PROCESS UNITY

IDENTIFYING VENDOR RISK

THE CRITICAL FIRST STEP IN CREATING AN EFFECTIVE VENDOR RISK MANAGEMENT PROGRAM

HEADQUARTERS
33 Bradford Street
Concord, MA 01742
PHONE: 978-451-7655

© 2014 ProcessUnity, Inc. All Rights Reserved | www.processunity.com

THE CRITICAL FIRST STEP IN CREATING AN EFFECTIVE VENDOR RISK MANAGEMENT PROGRAM

In May 2012, Jonathan Woodson, director of TRICARE Management Activity, received a letter from the Congress of the United States. The letter strongly criticized TRICARE for its inability to safeguard the protected health information (PHI) of U.S. members and their families.[1] The reprimand stemmed from a 2011 data breach in which an unsecured data tape, containing the PHI of 4.9 million patients, was stolen from the car of an employee of TRICARE vendor Science Applications International Corporation (SAIC).

The admonishment from Congress was serious, but TRICARE also faced class--action lawsuits seeking nearly $5 billion in damages in addition to credit monitoring for the affected individuals. Although the tape was in SAIC's possession at the time of the theft, TRICARE was fully accountable for the ramifications of the breach.

The congressional letter stated that TRICARE "does not mandate that its contractors' handling sensitive information implement a commonsense risk management practice." By failing to recognize and prevent the practice that caused the theft, TRICARE had failed to implement an effective risk management program of its own. As a direct result of its vendor's actions, TRICARE suffered a serious blow to its reputation and financial position.

Can you picture your company in this type of situation—one in which an action committed by a third-party service provider causes your company to take the fall? It happens all the time. In fact, the Ponemon Institute reports that 65 percent of companies that outsourced work to a vendor have had a breach involving consumer data; 64 percent said it has happened more than once.[2]

1. Letter from United States Congress to TRICARE Management Authority, May 7, 2012
2. Ponemon Institute LLC, "Securing Outsourced Consumer Data," February 2013

© 2014 ProcessUnity, Inc. All Rights Reserved | www.processunity.com

Data breaches are just one scenario in which vendors can pose a risk to your business. There's an endless string of "what-if" questions:

- What if a supplier to your manufacturing process uses the mineral tungsten in its components?
- What if your overseas manufacturer subcontracts work to companies that use child labor?
- What if a consultant you hire to negotiate building leases in another country uses bribes to obtain the necessary permits?
- What if you discover that, when you set up encryption with your cloud service provider, you also handed them your private keys for your digital certificates?

It's your responsibility to know not only the answers to the questions but also the questions to ask in the first place.

An effective vendor relationship management (VRM) program starts with knowing what the risks are. You can't manage what you don't know; therefore, you need to create assessments that help you clearly identify the risks of doing business with third parties. This includes vendors, service providers, suppliers, contractors, and other people and companies with whom you have a business relationship.

There are numerous methods to assess vendor risk. The questions of who to evaluate, what to evaluate, and how to evaluate vary widely from company to company and vendor to vendor. But the question of why to evaluate is universal. Read on for our guidance on various techniques you can use to identify third-party risk that could adversely impact your organization. We've included helpful tips from our expert risk management advisors.

WHY CONSIDER VENDOR RISK?

"No company is an island unto itself," says Michael Rasmussen, chief GRC pundit at GRC 20/20. "Organizations are a complex and diverse system of business relationships. Risk and compliance challenges do not stop at traditional organizational boundaries. When questions of third-party business practices, compliance, and controls arise, the organization is held accountable, and it must ensure that business partners behave appropriately."

Many companies simply have to manage vendor risk—that is, it's mandated by numerous regulatory requirements in the Health Information Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank), and many other laws. And such regulations aren't just for large public corporations; they may also apply to public institutions, government agencies, and small businesses.

There are other reasons for assessing vendor risk. As TRICARE learned the hard way, it's critical to protect your company brand and reputation. Research from the Ponemon Institute reveals it can take a year to restore an organization's reputation after an incident such as a data breach.[3]

There are a host of issues that can put your company at financial, reputational, or legal risk, depending on your industry. They include:

- Information security for companies handling sensitive information
- Social responsibility and labor standards, especially in third-world countries
- Bribery and corruption
- Conflict minerals in the manufacturing supply chain
- Financial stability of critical suppliers
- Geopolitical risks that threaten to disrupt business

INFORMATION SECURITY DESERVES DEEP SCRUTINY

Nowadays there are stiff penalties and costs for data breaches. The loss of a mere 1,000 records—whether or not they are used to commit fraud—can result in penalties and expenses totaling millions of dollars. Because of technology's inherent complexities, your service providers require comprehensive scrutiny. It's prudent to ask for proof of policy from the start.

The controls to look for vary depending on the nature of the data being handled and the nature of the service being provided during that data handling. For example, with market data feeds, you need to worry about data integrity. The data may not be confidential, but it has to be accurate. In healthcare, your patients' confidentiality is of concern. Data integrity and data confidentiality require different controls, so you need to gauge what's important for your situation.

[3] Ponemon Institute, "Reputation Impact of a Data Breach: U.S. Study of Executives & Managers," November 2011.

© 2014 ProcessUnity, Inc. All Rights Reserved | www.processunity.com

NEW LEGISLATION ON CONFLICT MINERALS HAS BROAD IMPLICATIONS

The Dodd-Frank Act is an expansive piece of legislation that imposes many regulations on companies. Section 150, which focuses on conflict minerals—those mined in conditions of armed conflict and human rights abuse—requires compliance from public companies listed with the U.S. Securities and Exchange Commission (SEC). These issuers must examine their supply chain to determine if they manufacture or contract to manufacture products that contain conflict minerals defined as cassiterite, columbite--tantalite (coltan), gold, and wolframite, as well as their derivatives tin, tantalum, and tungsten.

If this legislation applies to your company, you will need to rely on your suppliers and possibly their suppliers to gather accurate information about the origin of materials you use in your products. Ultimately, however, your company is responsible for obtaining, verifying, and then providing that information, so you need to collaborate with your suppliers out of necessity.

In other words, without an effective VRM program, you cannot ensure quality of service from your vendors and to your customers and prevent disruptions in your business processes.

THE TWO MEASURES OF RISK: INHERENT RISK AND RESIDUAL RISK

There are two ways to look at vendor risk:

1. Inherent risk is based on criteria such as what a vendor is doing for your company; how critical they are to your business; where they are located; what data they are handling; and what naturally occurring threats they face. For example, a company that processes your credit card payments has a higher inherent risk than a vendor who provides office supplies. A vendor's low inherent risk rating can save you the time and expense of doing further assessment.

2. Residual risk is the difference between the inherent risk and what the vendor's controls alleviate. So, for example, if you're worried about cyber security risks, you would want to evaluate the vendor's firewalls, host hardening, antivirus, and other security measures. At the end of that assessment you can decide whether or not they have sufficiently mitigated that risk; the answers you get reveal the vendor's residual risk.

Your comfort with the level of residual risk determines what you do next: continue the business relationship by working with the vendor to further reduce that risk, or sever the relationship and find an alternate supplier.

© 2014 ProcessUnity, Inc. All Rights Reserved | www.processunity.com

CONDUCTING EFFECTIVE ASSESSMENTS

Conducting effective assessments will help you determine the risks of doing business with third parties. There are a number of steps involved:

1. Catalog vendors. This may seem like a given, but you'd be surprised how many companies have a disorganized approach when it comes to hiring third parties. You need to assess your vendors and suppliers and keep ongoing records. Some companies don't have a coherent purchasing strategy, and in cases like this, risk assessment is typically not even considered. Well-managed companies, on the other hand, have a comprehensive catalog of all their suppliers with information about what services they provide and which departments they serve.

2. Profile vendors internally to gauge inherent risk. Develop a profile by questioning the business unit that engages the vendor. For example, in the case of information security, you'll want to know where this vendor is located, how mission-critical this vendor's products or services are, how much confidential information they will be handling, and whether or not they will access your computer network. The vendor profile determines what mitigating controls you will look for as you assess the vendor.

Expert's Tip: Categorize your vendors into "buckets" to facilitate further assessment. For example, a hospital would have an insurance company bucket, a lab services bucket, a medical equipment supplier bucket, and so on. The vendors in any given bucket can be assessed in a similar fashion because they should have many common risk factors. In this example, the insurance companies would all have access to PHI, requiring their compliance with HIPAA. The providers of medical equipment may need to be queried about conflict minerals in their machines.

3. Use a questionnaire for self-assessment. Giving a vendor a questionnaire for self-assessment is standard practice, particularly for those with a high or medium inherent risk rating. The type and depth of the questions should be guided by the vendor's "bucket" and their level of inherent risk. Use the questionnaire to probe a vendor's policies, procedures, and processes to help you determine the company's residual risk.

Ask for evidence or documentation proving the company's standards in areas of concern to your business. Examples of evidence include screen-shots that verify computer controls; proof of professional certifications or licenses; SSAE 16, SOC 2, and SOC 3 reports for data centers; policies and procedures; financial reports; and external audit reports.

Expert's Tip: Don't overwhelm vendors with too many items on the questionnaire. If the survey is too long and asks esoteric or free-form questions, you are likely to get inaccurate, incomplete, and flippant responses. Use simple, standard, objective questions, or tailor your questions to probe areas of real concern.

4. Conduct an on-site audit. Depending on the responses you get on the questionnaire, you may need to dig deeper to understand more about a vendor's practices and ways of work. In some cases, you will need to do an on-site audit, which will provide a more in-depth evaluation, especially of mission-critical partners. Moreover, external regulations require yearly on-site assessments for specific types of vendors.

Expert's Tip: You can learn a lot about an organization by visiting and watching the people go about their day. Interview not just a company's outward-facing employees. Also spend 20 minutes or so with people in departments such as human resources, operations, and finance to flesh out potential risk issues. This gives you a deeper sense of what the organization is about. You get a feel for the tone at the top and other factors that can influence how much faith you place in that vendor.

5. Assign or hire a risk analyst to assess the information and produce a findings report that you review with the vendor. Finally, have a risk analyst—or a team consisting of staff from the legal, procurement and business units—assess the information you've gathered and compare it to your company's standards. The analyst should produce a findings report containing any further issues to be discussed with the vendor, such as residual risk. You want to give the vendor an opportunity to obviate the

© 2014 ProcessUnity, Inc. All Rights Reserved | www.processunity.com

risks you've identified as worrisome.

Expert's Tip: No organization is without risk, but you should always try to minimize any existing risk. When you approach the vendor with your findings, take note of whether the vendor is responsive to your concerns. If the vendor doesn't seem to want to work to keep your business, you need to determine whether you wish to continue the relationship. You have all the leverage in this discussion.

It's certainly a best practice to automate as much of your vendor assessment process as possible. By using an assessment tool on an ongoing basis, your company will be consistent in its evaluations, automate many of your routine tasks, and infuse global standards and frameworks into your assessments. What's more, you can store your documents in a central repository and track and trend assessments over time.

CONCLUSION

You must recognize that when a vendor performs a service or function on your behalf, your company bears the ultimate responsibility for minimizing business exposure and for ensuring compliance with regulatory mandates. It's imperative to conduct a risk assessment of each provider to know what level of exposure you have. With effective VRM, your company can minimize the risk of less direct oversight and control and maximize the benefits gained through a well-managed vendor relationship.

Vendors provide value in the expertise and services they offer; however, it is imperative that companies maintain active oversight. As a manager of business risk, you must recognize that when a vendor performs a service or function on your behalf, your company bears the ultimate responsibility for minimizing business exposure and ensuring compliance.

PROCESSUNITY & VENDOR RISK MANAGEMENT

ProcessUnity is a leading provider of cloud-based applications for risk management and service delivery management. The company's software-as-a-service (SaaS) platform gives organizations the control to assess, measure, and mitigate risk and to ensure the optimal performance of key business processes.

ProcessUnity's cloud-based Vendor Risk Management solution helps companies effectively identify and mitigate risks posed by third-party service providers in critical risk areas such as information security, service delivery, supply chain processing, financial processing, reputation, and regulatory compliance. ProcessUnity provides organizations with clear visibility into the business impact of third-party risk via direct links from vendors and their services to specific business elements such as processes and lines of business. Powerful assessment tools enable evaluation of vendor performance based on customer-defined criteria through automated, questionnaire-based self-assessments as well as through detailed audits of vendor controls. Flexible reports and dashboards enable ongoing monitoring of vendor ratings, assessment progress, and status of remediation activity. Learn more at www.processunity.com.

© 2014 ProcessUnity, Inc. All Rights Reserved | www.processunity.com

ABOUT PROCESS UNITY

ProcessUnity is a leading provider of cloud-based applications for risk management and service delivery management. The company's software as a service (SaaS) platform gives organizations the control to assess, measure, and mitigate risk and to ensure the optimal performance of key business processes. For public companies and regulated industries, ProcessUnity Risk Suite delivers effective governance and control, vendor risk mitigation, and regulatory compliance. For benefit plan administrators and other financial service firms, ProcessUnity Service Delivery Risk Management (SDRM) controls complex product offerings and strengthens client service experience. ProcessUnity is used by the world's leading financial service firms and commercial enterprises. The company is headquartered outside Boston, Massachusetts and is funded by Rose Park Advisors and other private investors.

HEADQUARTERS
33 Bradford Street
Concord, MA 01742
PHONE: 978-451-7655

© 2014 ProcessUnity, Inc. All Rights Reserved | www.processunity.com