IRON MOUNTAIN®

SUPPLY CHAIN RISK MANAGEMENT IN LAW FIRMS: GETTING STARTED AND PRACTICAL GUIDANCE

2021 LAW FIRM INFORMATION GOVERNANCE SYMPOSIUM

CONTENTS

AUTHORS:

BRIAN DONATO
Chief Information Officer
Vorys, Sater, Seymour and Pease llp.

BETH FAIRCLOTH
Client Services Director
Jones Day

RODNEY MILLER
Director of Business Information Governance
Alston & Bird LLP

DERICK J. ARTHUR
Director of Records & Information Governance
King & Spalding LLP

PATRICIA FITZPATRICK, CPA, CIGO
Senior Director of Compliance and Information Governance
Seyfarth Shaw LLP

GALINA DATSKOVSKY, PhD, CRM, FAI
Board of Directors
Open Axes

RUDY MOLIERE
Director of Information Governance
Morgan Lewis & Bockius LLP

ROBERT WEAVER
CHIEF RISK & SECURITY OFFICER
BLANKROME

KATHERINE WEISENREDER
Information Governance Compliance Manager
Cooley LLP

CHRIS EDWARDS, CISSP, CISM, CISA
Cyber Risk Manager
King & Spalding LLP

MICHELE GOSSMEYER
Global Director, Information Governance, Risk & Compliance
Dentons

JENNIFER CARLSON
Privacy Consultant
Kyndryl

EXECUTIVE SUMMARY

Law firms are no stranger to attacks on their supply chain where the intended target is often a lawyer, staff member or client. If businesses, including law firms, suffer a data breach due to their own, or that of their sub-contractors, mishandling of data, it can result in significant client / business loss, reputational damage and significant financial impact. According to the Ponemon Institute's "Cost of a Data Breach Report" published by IBM Security, the average cost of a breach in 2020 was $3.86 million. This is not insignificant even for the largest law firms. In addition to security, as well as risk and reputational brand management, law firms are now subject to various supply chain requirements from clients, including equity, resiliency and social responsibility.

The primary factors driving law firms to adopt Supply Chain Management programs included in this paper are: 1) Client Information Governance Requirements "CIGRs" (outside counsel guidelines "OCGs", master service agreements "MSA", collectively "Agreements") that not only require the firm to adhere to the client's security standards, but require the firm to pass those provisions down to any third or fourth parties engaged, 2) domestic and international data privacy laws and regulations, including GDPR and CCPA/CPRA, 3) industry regulatory requirements if your firm is considered a governmental, health care or other specialized industry contractor, and 4) insurer requirements relating to your Supply Chain Management as part of the underwriting questionnaire for cybersecurity coverage.

We also address key areas of Supply Chain Management with a particular focus on risk management related to information governance. We look at who in your firm can serve critical roles aligned with risk operations, and finally, we address contracting points, tools and processes to best protect you, your clients and the industries involved.

WHAT IS SUPPLY CHAIN MANAGEMENT?

Supply Chain Management is the handling of the entire production flow of a good or service to maximize quality, delivery, customer experience and profitability[1]. Supply chains are typically more of a web than linear; Supply Chain Management and its relevance constantly evolve. As recently as April of 2021, manufacturing.net[2] highlighted new areas of focus, beyond the standard delivery of product/services that drive managing the supply chain. These newer key aspects include: 1) health equity and the need for focus on full delivery 2) resiliency and the ability to be more adaptable and robust to unforeseen shocks and 3) corporate social responsibility, supplier diversity and sustainability, as these are increasingly being demanded by shareholders.

Supply chain and its associated logistics are most commonly thought of as impacting consumer industries such as grocery, automotive, energy and manufacturing. The CoVid19 pandemic has certainly demonstrated the importance of supply chain logistics in the healthcare industry. The distribution of vaccines exposed us to many of the insider challenges and risks of global logistics planning. Other recent news about Supply Chain Management includes the impact of lumber shortages on the construction and housing markets and semi-conductor chip shortages on the supply of computers for businesses in just about every industry. And of course, the 2021 Suez Ship Canal blockage affected nearly every industry across numerous countries, impacting approximately 12% of global trade[3].

WHY IS IT IMPORTANT TO LAW FIRMS?

So why is Supply Chain Management and its evolution important to law firms? As those in the legal industry know, a significant amount of time and resources are devoted to third-party risk in Supply Chain Management, where law firms are typically viewed as 'vendors' of the world's largest companies. All of the supply chain impacts listed above are in industries that are either clients and/or vendors of just about every law firm on the planet. And most every client industry represented by law firms requires some form of assessment of how the firm handles and secures their data. In turn, law firms must assess their vendors, such as those who supply their computers, manage their critical data, store their backups in the cloud or in off-site storage facilitates, write their software code or even have access to their physical space to water their plants or clean their offices. Many such vendors have their own suppliers, sub-contractors, contract and temporary employees and so forth. This is even more typical in today's distributed work environment. One quickly begins to see the web, versus linear, supply chain reference above and the complexities of (and impacts of not) managing the risks associated with it.

Some attacks on the supply chain that have directly impacted law firms include the recent SolarWinds attack which was used to send malicious code to many systems in their supply chain[4], and the breach of the secure file-sharing platform Accellion which threatened to post sensitive stolen data[5]. Both of these examples highlight how critical it is to know who is in your supply chain and how each member of the chain assesses and helps ensure the security of their service/product delivery. Of course, remember that law firms are a supplier to other companies as mentioned earlier, and attackers may want to gain access in order to breach entry into a client's trusted environment. Trusted entry can occur in the physical office space or on the firm's computer systems. Awareness of being a consumer of supply chain services, as well as being a provider, is important in building greater awareness of the need for caution as described in this paper.

Much can be said about assessing risk when selecting vendors. Many firms simply have the vendor fill out a questionnaire, similar to what firms fill out for their clients. However, a closer look and consideration should be given to this issue during vendor selection. A problem that many law firms in particular have to deal with is the lack of a central procurement department. Since attorneys, practice groups and departments often select vendors, it is essential to develop procedures and ensure they are followed uniformly to protect the data assets of the firm. This is easier said than done. The process needs to be clearly defined, allowing decisions to be made quickly but securely. Any perception of unnecessary delay can jeopardize adherence to the process. Questionnaires and other materials should be readily available to all and communication is key. The most effective way to socialize the process is to explain to the stakeholders how this necessitates the firm to onboard clients they might otherwise need to decline.

The case study presented in Appendix I provides insight on how to get a Supply Chain Management program off the ground. An example to justify the need for such a program is found in a California training company that won a large contract with a major insurance vendor. The training company used subcontractors who could not meet the security and privacy requirements of the client. They quickly had to scramble and buy an appropriate solution to make themselves compliant with client regulations and provide evidence of the training of their subcontractor ecosystem. If the clients of your firm demand defined levels of security, make sure that those who select technology understand the requirements.

An additional layer of focus includes your physical security. Improving physical security includes safeguarding offices, securing data centers and protection against natural disasters such as power outages, fires, floods and other cases of severe weather. Various systems and suppliers need to be put in place to proactively manage numerous types of natural disasters[6].

ACCORDING TO THE 2020 COST OF A DATA BREACH REPORT

10% of malicious breaches in the study were caused by a physical security compromise, at an average cost of $4.4 million

RISK MITIGATION STRATEGIES

There are essentially two risk mitigation strategies which should be considered when assessing a vendor. One is the practical protection of information and the assessment of the vendor's abilities to do so. The second is having appropriate legal protections and assurances should the vendor suffer a breach that includes your data.

PRACTICAL PROTECTION / VENDOR ASSESSMENT:

A Supply Chain Management Program should require vendors to complete comprehensive questionnaires, no matter who contracts them. There are, however, items that are frequently overlooked in a standard assessment that we suggest be included:

1. Does the vendor allow work-from-home for its workforce? Some form of remote working is likely more common due to the pandemic. If the answer is yes, what steps are taken to protect employees' equipment at home, especially if "bring your own device" (BYOD) is allowed? Will the firm's data make its way locally to those machines? How is it controlled when there? How is it brought back to the vendor's system? If the vendor subcontracts to various providers, what is the process of making sure the data itself is not proliferated? **Many vendor assessment questionnaires omit data leakage components**. Often it is up to the Information Governance professional to point this out.

2. If the vendor has suppliers down the supply chain, are they being assessed? How is data security maintained when subcontractors are given access to the data? Make sure it is clear how access is controlled and what guarantees the vendor is willing - or able- to make related to data. Subcontractors must be held to the same standard contractually as the supplier.

3. Frequently in remote work or supply chain situations, shared or collaborative work spaces such as Microsoft365 Teams or Google Drive are utilized. It should be clear exactly how the information is governed. Access control, download and check-in policies are always important and should be part of any questionnaire.

In some instances, very large vendors may be less willing to modify their methodologies or disclose requested information. As an example, Amazon and Microsoft may not accommodate customized processes for smaller clients such as law firms. Fortunately, such vendors are conscientious about their data practices and many have received certifications documenting their adherence to defined frameworks such as SOC2, ISO and NIST. Nonetheless, it is important to request their standards and procedures and to analyze them as sufficient for the firm. Conversely, a potential advantage of smaller vendors is that they are often more willing to work with clients in a customized fashion. On the downside, smaller vendors may not be as sophisticated, may not have complex security protocols and may not have formal ISO or SOC 2 certifications in place. Regardless of the vendor's flexibility or how they are publicly perceived, the buck always stops with you, as you are ultimately responsible for the data that your clients entrust to your firm.

LEGAL PROTECTION & ASSURANCES

While this section of the paper discusses legal protections and assurances, it is not intended to provide legal advice. The comments provided should be used to start a conversation with your internal legal counsel so that you can have a guided discussion. It is common practice for firms to obtain NDAs from its vendors, especially when data is shared. The use of an indemnification clause should be discussed with your internal counsel in the context of when the vendor experiences a data breach. This scenario also gives rise to the need to review the stated insurance coverage limits with your legal advisor. When subcontractors of a vendor are involved, it is up to the vendor to establish appropriate contractual terms with their providers. The firm will hold the vendor with whom they have contracted responsible for any breach, even if a subcontractor is at fault. Ensure that you have standard and consistent language to help clarify your requirements. Also be sure that your NDAs and MSAs include a right to review clause so that you can appropriately explore the components above should you need further validation or assurance.

Supply chain security provisions in legal services contracts are articulated in CIGRs and/or information security sections or appendices. Many client cybersecurity risk assessments contain sections that make extensive inquiries regarding the law firm's vendor risk assessment (VRA) process. As stated in the previous section, this is a result of the need to secure client data throughout the legal service relationship, whether it is confidential company information or personal data protected under jurisdictional regulations such as GDPR or HIPAA.

Many clients explicitly require law firms to provide and enforce all agreement provisions with any third-party vendors engaged by the firm to assist with the engagements. The Association of Corporate Counsel (ACC) created a document to attempt to standardize information protection and security control provisions in outside counsel guidelines, and Supply Chain Management is a central component to the document (Model Information Protection and Security Controls for Outside Counsel Possessing Company Confidential Information). These agreements often require the firm to request approval from the client before engaging matter-specific vendors (e.g., expert witnesses, consultants, eDiscovery services, court reporters or deal rooms). Be sure to carefully review and limit, where appropriate, when the client requires explicit approval. It is not realistic, for example, to have clients approve the hiring of every technology service contractor. This approach is not feasible because it would require third parties to constantly renegotiate and agree to new terms and would create a logistical nightmare for the law firm. Utilizing a separate agreement allows a firm to respond to client requests that require third parties to agree to substantially the same terms binding the firm. Appendix III of this paper provides additional guidance for the modification of the vendor's agreement or the development of a universal firm drafted privacy and security agreement.

One method for managing the third-party vendor provisions is to provide notification to attorneys and staff on the matter team servicing the client. Some firms accomplish this through software that sends a summary of the client agreement, including vendor provisions, to anyone who bills a client for the first time. Some law firms have started to develop matter-specific VRAs designed to assess vendors for the purpose of performing sub-contract work for clients. Law firms should consider centrally managing the engagement of matter-specific vendors, including the documentation of the client's approval of the vendor as part of the procurement process. This is of particular importance when engaging any vendor who would have direct access to the client's data for any purpose.

In addition to finding provisions in Agreement sections labelled Third-Party Service Providers, related provisions are often found in various sections labelled Insurance, Data Processing/ Security, Background Checks, Business Continuity or Business/Material Change Notification. These provisions may require the law firm to provide notice to the client when technology infrastructure is changed or modified. They may also require the firm to perform background checks for subcontractors who perform work on the its core systems just as they would full-time employees since they would have access to the same client data.

If your law firm takes a "divide and conquer" approach to reviewing the OCGs by doling out the various sections to specific administrative departments, it is important to educate all reviewers regarding the implications of these provisions. All reviewers need to be on the lookout to determine how these requirements affect the firm's engagement of vendors used to provide legal services to a specific client or to support the operations of the firm.

Law firms regularly provide information in client risk assessment questionnaires about the VRA process or how they secure data in internally managed repositories. However, they should be wary of making vendor agreements subject to the multitude of client engagement terms, as they can vary greatly by client. Important areas include: clients' confidentiality expectations, need-to-know access controls and general security and privacy training for legal support, and whether there is an expectation that the law firm cascade those expectations to the vendors. It would be impossible for a law firm to manage its operations while abiding by conflicting client requirements. Therefore, it is important that a firm understand the extent to which the client's third-party provisions apply.

BREACH NOTIFICATION PROVISIONS

While many clients push provisions for breach notification requirements that establish full and direct liability for all firm vendors onto the firm, agreement to such terms can quickly put the firm in jeopardy of falling out of alignment with its own liability insurance. Firms should carefully review any such language, but the reality is that some clients will not budge on their expectations; in those cases, the appropriate department (e.g., General Counsel's office, IT or Procurement) should be consulted to help negotiate a balanced approach.

Because of liability, and in order to avoid bringing on redundant capabilities through various vendors, many firms recommend that clients execute agreements directly with vendors that process client matter data. Examples of these types of vendors include expert witnesses, trial experts, eDiscovery hosting providers and corporate deal rooms. Firms should be proactive about standardizing their obligations around the language for breach notification. While some clients may require immediate notification of any suspected accident, others may have more reasonable "without undue delay" obligations for notification of a confirmed breach. These terms are worth defining in the Agreement to avoid inconsistency and to ensure adequacy of the firm's internal IT alerting procedures. The agreed commitment ideally balances the firm's reasonable ability to provide valuable information with the client's ability to manage the volume of notifications, resulting in actionable, applicable intelligence. For example, if a client gets hundreds or thousands of 'potential breach' notifications from each of their law firms every day it is doubtful they can digest and action that information effectively. Keep in mind that by some clients' standards, an attorney leaving a firm laptop open without locking it in his own home may constitute a "potential breach". A "potential breach" could also include lost phones, tablets, stolen or misplaced laptops, and other events that could be low-impact if encryption and remote wipe tools are effectively deployed on the device.

Breach notifications include those that are required to authorities as well as requirements to notify affected data subjects whose information was breached. OCGs require support in providing information to the client so that the client can uphold obligations to report the breach to authorities and to data subjects as needed. Realistically, the notification sent to a data subject would be best received from the company she or he would be most familiar with. Conducting a tabletop exercise with the client is one such way that this could be achieved.

> IT'S WORTH CONFIRMING HOW A BREACH RESPONSE EFFORT WOULD WORK BEFORE A BREACH OCCURS SO BOTH PARTIES ARE FAMILIAR WITH THEIR ROLES AND RESPONSIBILITIES IN ANY SUCH SITUATION.

GDPR

Many law firms take the stance of operating under data protection laws as "data controllers" since they make independent decisions regarding the purpose and the means by which personal information is processed. Other firms may operate in certain circumstances as data processors, where firms are obligated to process client personal information only under the direct instructions of the client.

While firms are often controllers, they are frequently asked to agree to processor-like provisions about use of data and deletion requirements at the close of a matter. It is worth ensuring that your clients understand and agree to your firm designation under GDPR or Business under CCPA in relation to the data entrusted to you.

Consider GDPR fines when you contemplate the limitations of liability set out in Data Processing Agreements (DPAs) and in MSAs. These can be up to 4% of top line revenue (i.e., before taxes) or 20 million Euros whichever is greater, which is nothing to ignore. Waterfall obligations from controller to processor and then down to sub-processors apply, but that's the responsibility of your processors since it should be expressly stated in your DPA with all vendors processing personal data as (Sole) Controllers, Joint Controllers and Processors.

Keep in mind that there are many data types not covered by standard GDPR-compliant data processing agreements since they're scoped for only personal data and don't expressly cover intellectual property rights of ownership, trade secrets, confidential strategic plans, M&A details or other types of sensitive, confidential and proprietary information.

NDAs and employee confidentiality agreements extend attorney responsibilities down to those acting in the capacity as processors of the firm. Additionally, background checks are maintained for employees and contractors, heightening the protections afforded to the data processed by the firm.

WHO IS INVOLVED IN THE PROCESS?

The inclusion of supply chain security requirements is creating a fundamental shift in the way attorneys handle the engagement of vendors for legal work. Attorneys are accustomed to engaging directly with client-specific vendors such as local counsel, experts, court reporters, eDiscovery consultants and other service providers. While the client may be aware of the need to engage a particular vendor, and may have verbally approved it for the matter, it may or may not have been listed in the engagement letter. Typically, client or matter specific vendors invoice the law firm, then the firm pays the vendor and seeks reimbursement from the client. Due to the decentralized nature of this process, the firm may not have a copy of the vendor agreement in a central repository with the only copy existing in the attorney's client file.

With the advent of State and Province enacted data privacy regulations, as well as GDPR, comes the requirement to document who handles personal data and why. Client risk assessments are also driving a need for change in this process. Clients may ask law firms to provide information about all vendors who have access to client data. If the matter-specific vendor process is not centralized, the law firm administrative teams responsible for responding to these questions need to poll the attorneys for a complete answer. At a minimum, firms should consider establishing standard procedures for attorneys to engage vendors for client work with template agreements and centralized documentation. When it comes to processing data, law firms have started to vet eDiscovery consultants and service providers through the vendor assessment process. Following adequate due diligence and vetting, firms should establish master service agreements with vendors, including data processing agreements where appropriate. Some law firms may want to consider centralizing the management of contracting with vendors for client engagement through a procurement department.

It is often the role of the law firm's office of general counsel (OGC) to oversee the review of all firm contracts and engagements, whether it involves clients or vendors. The OGC may review these documents or provide instructions and criteria for the risk department or appropriate group to review the contracts and risk assessments. The OGC is uniquely positioned to inform law firm management of these requirements and how breaching them may have broader regulatory implications. This law firm management to develop an approach and strategy for handling these requirements.

Typically, law firms have an accounts payable team within the finance or accounting department which is responsible for reviewing invoices and vetting appropriate approvals, coding invoices, minimizing duplicate payments, collecting required tax forms such as a W-9 or W-8 and issuing payments. Firms with more advanced processes are likely to have a dedicated procurement function to maintain vendor evaluations, on-boarding processes and overall supplier relationships. Having a centralized and defined process allows the firm to consistently evaluate five pillars of risk associated with each vendor:

- conflicts risk with current and potential firm clients
- business risk with vendors that may be defendants in lawsuits brought against them by their customers
- reputational risk with vendors that may be perceived as not operating ethically or have had negative press
- financial risk with vendors that have weak credit scores, or have even filed for bankruptcy; and
- information security risk by not having proper controls in place to protect their systems and data.

Conflicts and library personnel typically run searches to identify potential business risks and corporate responsibility reporting. In some firms, procurement also negotiates pricing, favorable contract terms and holds the vendor accountable to meeting agreed upon service levels. Absent a defined procurement function, most firms defer to the individual that has the business relationship with the vendor to perform this analysis, which likely is not being done consistently, if at all.

Due diligence performed by *privacy and security* professionals is key before onboarding a new vendor. Firms should consider the risks, costs and benefits of involving organizations that provide services supporting client matter data processing. Security reviews can highlight gaps in vendors' programs that firms can proactively work to account for or remediate, or firms can seek alternative vendors that are better able to meet expected security standards. Security questionnaires should ask the vendor about its screening process when on-boarding new employees. If the vendor does not already perform background checks, especially related to criminal offenses, then you may want to involve your human resources department so they can order the background check.

Vendors may not be familiar with their obligations or the relevance of data privacy coverage if they're not clear on the definition of data processing under relevant legislation (e.g., GDPR and CCPA), therefore reviewing the obligations and communicating the purpose of the DPA and details of processing on the front-end is essential. Vendors also may not realize that they're processing data by simply accessing or hosting it. Explaining the broad definition of processing may be required to reach an accord about the data privacy coverage.

Adequate privacy coverage in vendor contracts may require consideration for data transfers. Be aware that some vendors may not understand they are transferring data. If European personal data is processed by stateside processors for your firm, then an approved mechanism for international data transfers is likely required. Legal transfers can be accomplished by having the proper legal documentation to support the transfer.

Any well executed risk program is likely to identify issues that either need to be mitigated or accepted. It is likely that your program will shine a light on at least a few suppliers that fall below the firm's appetite for risk tolerance. When this occurs, you may need to consult with your executive management team and internal counsel to determine the appropriate next steps which may sometimes include termination of the supplier relationship.

WHAT TECHNOLOGIES?

Technologies to help with Supply Chain Management fall into a few buckets: those that help track requests, launch assessments, manage contracts and/or monitor security ratings.

Firms may be overwhelmed with the number of internal requests for third party vetting. To that end, leveraging a ticketing or tracking system to manage requests and reduce gaps may be useful. If your firm has a service desk ticketing system, it may be simplest to create a queue for this purpose, otherwise an Excel spreadsheet or SharePoint site can work just as well.

Vendor risk assessment tools aid to centralize the distribution of questionnaires, analysis of responses and remediation of issues flagged during analysis. Security rating tools offer dynamic measurements of an organization's cybersecurity posture through continuous monitoring. Ratings are a useful point of reference both when onboarding a vendor as well as continuing to monitor the efficacy of controls agreed to between firm and vendor. Some vendors offer both risk assessment tools and security rating services, including an option for an on-site audit of the supplier's facility. Others focus on one aspect or the other. An overview of tools in this space can be found here: https://www.gartner.com/reviews/market/it-vendor-risk-management.

Contract management tools may satisfy a number of issues in the Supply Chain Management workflow, as they tend to have features to set up a workflow; create new tickets; adjust existing tickets; provide workflow alerts and clarity on assignments; ingest vendor side email give business user visibility into status; intake form capabilities, document collaboration capabilities, contain clause libraries, enable native document comparisons, audit trails, dashboards and reporting; and even integrate with other systems. If you have a team of corporate or other transactional lawyers, you may already license tools that you could use.

ADDITIONAL SUPPLY CHAIN MANAGEMENT CONSIDERATIONS

Other key initiatives related to supply chain vendor management that were not the focus of this paper include equity, resiliency and social responsibility. The importance of these social consciousness metrics in equitable global business development has grown tremendously for organizations of all sizes in recent years. The importance of these initiatives for law firms was highlighted in The American Lawyer article, "Three Procurement Priorities for Law Firms in 2019." The article discussed the three priorities of 1) supplier risk, 2) supplier relationships and 3) supplier diversity. In order to meet the risk requirements discussed in this paper as well as supplier diversity and related social responsibility metrics, law firms will need to develop appropriate staffing structures and processes. These structures and processes are essential for the initial collection and on-going maintenance of supplier diversity metrics in order to remain responsive to their clients' commitment to selecting law firms who reflect their commitment to utilizing diverse suppliers.

CONCLUSION

This paper provides practical guidance and tools compiled from actual procedures in place at an assortment of large firms in various stages of maturity with respect to their internal Supply Chain Management program. Appendix I speaks to getting started with supply change management at your firm. Appendix II provides a practical summary of how one firm has put into practice several of the recommendations provided throughout this paper. It provides a description of the talent and processes employed by the firm to implement the risk mitigation strategies described earlier. While not every firm may have access to all of these resources, this paper lays out the framework that allows you to develop your own roadmap to move towards accomplishing your firm's Supply Chain Management goals.

Developing a robust program does not happen overnight. It requires significant research, planning and development, and, importantly, sound organizational change management. Engaging a multi-disciplinary team is a key component to the successful implementation of your program. Start small and identify a few new vendors to test the process before it is announced to the firm. Doing so you to foster support and engage internal advocates that can help spread the word and build trust. Use this opportunity to refine your procedures then get ready to launch the program. As is the norm, be sure you have top-down support from your General Counsel, Managing Partner, CIO, CFO and others – you may need to lean on them when you encounter resistance. Involve your marketing department to build creative messaging and storytelling as part of your training and awareness campaign. Don't be afraid to adjust the program along the way. Being a successful change manager requires that you are able to quickly identify what isn't working and fix it. Finally, develop an elevator pitch and share it with your team. Everyone needs to be able to succinctly describe why Supply Chain Management is so important in today's complex global economy. Doing your homework to really know your vendors and how they operate make you aware of risks that either need to be accepted or mitigated which allows you to enter into agreements with your eyes wide open.

APPENDIX I

CASE STUDY 1: GETTING STARTED WITH SUPPLY CHAIN MANAGEMENT

There are many things that a firm can do to get started with a Supply Chain Management program, a number of which can be accomplished with little or no additional cost to the firm. Utilizing existing systems and personnel, the firm can leverage these resources in the development of a formal Third-Party Risk Management Policy and related processes to support the policy. A key element to this policy is the Risk Scoring Matrix. This defines matrix outlines how vendors are categorized and assigned a tier for risk. Below is an example of what that might look like. Each firm should define its own examples and have internal discussions with a collaborative team of representatives from various departments (i.e., information technology, data privacy, data security, information governance, office of general counsel practice group leaders, procurement and finance) to agree upon which categories of vendors pose the highest risk to their firm.

RISK SCORING MATRIX

Tier 1 Attributes - Highest Risk *(If any attribute met, then Tier 1)*	**Tier 2 Attributes- Moderate Risk**	**Tier 3 Attributes- Lowest Risk**
Stores, processes or hosts client confidential information or firm proprietary information	Provides maintenance or support for client confidential information or firm proprietary information stored on premise	Does not have access to client confidential information or firm proprietary information, only public information
Supports critical business functions or provides unique services to firm	Support essential business functions	Services are not critical; easily replaced
Limited pool of available vendors providing same products or services	Moderate pool of available vendors providing same products or services	Large pool of available vendors providing same products or services
Requires access to PII/PHI/PCI for service	Usually does not have access to PII/PHI/PCI	Does not have access to PII/PHI/PCI
Requires access to personal data as defined under GDPR or State/ Province regulators for service	Usually does not have access to personal data as defined under GDPR or State/Province regulators	Does not have access to personal data as defined under GDPR or State/Province regulators
Represents critical risk to firm's services should they fail	Represents moderate risk to firm's services should they fail	Represents low to no risk to firm's services should they fail
Data may be stored on servers outside the United States pr Canada	Data is only stored on servers inside the United States or Canada	Location of data not relevant
Privacy breach would trigger reporting obligations to clients, regulators, the public or insurance carriers	Privacy breach may trigger reporting obligations to clients, regulators, the public or insurance carriers	Privacy breach does not trigger reporting obligations to clients, the public or insurance carriers
Breach would activate your organization's Incident Response Plan, Business Continuity Plan, or Disaster Recovery Plan	Breach may activate your organization's Incident Response Plan, Business Continuity Plan, or Disaster Recovery Plan	Breach does not activate your organization's Incident Response Plan, Business Continuity Plan, or Disaster Recovery Plan
Examples: Provider of critical software applications (e.g., DMS, email)	**Examples: Software development providers**	**Examples: Office supply or computer hardware provider of shrink-wrapped products**

Firms must develop a process to collect key information within a centralized repository (i.e., GRC solution) for all prospective suppliers. Internal business sponsors should be tasked with providing such information. Supplier profiles should capture the below at a minimum:

- Data sensitivity (e.g., Restricted, Confidential, Public)
- Data types (e.g., firm, client, PHI, PII)
- Impact of a breach (e.g., limited, severe, no impact)
- Who hosts the data?
- Type of access (e.g., periodic vs limited, standard vs privileged)
- Unescorted physical access to a firm facility?

These questions should carry weighted response options and be used to auto-classify suppliers into tiers based on risk. As supplier relationships are dynamic, profile details should be reviewed annually to ensure they remain accurate. High risk suppliers should be subjected to a thorough risk assessment prior to onboarding and annually thereafter, while low risk suppliers may complete limited assessments on a less frequent basis.

Once a law firm has approved their profiling process, they should work to generate awareness and populate their repository with all current suppliers not captured in the firm's centralized repository. The below methods can assist firms in capturing this information:

Meet with key stakeholders from all Staff departments and Practice Groups

Leverage finance data (i.e., 'follow the money')

- Review report of all suppliers paid during prior fiscal year
  - Which suppliers have a large spend?
  - Which suppliers have time charged back to many unique clients?
  - Which invoice descriptions contain keywords (e.g., 'relativity', 'host', 'storage')
- Establish real-time alerting to highlight new suppliers in AP system not vetted by Legal, Security, and the General Counsel

Law firms should develop supplier assessment questionnaires custom to their specific needs. This can appear daunting at first, however, there are many industry resources that can be utilized (examples below):

- NIST SP 800-53 (Security and Privacy Controls for Information Systems and Organizations)
- ISO/IEC 27001:2013 (Information Security Management)
- Center for Internet Security (CIS) Top 20 Critical Security Controls
- HITRUST Common Security Framework (CSF)
- Standardized Information Gathering (SIG) Lite and Core

A firm's assessment process should be commensurate with the level of risk associated with a supplier, as described above. For example, a supplier with periodic remote access to your network through a secure remote access solution might complete a 'lite' assessment every two years while a supplier that hosts confidential data might complete a 'full' assessment annually. Additionally, a supplier with unescorted physical access may only be required to answer a single question pertaining to their background check process.

Assessment questionnaires should be dynamic to ensure suppliers are only answering questions applicable to their service offering. For example, questions related to Software Development Life Cycle (SDLC), Data Center Physical/Environmental Security, Personally Identifiable Information (PII), and Protected Health Information (PHI) should leverage conditional logic. Supporting evidence should be required to confirm the accuracy of key responses (i.e., 'trust but verify'). The below evidence should be collected at a minimum:

- Information Security Policy Documentation
- Independent Audit Report (e.g., ISO 27001, SOC 2 Type 2)
- Independent External/Internal Penetration Test Report

Law firms should review their questionnaires annually to ensure they remain relevant and holistic to the current threat landscape.

Completed supplier questionnaires should be dynamically scored and evaluated against your firm's risk tolerance level. A formal risk acceptance process should be utilized when business sponsors pursue onboarding a supplier not aligned with your firm's baseline security requirements. High-level reports should be developed to summarize risks and facilitate an informed business decision. Authorized suppliers should have their findings prioritized and formally tracked through remediation. Standardized metrics should be presented to senior management on a set cadence to demonstrate compliance with policy, risk reduction statistics, and any relevant risks requiring discussion.

The success or failure of any policy driven program, such as a third-party risk management policy, starts and ends with a well-defined and executed awareness program. This particular risk awareness is mostly benign and thought to be less relevant to employees' day-to-day interaction with firm/client related data and service providers. A well thought out awareness program encompasses a very clear and concise definition of a third-party vendor. The inclusion of all entities considered to be third-party can often escape the most diligent of subject matter experts, both lawyers and professionals in the various business departments. A holistic approach that's all inclusive, with varying instruments to deploy this messaging is key. Some examples in the way of deployment along with a consistent cadence may include.

- Yearly awareness training. This timely effort should be inclusive of annual updates to any third-party manifesto that is in place. Interactive video training with some form of recap and quiz are very effective. This delivery method has proven to be reliable for retaining subject knowledge and a great source to reference as a reminder. Most LMS (Learning Management System) can assist in tracking user participation which further enables policy requirements.
- Continuous Education. As new hires are on-boarded, it is important to include third party awareness along with other security awareness programs into the new hire curriculum. In addition, varying messages specific to Third Party policy should be considered as part of any number of firms related campaigns, such as New Business Intake training, RFP responses along with other business development opportunities.
- Metric Data. Successful awareness training for both staffers and lawyers **presents an opportunity to put forth a key data point which is marketable to clients and/or other panel opportunities being considered**. Turning a successful awareness program into an asset not only assists with protecting your firm but makes the argument for a potential competitive advantage.

APPENDIX II

CASE STUDY 2: AN ESTABLISHED SUPPLY CHAIN MANAGEMENT PROGRAM

This case study takes a look at a mature third-party supplier onboarding program at a law firm which begins with a centralized group of individuals tasked with taking contracts and agreements from start to finish. Within this organization, there are 5 people across 3 distinct teams who comprise the group responsible for supplier onboarding:

- 1 in house contract attorney
- 1 in house privacy attorney
- 1 Operation Manager
- 2 IG Security and Compliance Specialists

The in-house attorneys, who report to the General Counsel, are primarily responsible to review and negotiate contracts and privacy agreements respectively. Next, the Operations Manager is responsible to oversee the lifecycle of the contract review. He or she accounts for the documentation essential to the process and remains abreast of the status of contract review throughout. Finally, two Information Governance Security and Compliance Specialists perform security assessments, initiate Data Processing Agreements and evaluate whether the vendor's security posture is in line with the firm's risk threshold.

The purpose of the combined Vendor Onboarding Team is to advocate on internal customer's behalf to properly and efficiently get contracts completed for all services across the firm. The team ensures the firm is armed with appropriate protections within agreements, that vendors have proper security controls to protect the firm, document the vendor compliance with regulatory requirements like GDPR and ensure software is compatible with the firm's computing environment.

THE WORKFLOW

Start	Create a request for a new contract › Create new task in workflow tool › Upload documents › Complete Questionnaire
Middle	Begin Contract, Security & Privacy Review › Mutual Non-disclosure Agreement › Contract Negotiation › Security Assessment › Data Processing Agreement
End	Final State › Security Assessment Results › Executed Agreements

The workflow begins with the internal customer submitting a new request for contract review via the firm's workflow tool in which information about the vendor and product is collected, including a description of the product and/or services, contact information for the vendor, details about how the firm uses the product, and business terms. Additionally, the customer is asked to attach documentation such as an executed Mutual Non-Disclosure Agreement (MNDA) if one was already initiated along with the contract to be negotiated. The form collects limited information describing the architecture of the product (on-premise, cloud, combination) and how the vendor has access to the firm's network. Some contracts for new systems get flagged for review by an architectural review board (ARB). The ARB ensures technical aspects required by the vendor can be satisfied and align with the firm's overall computing ecosystem. A final section of the form acts as a mini-Data Protection Impact Assessment (DPIA). It confirms the nature of the data and data subjects the vendor processes, whether it includes personal information from individuals in the EU/UK or other jurisdictions, and determines the purpose for which the data is being collected.

Next, several processes kick off in tandem. If an MNDA wasn't previously executed, it is kicked off here. The firm's contract attorney begins their review of the Master Services Agreement (MSA) and if any redlines, sends back to the vendor. IG checks the DPIA to determine the necessity of a Data Processing Agreement (DPA). The IG team evaluates which flavor of DPA is required (controller to controller, controller to processor) and sends this out along with launching a security assessment. If the vendor provides its own DPA, privacy counsel reviews and redlines the agreement or waits for the vendor's redlines on the firm's DPA. These reviews, negotiations and assessments are inevitably the longest part of the process. Often the Operations Manager is coordinating meetings between in house counsel and vendor counsel. Meanwhile, IG evaluates the security assessment which results in a risk score which translates to passing or failing. Responses to the security assessment questions are weighed against the context of the service being offered and data being collected though at times conversation is necessary to clarify responses. At times, these negotiations can take months, and tracking the status of agreements can be challenging.

Finally, with both parties in agreement, documents are sent via DocuSign for execution and ultimately stored in the firm's document management system.

The process for contracts was previously decentralized, each department or office handled its own procurement and negotiation. The firm was far less efficient at evaluating vendor risk and was not involved with evaluating agreement terms. To bring awareness to the Vendor Onboarding Team, department-specific meetings were organized to present and market the team's services. It has taken the firm a few years to get the right people involved in the process and gain traction for the program.

In order to bring further efficiency and transparency to the process, additional tools are being evaluated. For example, the attorneys would like to leverage a contract management tool to help with tracking of redlines passed between firm and vendor as well as to set up ticklers for contract renewal.

APPENDIX III

BINDING TERMS: IN MASTER SERVICE AGREEMENTS, DPAS, ETC.

Clients are increasingly asking their law firms to bind their third parties to the same or similar security terms being imposed by the client on the law firm. However, even if this wasn't the case, security best practices, and prudence, dictate that contractual terms be used to help mitigate additional risks with third parties.

One first step is to get control of the vendor selection and on-boarding process. Find out who in your firm is signing agreements with vendors. You may find that agreements are being signed without considering the terms and conditions outside of the desired service delivery description. Finance is a good place to start looking to see what vendors are being paid, and then you can determine if a contract was properly reviewed. A good next step is a policy stating who has the authority to commit the firm to obligations, and when/how agreements should be reviewed.

Ideally, these concepts extend across the entire supply chain, with third parties enforcing the same or similar terms for their third parties and so on. There are, broadly speaking, two ways to approach this challenge: modification of the vendor's agreement or utilization of a separate, firm drafted privacy and security agreement. The two approaches don't have to be mutually exclusive.

MODIFICATION OF THE VENDOR'S AGREEMENT

Many third parties have some sort of agreement for your firm to execute in order to procure their services. Some of these agreements include terms that address confidentiality, privacy and security. However, few of these agreements adequately protect the interests of the law firm or its clients.

Most law firms have attorneys that specialize in privacy, security or technology contracts. We recommend you utilize your in-house knowledge to develop a clause bank or playbook that addresses the typical concerns. If it is challenging to get resources to review contracts, a firm may look into providing attorneys billing credit for the time spent reviewing contracts on behalf of the firm.

The terms found in vendor-provided agreements will no doubt favor the vendor. Some items to look out for include:

- Confidentiality provisions, or lack thereof
- Limitations of the vendor's liability for damages
- Broad indemnification provisions (who does your insurer cover?)
- Poor (or no) restrictions on who can access to the data
- Are third parties involved in providing the service, and what are their obligations
- If the vendor is providing a service to your client, who pays, and could a client stick you with the bill
- Assignment without consent
- Arbitration provisions
- Recourse provisions
- Choice of law or venue favoring the vendor
- Ownership of the data
- Unacceptable termination provisions
- Liquidated damages provisions or penalty clauses

WHAT TERMS SHOULD YOU ASK FOR? A CHECKLIST:

- Definition of the data elements in scope
- Confidentiality: do not disclose to anyone other than those employees, contractors, and agents with a need to know in order to service the agreement
- Use data only for the purpose of the agreed upon business need
- Indemnification of the firm from any breach by the vendor
- Data is not transferred out of approved geopolitical boundaries
- Existence of written information security program
- Existence of vulnerability management program matching certain parameters
- Right to perform security assessment
- Annual audit and penetration testing
- Summary of results and remediation plan
- Existence of incident response plan
- Reporting responsibilities back to firm
- Right for firm to be involved in investigation
- Breach notification within agreed time (typically 24 or 48 hours)
- Right for firm to control breach notification to its clients
- Appropriate technical, physical, and administrative controls
- Subcontractors are bound by an agreement at least as stringent as this one
- Appropriate resilience in order for the vendor to continue providing services in the event of reasonably foreseeable events
- Destroy or return data upon termination of agreement
- Abide by applicable law, rules and regulations (confirm and review governing law and forum location)
- Compelled disclosure: give the firm notice of blind subpoena unless not allowed by law enforcement
- Restrictions for HIPAA/ITAR/EAR/ China PIPL data

ENDNOTES

[1] https://www.ibm.com/topics/supply-chain-management

[2] https://www.manufacturing.net/supply-chain/blog/21403746/the-new-realities-of-supply-chain-management

[3] https://www.bbc.com/news/business-56559073

[4] https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12

[5] https://www.accellion.com/sites/default/files/trust-center/accellion-fta-attack-mandiant-report-full.pdf

[6] https://securityintelligence.com/articles/data-breach-protection-physical-security/ [securityintelligence.com]

IRON MOUNTAIN®

800.899.IRON | IRONMOUNTAIN.COM

ABOUT IRON MOUNTAIN

Iron Mountain Incorporated (NYSE: IRM) provides information management services that help organizations lower the costs, risks and inefficiencies of managing their physical and digital data. Founded in 1951, Iron Mountain manages billions of information assets, including backup and archival data, electronic records, document imaging, business records, secure shredding, and more, for organizations around the world. Visit the company website at www.ironmountain.com for more information.

USLGL-RPT-102521A