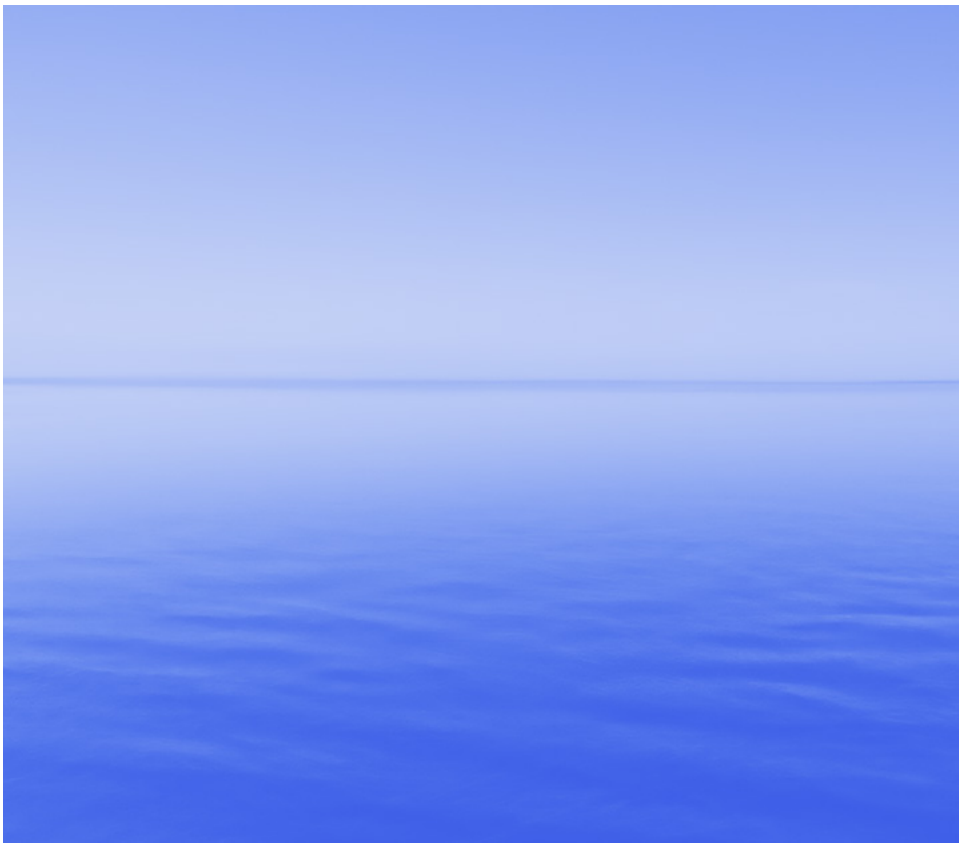
Clearwater

Whitepaper

Vendor Risk Management: Know your riskiest vendors

Table of Contents



Introduction

You just received notice that a vendor that maintains your organization's data was hacked, and the bad actors downloaded files containing thousands of records with personally identifiable information or protected health information. You relied on the vendor to keep your data safe. Now you wonder if you have an effective vendor risk management program.

Following any significant security incident, you must take a hard look at your organization's relationship with the vendor. When onboarding the vendor, did the organization thoroughly vet their privacy and security practices? Was the organization apprised of any changes to the vendor's privacy or security practices? What could have mitigated the effect of the incident? What could your organization have done?

The answer lies in having a risk management process for analyzing and managing risks associated with utilizing the products or services of vendors. Establishing a vendor risk management program that includes governance and technology tools can reduce the risks to your organization at the operational, financial, reputational, cybersecurity and compliance level.

Determine program parameters

To develop an effective vendor risk management program and framework, you need to understand and acknowledge the challenges that many organizations face when implementing a strategy to reduce risk, particularly through resources, complexity and governance.

Resources

Cybersecurity incidents are increasing, and a key contributing factor is the growing complexity of the vendor landscape. Organizations continue to increase their reliance on vendors and tend to share confidential and sensitive information with a larger network of vendors. Yet, many organizations don't keep a comprehensive inventory of these vendors, and lack centralized control. Additionally, a growing number of state laws require more robust reviews of vendor or third-party relationships.

The number of vendors that organizations are relying on is increasing, and at the same time the threats those vendors pose are escalating in frequency and severity. Consequently, managing these risks has become a seemingly overwhelming problem. The result is that more budgeted resources are needed to manage this complex vendor environment. Determine what resources are appropriate through modeling and external benchmarking.

Complexity and governance

Another challenging factor regarding vendor risks is that many organizations do not have a coherent process to identify, monitor and assess the multiple risks posed by vendors. For many organizations, the vendor risk management approach has changed little for many years, despite the increased complexity of their vendor relationships.

Vendor risk management is often fragmented, siloed or operating with minimal visibility or oversight. Siloed business functions, where each line of business is responsible for assessing their own vendors, coupled with ineffective tools and incomplete or unsophisticated assessment models, all compound the problem.

Vendor risk management is often fragmented, siloed or operating with minimal visibility or oversight.

Mature programs have made a concerted effort to centralize vendor risk management and build a governance structure that includes representation from the various stakeholders (e.g., technology, procurement, contracting, privacy, security). A collaborative approach can lead to an approved pool of vendors for the entire organization. The result reduces the siloes between business functions, eliminates duplicative efforts, and sometimes reduces the total number of vendors needed by the organization. Select a model of centralization and complexity that is compatible with your organization's style of management and risk tolerance.

Once your strategies have been decided, the program can be developed in three stages.

1 – Conceptualize your program

The best vendor risk management programs are backed by management. They operate with the full support of the board and senior leadership, which influences the people, processes and technology that can be used to implement and manage the vendor risk management lifecycle.

Before you can quantify your risk, ensure that your vendor risk management vision and framework are scalable, data driven, automated and cost effective for your organization. Manual risk management processes may not be able to keep pace with cyberthreats and vulnerabilities. Reliance on inefficient processes and the inability to automate risk assessments and remediation will create an environment where vendor breaches are commonplace and expensive.

To fully understand where you are in the maturity lifecycle of your vendor risk management program and where you want to be, you need to understand your current state and structure. Relevant graphics can help to visualize the structure, establish a management process, outline the roles and responsibilities, identify stakeholders and ensure that your people, processes and technologies are deployed appropriately and efficiently.

> *Centralize vendor risk management with a governance structure that represents various stakeholders.*

2 – Operationalize the program

Once the framework and structure are determined, your program can be established or modified.

Establish policies and procedures

Establish formal policies and procedures to help your employees understand the process and their responsibilities. The policies should explain at a high level how vendor risk will be managed. You do not have to begin from nothing. You can leverage existing policies and procedures and enhance them.

Procedure documents should detail roles and responsibilities, including those of senior management and business line management. The procedures should be comprehensive—not just about establishing new associations and contracts. The procedures should address the entire relationship lifecycle as summarized in Exhibit 1.

When you begin to formalize your program, focus on the biggest risk areas, get started with the fundamentals, and continuously mature and right-size the program for your organization and its risk appetite.

Identify and inventory vendors

A lot of vendor relationships sit outside the standard contracting process, and even if you have an established program, you still may not be aware of every vendor. Be

Exhibit 1 – Necessary procedures

1. Initial vendor selection and vetting
2. Security questionnaires and associated documents for vendor submission
3. Internal coordination with business or system owners
4. Risk rating/scoring
5. Vendor agreements, including HIPAA requirements
6. Vendor onboarding, including training and care in issuing security credentials and limiting physical and system access
7. Controls for accessing data
8. Ongoing monitoring and review
9. Vendor offboarding, including cancelling security and access credentials and retrieving or destroying data

sure to capture data from multiple systems and sources to ensure a complete and accurate inventory.

The inventory is the first step in classifying vendors from highest risk to lowest risk based on the systems, networks and data they access. For example, some of your riskier vendors may be infrastructure-as-a-service or platform-as-a-service providers who store patient data, proprietary information and business-critical software such as operating systems and databases.

Additionally, a point-of-sale system vendor may have access to customer cardholder data, and a payroll vendor will be able to access nonpublic employee personally identifiable information (PII). Each of these vendors with access to sensitive or regulated data should be identified in the early stages of procurement as a high risk.

Once a comprehensive inventory of all the vendors with possession of or access to your information is established, tracking who has access to sensitive data and how many of these parties are sharing this data with others will be more manageable.

If you have limited resources, the identification process can help if you need to conduct a staggered approach for assessing vendors, with a focus on business operations and vendors with access to more critical data.

Assess and prioritize

Regardless of the industry, a risk-based approach to managing vendors is preferred. Vendors that handle critical business processes will be a bigger threat than smaller contractors who may work with a single department.

Security assessments can be conducted in several ways, but consider what is right for your organization. If your organization is small or a start-up with a limited number of vendors maintaining data, you may find that manually disseminating security questionnaires and assessing vendors is the only feasible approach.

However, if your organization is large with a significant number of vendors, you may need a more sophisticated vendor management program. The functionality could include a software system that has automated features, maintains all assessments and documentation, and generates reports and dashboards.

A number of technology solutions are available that can assist in streamlining and automating the assessment and prioritization process, including using industry standard frameworks (NIST Cybersecurity Framework, NIST 800-53) as the baseline for the assessments. The information gathered through this technology can help quantify the risk for prioritizing your vendors.

Regardless of the size of the organization and vendor inventory, the security assessment should be comprehensive and address all areas that are applicable to your organization. Not all vendors will voluntarily provide evidence of their compliance, but you can request available Service Organization Controls reports, policies and procedures, attestations, and data flow diagrams. In some cases, vendors make documents and resources related to their security protocols available on their website.

Respond to risks

Risk response is about making informed decisions on how to treat risk. Any response should align with your organization's risk appetite and any residual risk. Once you understand the risks associated with each of your vendors, you can decide how to respond to them, by accepting, avoiding, mitigating or transferring the risk.

Your organization can accept a low risk or a risk that can be managed. Acceptance often occurs with vendors that provide a highly valued or niche service or product. For example, you may have challenges obtaining specific documentation or assurances from a cloud provider. However, because of the reputation and the value of that organization, the risk may be acceptable.

Risk can be avoided at the very start of vendor vetting by determining that the risk is too great to contract for a particular vendor's products or services. Risk can be transferred through insurance or indemnification, but neither might be a complete solution for the transfer of risk. For example, cybersecurity insurance may have limitations on what is covered.

Mitigating risk requires planning and action on the part of the vendor that may require reevaluation and assessment by your organization. Mitigating is also dependent on the organization's appetite to control or direct a vendor to mitigate risk.

While many organizations collect information regarding their vendors, they often do nothing with the information. Inaction is a risk to your organization.

> *The program's vision and framework should be scalable, data driven, automated and cost effective for your organization.*

3 – Establish protocols

Ongoing monitoring and periodic assessments

Risks with your vendors change. Risks are not static, and their management is not a one-and-done proposition. You need to regularly evaluate and monitor them.

You can conduct audits, evaluate security and privacy practices or obtain a letter of attestation from the vendor that nothing has changed in their practices or environment that would now require a security assessment.

Assessing vendors annually is important in verifying that they continue to meet and maintain the necessary security standards. Surprisingly, this is an area that many organizations fail to follow through on.

Offboarding

Termination of the relationship with a vendor is an especially important step to manage. Do not let a vendor leave with access to your data.

Plan an exit strategy for the end of the contract. Ensure that both parties understand

what their respective responsibilities are for offboarding and verifying that your data are returned or destroyed.

Inaction on collected vendor information is a risk to your organization.

Summary

Establishing a vendor risk management program can seem overwhelming. Breaking the program down into stages makes the program easier to implement.

The first stage is to understand your business operations, identify and leverage already available internal resources, and establish a structure and framework. The second stage requires putting policies and procedures in place, developing vendor inventories, conducting vendor assessments and determining priorities based on risk and risk response. The third stage focuses on establishing protocols for ongoing monitoring, periodic reassessments and offboarding.

Throughout the stages, frequently review your vendor management program and processes, implement technology solutions where feasible, and address new organizational practices and technological changes to ensure that your program stays aligned with business operations and compliance requirements.

Dawn Morgenstern, MBA, CHPC, CCSFP, is the Chief Privacy Officer and a Senior Principal Consultant at Clearwater Compliance, LLC. She assists and provides consultation to covered entities and business associates for HIPAA privacy, security and breach notification programs. Dawn can be reached at 615-610-4347 and Dawn.Morgenstern@clearwatercompliance.com.

Clearwater is the leading provider of Enterprise Cyber Risk Management and HIPAA compliance software and consulting services for the healthcare industry. Our solutions enable organizations to gain enterprise-wide visibility into cybersecurity risks and more effectively prioritize and manage them, ensuring compliance with industry regulations. Clearwater's suite of IRM|Pro® software products and consulting services help healthcare organizations to avoid preventable breaches, protect patients and their data, and meet OCR's expectations, while optimizing cybersecurity investments. More than 400 healthcare organizations, including 64 of the nation's largest health systems and a large universe of business associates that serve the industry, trust Clearwater to meet their information security needs.

Have questions regarding this white paper? Engage with Clearwater for a specific discussion about your organization's approach.

- ClearwaterSecurity.com/Contact