Understanding the Vendor Management Lifecycle

securing personal information at the hands of third parties.
Introduction

As organizations struggle to keep up with service demands, adopt new technologies, and stay ahead of continuously evolving domestic and international regulations, many are choosing to engage third parties to tackle some of their biggest business challenges. Third parties, however, introduce new privacy and security risks for personal information that is accessed, processed, transmitted, or stored by the organizations’ vendors. These risks must be considered when an organization is determining its control environment and the risk management activities associated with privacy and information security.

These risks are growing every day. In a May 2016 Ponemon survey of industry risk management professionals, 70 percent of respondents said third-party risk in their organizations is either significantly increasing, increasing, or staying the same. The risk is driven in large part by a changing threat landscape – including the Internet of Things (IoT) and Cloud migrations – and an increasing reliance on third parties. Complicating the issue, many organizations do not adequately understand where and when third parties have access to their personal information.

To date, many organizations have failed to meet this challenge. Only 29% of the organizations polled by Ponemon have a vendor management program in place. And those that were breached as a result of negligent or malicious third parties paid for their inaction, on the order of roughly $10 million per security incident.

To help identify and mitigate these risks, organizations should implement a vendor risk management program that addresses every step of the vendor management lifecycle, including due diligence procedures, active monitoring, and breach response procedures. The following paper outlines key action steps as you set out to build a vendor risk management program within your organization that is appropriate, manageable, and sustainable.

"Only 29% of the organizations polled by Ponemon have a vendor management program in place."
**Understanding Your Data**

Before identifying your vendor management lifecycle, you must be aware of the What, Who, Which, and Where of your personal information.

1. **What is personal information?**
2. **Who is considered a third party?**
3. **Which privacy regulations apply to the organization?**
4. **Where does PII reside within the organization?**

### What is Personal Information?

Under the Generally Accepted Privacy Principles (GAPP), a set of privacy principles created by the American Institute of CPAs and (AICPA) and the Canadian Institute of Chartered Accountants (CICA), most of the information collected by organizations about individuals is considered “personal information.” This information is:

- about or can be related to an identifiable individual;
- any information that can be linked to an individual or used to directly or indirectly identify an individual; and
- related to prospective, current, and former customers, employees, and others with whom the entity has a relationship.

Some common elements of personal information include:

- Name
- Home address
- Email address
- Consumer Purchase History
- Social Security Number
- Date of Birth

In addition to standard personal information, organizations may also collect a subset of sensitive information that faces stricter laws and regulations and requires an added level of privacy and security protection. This information is deemed “sensitive personal information” and includes:

- Medical information;
- Financial information;
- Racial or ethnic origins; and
- Information related to offenses or criminal convictions.

Other sensitive company information, including enterprise intellectual property (trade secrets, formulas, etc.), payroll data, non-public earnings information, private emails, and payment card data, should also be considered. While this data is often less likely to be processed through third parties, it can cause catastrophic damages for companies if compromised.

With this baseline understanding, you must then identify the types of sensitive information you are collecting, processing, and storing, and then identify which information has the highest risk value to the organization. Information with the highest risk value is commonly categorized as critical, confidential, or sensitive. Understanding the data in your or-
ganization allows you to better manage that data risk once it moves into the hands of third parties.

**Who is Considered a Third Party?**

For purposes of creating a vendor management program, a “third party” is any entity that is not affiliated with the organization and collects, accesses, processes, transmits, or stores personal information, and/or accesses the systems and applications that house this information.

**Which Privacy Regulations Apply?**

Identifying the privacy regulations relevant to your organization is vital in determining the types of personal information that is locally, federally, and internationally regulated, and will also help determine specific third parties requirements that you must consider.

As an example, health organizations engaging third parties to collect, transmit, and store protected health information (PHI) must ensure that privacy and security standards for engaging these third parties meet the Health Insurance Portability and Accountability Act (HIPAA) requirements. Furthermore, U.S. organizations with operations in the EU must consider privacy and security requirements outlined in the newly enacted General Data Protection Regulations (GDPR) if they plan to engage third parties to process personal information related to EU customers or employees.

**Where does Personal Information Reside within the Organization?**

If not already determined, you should identify the locations in which your organization’s personal and sensitive information resides. This is typically accomplished through an information mapping or information inventory assessment. Identifying the internal and third-party systems and applications that house personal information will assist the organization as part of the vendor management lifecycle.

**Building your Vendor Risk Management Program**

Now that you have identified the What, Who, Which, and Where of personal information, you can begin to develop your vendor management program. Once complete, this program will determine the risks associated with engaging third parties. The process for identifying these risks can be understood through a high-level vendor management lifecycle.

**The Vendor Management Lifecycle**

The high-level vendor management lifecycle can be seen to the right.

The organization must determine and formalize roles and responsibilities throughout the course of the vendor management lifecycle to ensure that procedures are formalized, implemented, and communicated to all parties involved.

**Step 1: Identify the Need for Third Party Service**

The vendor management lifecycle begins with identifying a need for a third-party service. Typically, the service is one that cannot be fulfilled by in-house employees or is more cost effective to outsource. Organizations should identify who has the authority to determine a service need and act as the primary point of contact for inquiries related to third-parties.
**Step 2: Perform Third-Party Security Review**

Once a potential vendor has been identified, the organization should determine whether the third party will collect, access, process, transmit, or store the organization’s personal information, and whether the third party will require access to the organization’s systems and applications that house the information.

Once this has been determined, the organization should perform a third-party security review to identify any potential privacy and security risks associated with engaging the third party. In the initial stages of the security review, the organization must ensure certain key procedures are in place:

**Establish a Third-Party Risk Profile**

The organization should determine a risk profile for each vendor it considers. The risk profile should include:

- what does the vendor supply;
- what kind and how much of your data does the vendor store;
- what would be the business impact of the loss or compromise of this data;
- where is the data stored physically; and
- which internal systems and applications would the third party require access to.

The organization should leverage the expertise of its information security team to help determine the full risk criteria. Standard risk profiles include low, moderate, and high. As an example, a third party maybe be classified as high-risk if it requires access to sensitive customer information such as social security numbers and payment card information, or considered low-risk if the third party requires access to small amounts of personal information of the lowest sensitivity, such as a customer’s first name.

**Determine Third Party Security Requirements**

Once you have developed a risk profile, your organization should determine the levels of security controls and activities the third party must have in place to ensure that personal information is adequately protected. This control population should be the basis for the third-party security review. Many organizations choose to develop their own security review control framework leveraging best practices from various standards and frameworks including:

- ISO27001/2
- COBIT 5.0
- ITIL V3
- NIST Special Publication 800-53
The security review controls frameworks should consider areas related to a third party’s:

- Organization Security
- Physical and Environmental Security
- Access Controls
- Incident Management Procedures
- Overall Compliance Environment
- Business Continuity Management

Using the risk profiles, you can determine the level of scrutiny to which each vendor should be subjected. For low-risk vendors, a self-assessment or questionnaire may suffice. Higher-risk vendors may require an in-depth on-site review. By ranking third parties according to their inherent risk level, you are able to make efficient decisions related to vendor selection and security.

**Determine High-Risk Observations**

The security review controls framework will help the organization identify gaps in the third party’s control environment that may increase the risk to your personal information. With this assessment in place, you can make an informed decision on whether to require control improvements from the third party, terminate your relationship with the third party if risks cannot be mitigated, or continue to engage the third party and assume the risk. These decisions should be made with input from the department contact engaging the third party, the information security department, internal audit, compliance departments, and/or the legal department. The acceptance of any risks not properly met by the third party should be formally documented and accepted by applicable parties via a risk acceptance form. The form should include information related to:

- A description of the observations identified in the third party security review;
- The justification for the risk acceptance; and
- The compensating controls in place within the organization to help mitigate the risk.

**Step 3: Review Vendor Agreement**

If a decision to engage a third party has been made by the organization, the next step in the vendor management lifecycle involves the review of the vendor management agreement. If provided by the third party, this review should require input from your legal department and information security team, to ensure that organizational privacy and security requirements are reflected in the agreement. The organization should further maintain a master services agreement (MSA) or standard third-party contract template language that contains privacy and security-related contract language by default.

**Step 4: Perform On-going Vendor Management Monitoring Activities**

As part of the risk profile determination and results of the third-party security review assessment, the organization must ensure to establish on-going vendor management monitoring activities. Once an organization has determined the risk associated with the third party, continuous monitoring programs should be established to ensure that risk levels remain constant and that third parties are maintaining their privacy and security standards.

On-going vendor management monitoring activities, however, should not be limited to the third parties. Organizations must also ensure they maintain vendor management procedures and monitor for changes in the way that data is used. This includes ensuring that the organization is properly...
training its employees in the vendor management process, updating and maintaining an approved list of third parties that have undergone the security review process, and ensuring that standard contract language is current and contains up-to-date privacy and security language.

CONCLUSION

With an increasing number of data breaches involving personal information being traced back to third parties, now is the time to implement or strengthen the vendor management program in your organization. By mapping your process to the vendor management lifecycle outlined in this paper, you can begin to build a program that protects your data, customers, and reputation from risks introduced by your vendors.

While your vendor management program should be designed around your needs and your level of reliance on third parties, it should at a minimum provide guidance on:

- Evaluating the need for third parties;
- Assigning risk profiles and conducting security reviews;
- Reviewing vendor agreements; and
- Performing on-going vendor management monitoring activities.

For organizations with complex vendor management programs, or for companies that rely heavily on a large number of vendors, Focal Point frequently provides guidance and expertise on building effective vendor management programs. To discuss your challenges with an expert, please contact Eric Dieterich at edieterich@focal-point.com.

THE AUTHOR

Understanding the Vendor Management Lifecycle was written by:

Melinda Tijerino, CIPP/US
mtijerino@focal-point.com

Melinda is a Senior Manager with Focal Point’s national Data Privacy practice. She currently manages mid to large scale data privacy and security assessments, with experience that spans across local, federal, and international privacy and security standards within public and private sector organizations, including: government agencies (U.S. and Native American tribal government), global technology firms, global retail chains, financial services, and mixed medical facilities that include hospitals, pharmacies, rehabilitation centers, and behavioral/mental health facilities.

ABOUT FOCAL POINT

Focal Point Data Risk is a new type of risk management firm, one that delivers a unified approach to addressing data risk through a unique combination of service offerings. Focal Point has brought together industry-leading expertise in cyber security, identity governance and access management, data privacy and analytics, internal audit, and hands-on training services, giving companies everything they need to plan and develop effective risk and security programs. By integrating these services, we provide our clients with the flexible support they need to protect and leverage data across any part of their organization. Simply put, Focal Point is the next generation of risk management.


Disclaimer: Focal Point Data Risk, LLC is not a law firm and does not provide legal advice. This document is intended for informational purposes only.