the determination that personal identifying information was, or is reasonably believed to have been, acquired by an unauthorized person. The entity that maintains the data on behalf of another business entity and the owner or licensee of the data may agree which entity will provide any required notice, as only a single notice for each breach of the security of the system is required. If an agreement regarding notification cannot be reached, the person who has the direct business relationship with the affected persons must provide notice.	Wyoming Stat. Ann. § 40-12-502(g)

Appendix G
Resources for Vendor Management Practices

National Cyber Security Alliance, "Stay Safe Online" Resources – October 2018.

FTC Start with Security: A Guide for Business (lessons learned from FTC cases) – June 2015

United States Computer Emergency Readiness Team, "Cybersecurity Tips" – October 2018

Center for Internet Security, 20 Critical Security Controls for Effective Cyber Defense (Version 7.0), -- March 2018

U.S. Department of Justice, Best Practices for Victim Response and Reporting of Cyber Incidents – September 2018

Legal Cloud Computing Association, Cloud Security Standards for Law Firms

General Application
NIST Framework Version 1.1
FINRA's Report on Cybersecurity Practices (Supplemented by Report on Selected Cybersecurity Practices)
SANS Critical Security Controls for Effective Cyber Defense
Identify and Assess Risks-Inventory
Personally Identifiable Information, NIST's Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) (see pages 2-1 and 2-2)
Inventory of PII and Firm Sensitive Information, please see FINRA's Report on Cybersecurity Practices (see pages 12-13)
Identify and Assess Risks-Minimize Use
Minimizing Collection of PII, NIST's Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) (see pages 4-1 through 4-8)
Identify and Assess Risks-Third Party
Vendor Management, FINRA's Report on Cybersecurity Practices (see pages 26-30)

AICPA's Reporting on Controls at a Service Organization; SOC 2 Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy | Publication | AICPA
Questions to ask third parties who access your PII and Firm sensitive information, Standards Information Gathering (SIG) questionnaire (lite version) that firms can use to collect information on vendors (available for purchase).
Protect-Information Assets
Malware Prevention, NIST's Guide to Malware Incident Prevention and Handling for Desktops and Laptops (see pages 6-16)
Password Construction Guidelines, SANS Consensus Policy Resource Community - Password Protection Policy
Protect-System Assets
Identifying Critical Assets to Protect, FINRA's Report on Cybersecurity Practices for a discussion on conducting the inventory, see page 12 (Supplemented by Report on Selected Cybersecurity Practices, see page 3)
Protect-Encryption
Understanding Encryption, FINRA's Report on Cybersecurity Practices (see pages 20-21)
Protect-Employees Devices
Securing Mobile Devices, SANS Institute on Cybersecurity, The Critical Security Controls for Effective Cyber Defense Version 5.0 (see page 19) Version 7.1: https://www.sans.org/critical-security-controls View the Report on Selected Cybersecurity Practices (page 14-15)
Protect- Controls and Staff Training
Vendor Management, FINRA's Report on Cybersecurity Practices (see pages 31-33) (Supplemented by Cybersecurity Checklist, see Section 8)
Detect-Penetration Testing
Conducting Penetration Testing, NIST's Technical Guide to Information Security Testing and Assessment
FINRA's Report on Cybersecurity Practices (see pages 21-22) (Supplemented by Report on Selected Cybersecurity Practices, see pages 13-14)

Detect-Intrusion
Intrusion Detection System, NIST's Guide to Intrusion Detection and Prevention Systems (IDPS)
Response Plan
Issues to Consider when Developing a Response Plan, FINRA's Report on Cybersecurity Practice (see pages 23-25) (Supplemented by Cybersecurity Checklist, see Section 11)
Recovery
Eradication of Cyber breach and Recovery, NIST's Computer Security Incident Handling Guide (see pages 35-37) Cybersecurity Checklist (see Section 12)

Appendix H
Resources for Establishing a Written Information Security Program

The most specific guidance on how to establish a written information security program (WISP) can be found in laws such as New York Cybersecurity Regulations for Financial Services Companies, New York SHIELD Act, and Massachusetts regulations.

A partial index of state data security laws is available from the National Conference of State Legislatures. A chart on data disposal is also available.

APPENDIX I

CERTIFICATES AND ATTESTATION

1) International Standards Organization (ISO)/International Electrotechnical Commission (IEC)

i. ISO/IEC 27001:2013 (*Information technology — Security techniques — Information security management systems — Requirements*) and 27002:2013 (*Information technology — Security techniques — Code of practice for information security controls*) are security management standards. ISO 27001 certifications are possible

ii. ISO/IEC 27701 (*Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*) specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS) in the form of an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management within the context of the organization. ISO 27701 certifications are possible (also requires ISO 27001).

2) Payment Card Industry Security Standards Council (PCI SSC)

i. The PCI Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards from the major card schemes.

ii. Payment brands and acquirers are responsible for enforcing compliance, rather than the PCI SSC.

iii. The PCI SSC website is the only source of official reporting templates and forms that are approved and accepted by all payment brands. These include Report on Compliance (ROC) templates, Attestations of Compliance (AOC), Self-Assessment Questionnaires (SAQ), and Attestations of Scan Compliance for ASV scans. Only these official documents and forms are acceptable for the purposes of compliance validation.

3) Health Information Trust Alliance (HITRUST) Common Security Framework (CSF): HITRUST is a US privately-held company. HITRUST CSF certification is frequently required by organizations that handle PII and it enables vendors and covered entities to demonstrate compliance to HIPAA requirements based on a standardized framework.

4) American Institute of Certified Public Accountants (AICPA)

i. Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization, was finalized by the Auditing Standards Board of AICPA in January 2010. SSAE 16 effectively replaces SAS 70 as the authoritative guidance for reporting on service organizations.

ii. Statements on Standards for Attestation Engagements in SSAE No. 18, Attestation Standards: Clarification and Recodification. The SSAE 18 SOC 1, sometimes just stated as SOC 1, is the report you get when you are audited for SSAE 18. The SOC 2 is a separate report that focuses on controls at a service provider relevant to security, availability, processing integrity, confidentiality, and privacy of a system. The SOC 1 and SOC 2 reports come in two forms: Type I and Type II. Type I reports evaluating whether proper controls are in place at a specific point in time. Type II reports are done over time to verify operational efficiency and effectiveness of the controls.

5) Cloud Certifications

i. Cloud Security Alliance (CSA) Security Trust Assurance and Risk (STAR)
   - CSA STAR Attestation is a collaboration between CSA and the AICPA to provide guidelines for CPAs to conduct SOC 2 engagements using criteria from the AICPA (Trust Service Principles, AT 101) and the CSA Cloud Controls Matrix. STAR Attestation provides for rigorous third-party independent assessments of cloud providers. Attestation listings will expire after one year unless updated.
   - The CSA STAR Certification is a rigorous third-party independent assessment of the security of a cloud service provider. The technology-neutral certification leverages the requirements of the ISO/IEC 27001:2013 management system standard together with the CSA Cloud Controls Matrix. Certification certificates follow normal ISO/IEC 27001 protocol and expire after three years unless updated.

ii. Federal Risk and Authorization Management Program (FedRAMP): FedRAMP is a U.S. Government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. This approach uses a "do once, use many times" framework that saves cost, time, and staff required to conduct redundant Agency security assessments.

6) DoD Cybersecurity Maturity Model Certification Program

Starting in Government Fiscal Year 2021, which began in October 2020, DoD is selecting up to 15 DoD programs to serve as pilot programs for requiring third party certification that the contractor or suppliers' systems at any tier are managed at a specified maturity level, which ranges from Level 1 (performs Basic Cyber Hygiene) through Level (optimizing Advanced/Pro-active cybersecurity). CMMC will gradually implemented over the next 5 years until it applies to all DoD contracts in October 2026. The third-party assessors are being accredited by a new non-profit organization, the CMMC Accountability Board (CMMC AB). You can learn more about CMMC at https://www.acq.osd.mil/cmmc and the CMMC AB at https://www.cmmcab.org/. Starting in November 2020, even if not subject to CMMC, DoD contractors and subcontractors will need to conduct NIST 800-171 self-assessments of covered internal networks and provide their scores to DoD to be eligible for award, and also will be subject to DoD audits of its NIST 800-171 implementation. *See* DFARS 252.204-7019 and 7020.

Additional Activities of Interest

i. NIST
   - NIST Cybersecurity Framework
   - NIST SP 800-53 Revision 5
   - No certifications available

ii. Control Objectives for Information and Related Technologies (COBIT): COBIT is a framework created by the Information Systems Audit and Control Association for IT governance and management. Professional certification available.

iii. The Committee of Sponsoring Organizations of the Treadway Commission (COSO): COSO is a joint venture sponsored by five professional associations: the Institute of Management Accountants (IMA), the American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), the Institute of Internal Auditors (IIA), and Financial Executives International (FEI). COSO developed a model for evaluating internal controls. This model has been adopted as the generally accepted framework for internal control and is widely recognized as the definitive standard against which organizations measure the effectiveness of their systems of internal control. Professional certification available.

iv. North American Electric Reliability Corporation (NERC): NERC is a not-for-profit international regulatory authority whose mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid. NERC develops and enforces Reliability Standards; annually assesses seasonal and long-term reliability; monitors the bulk power system through system awareness; and educates, trains, and certifies industry personnel. NERC's area of responsibility spans the continental United States, Canada, and the northern portion of Baja California, Mexico. NERC is the Electric Reliability Organization (ERO) for North America, subject to oversight by the Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada. Professional certification available.

v. Information Technology Infrastructure Library (ITIL): ITIL is a framework for managing IT service delivery around the world. ITIL defines a service lifecycle model that prescribes specific processes and activities during the design, development, delivery, and support of IT services. Professional certification available.

vi. Information Security Forum (ISF): ISF is an independent, not-for-profit organization that is dedicated to investigating, clarifying and resolving key issues in information security and risk management, by developing best practice

methodologies, processes and solutions that meet the business needs of its members. One of the key tools is the ISF Standard of Good Practice for Information Security.

vii. The Technical Committee on Cyber Security (TC CYBER): TC CYBER is a subcommittee or division of the European Telecommunications Standards Institute (ETSI). TC CYBER is recognized as a major trusted center of expertise offering market-driven cyber security standardization solutions, advice and guidance to users, manufacturers, network, infrastructure and service operators and regulators.

viii. Consensus Assessments Initiative Questionnaire (CAIQ): CAIQ assesses what security controls exist in IaaS, PaaS, and SaaS services. This is for cloud service providers seeking certification. Typically requires ISO 27001 certification first. If provider has CSA Star Certification, then it has already run the gauntlet on this. Customer can look and see on what criteria they were assessed.

ix. ISO 27701 – privacy controls extension if you're worried about GDPR or CCPA.

x. SOC2 and SOC3

xi. Statement on Standards for Attestation Engagements (SSAE) 18 - Auditing standard for financial service organizations, produced by American Institute of Certified Public Accountants (AICPA)

xii. CSA developing a new credential for cloud auditors.

APPENDIX J

CONTRACT PROVISIONS: TERMINATION

1) Transition Plan Sample Provision

Except when terminated by Supplier for a default by the Client as set forth in Section ___ and such default remains uncured, in which case Supplier shall have no obligation to continue to provide Services or Termination Assistance to Client, in connection with the natural expiration or any other termination of this Agreement, the Parties will, commencing promptly after the giving of any notice of termination or at least one hundred eighty (180) days prior to expiration of this Agreement in accordance with its terms, jointly develop a plan, to effect the orderly transition to Client or its designee from Supplier the Services then being performed or managed by Supplier. Such plan will be completed by the Parties within thirty (30) days and will set forth the tasks and actions to be performed by Supplier and Client, the time for completing such tasks and actions, and the criteria for declaring the transition completed. The Parties and their employees and agents will cooperate in good faith to execute such plan and each Party will perform those tasks and actions assigned to it in such plan. The Termination Assistance services will be invoiced and based on the same charging metrics as those used in calculating the Fees, or if not applicable, at the rate card rates in effect on the date of termination or expiration. Client will pay Supplier monthly, in advance, for any costs or expenses (mutually agreed in writing in advance of performing the service) and reasonably incurred by Supplier in delivering those portions of Termination. Any necessary decommissioning services shall also be charged to Client as part of Termination Assistance services hereunder. Notwithstanding anything herein to the contrary, if Supplier terminates this Agreement based upon the material breach of the Client, then Supplier agrees to provide Termination Assistance to the Client only if Client pays in full any outstanding invoices and deposits into escrow, with a party acceptable to Supplier and upon such terms and conditions as are acceptable to Supplier, funds in an amount equal to Fees for six (6) months of Services and Termination Assistance at the then applicable rate. The escrow agreement will provide, at minimum, if Client fails to pay any invoice for Services and/or Termination Assistance when due Supplier shall have the right, without notice to Client, to present the invoice to the escrow agent and immediately receive escrowed funds in the amount of the outstanding invoice. Supplier may stop Termination Assistance Services if there is not at least three (3) month's Fees in escrow at any time. Upon expiration or termination of the Agreement, after completion of transition to a successor Supplier, each Party will return or clear, purge, and destroy the other Party's Confidential Information.

2) Offboarding/Turnover Obligations

Often lost in the negotiation process is the "on-boarding" and "off-boarding" of data as clients move between service providers. If a client wants a vendor to process data that is presently NOT under an existing agreement, then the transition services language will address the potential for off-boarding or later transferring the data to a different vendor when the existing vendor is terminated. B below are typical provisions describing the services vendors will provide when they undertake a new client or terminate an existing one. In either scenario, an agreement will have

identified the type of data that is being collected, transmitted, processed, and maintained, and always with applicable and appropriate security measures in place.

i. On-Boarding or Transition Services

Supplier will perform or cause its Subcontractors to perform (as the case may be) the Supplier functions and services reasonably necessary to facilitate the prompt transition of the Services from Client's existing service provider to Supplier, as described in the Transition section of a SOW to be signed by the parties. Client shall perform (or have performed) the Client Responsibilities in the SOW. Client shall also fully cooperate with Supplier and cause Client's existing service provider to cooperate with Supplier to coordinate the transition of the Services, including executing any and all necessary documentation and notices to the existing service provider to deliver Client Data to Supplier. Supplier shall have no liability hereunder or otherwise for any failure of and/or delay in the transition of the Client Data and/or Services to Supplier caused by the acts and/or omissions of any existing third-party service provider Client or any party unrelated to Supplier.

ii. Off-Boarding or Termination Assistance

Except when terminated by Supplier for a default by the Customer and such default remains uncured, in which case Supplier shall have no obligation to continue to provide Services or Termination Assistance to Customer, in connection with the natural expiration or any other termination of this Agreement, the Parties will, commencing promptly after the giving of any notice of termination or at least _____ (__) days prior to expiration of this Agreement in accordance with its terms, jointly develop a plan, to effect the orderly transition of Supplier's Services from Supplier to Customer or its designee. Such plan will be completed by the Parties within ____ (__) days and will set forth the tasks and actions Supplier and Customer agrees to perform, the time for completing such tasks and actions, and the criteria for declaring the transition completed. The Parties and their employees and agents will cooperate in good faith to execute such plan and each Party agrees to perform those tasks and actions assigned to it in such plan. Fees for Termination Assistance will be based on the same charging metrics as those used in calculating the fees under the Agreement. Customer agrees to pay Supplier monthly, in advance, for any costs or expenses Supplier reasonably incurs. Any necessary decommissioning services shall also be charged to Customer as part of Termination Assistance Services hereunder. Notwithstanding anything herein to the contrary, if Supplier terminates this Agreement as provided in this Section, Supplier agrees to provide Termination Assistance to the Customer only if Customer pays in full any outstanding invoices and deposits into escrow, with a party acceptable to Supplier and upon such terms and conditions as are acceptable to Supplier, funds in an amount equal to fees for ____ (__) months of Services. The escrow agreement will provide, at minimum, if Customer fails to pay any invoice for Services and/or Termination Assistance when due Supplier shall have the right, without notice to Customer, to present the invoice to the escrow agent and immediately receive escrowed funds in the amount of the outstanding invoice.