Performing Vendor Risk Assessments

You can outsource the work, but you can’t outsource the risk!

Presented by
Jennifer F Alfafara
Consultant, Resources Global Professionals
Introduction

- There is significant Inherent Risk when engaging new Vendor relationships.
- Vendors may have access to restricted and confidential information belonging to or managed by your company.
- Such access may lead to undesired exposure.
Examples of Such Exposure

- Target (December 2013) – 40 million credit and debit cards
- Neiman Marcus (January 2014) – 1.1 million credit and debit cards
- JPMorgan Chase (October 2014) - customer information including names, addresses, phone numbers and email addresses were stolen in the cyberattack
- Anthem Blue Cross (February 2015) – 80 million customers and employees – names, birthdays, medical IDs, Social Security numbers, street addresses, e-mail addresses and employment information including income data
Risks We Should Remember

- Reputational Risk
- Information Security Risk
- Regulatory Risk
- Legal Risk
- Financial Risk
Vendors Likely to be Considered Out of Scope

- A vendor who sells an application to a customer and cannot access the application or associated data
- A vendor who just sells hardware.
Vendor Assessment Red Flags

- PHI – Personal Health Information (HIPAA)
- PII – Personally Identifiable Information
- PCI – Payment Card Industry
- Offshoring
- The Cloud
**PHI – Personal Health Information (HIPAA)**

<table>
<thead>
<tr>
<th>HIPAA Violation</th>
<th>Minimum Penalty</th>
<th>Maximum Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individual did not know (and by exercising reasonable diligence would not have known) that he/she violated HIPAA</td>
<td>$100 per violation, with an annual maximum of $25,000 for repeat violations (Note: maximum that can be imposed by State Attorneys General regardless of the type of violation)</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
<tr>
<td>HIPAA violation due to reasonable cause and not due to willful neglect</td>
<td>$1,000 per violation, with an annual maximum of $100,000 for repeat violations</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
</tbody>
</table>
## PHI – Personal Health Information (HIPAA) cont’

<table>
<thead>
<tr>
<th>HIPAA Violation</th>
<th>Minimum Penalty</th>
<th>Maximum Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIPAA violation due to willful neglect but violation is corrected within the required time period</td>
<td>$10,000 per violation, with an annual maximum of $250,000 for repeat violations</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
<tr>
<td>HIPAA violation is due to willful neglect and is not corrected</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
</tbody>
</table>
PII – Personally Identifiable Information

The following information is collected, used, disseminated or maintained by the Civil Money Penalty (CMP)-2001:

- Name
- Phone Numbers
- EIN (or Social Security Number but only when an EIN does not exist)
- Business address
- Mailing Address
- Business Phone
- Business e-mail address
- Residential address
PCI – Payment Card Industry

Control Objectives

- Manage enterprise entitlements by enforcing consistent, enterprise-wide access control over stored cardholder data.
- Protect cardholder data with automatic encryption before they are transmitted across open, public networks.
- Prevent cardholder information from being sent by e-mail, IM or other communications channels to unauthorized recipients.
- Establish information barriers across communication and collaboration channels to restrict access based on business need-to-know.
Offshoring is the relocation, by a company, of a business process from one country to another—typically an operational process, such as manufacturing, or supporting processes, such as accounting. Even state governments employ offshoring. More recently, offshoring has been associated primarily with the outsourcing of technical and administrative services supporting domestic and global operations from outside the home country ("offshore outsourcing").
Offshoring Risks

- Greatest threat has been data theft
- Natural disaster
- Geopolitical Unrest
- Infrastructure Breakdown
- Lack of formal documented Policies and Procedures
The Cloud

- Rackspace Managed Cloud
- Microsoft Azure Cloud
- Amazon Web Services (AWS)
- Facebook
- Twitter
- Google Inc.
- Software as a Service
# Cloud Advantages/Disadvantages

<table>
<thead>
<tr>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost Effectiveness</td>
<td>Technical Issues leading to Outages</td>
</tr>
<tr>
<td>Almost Unlimited Storage</td>
<td>Security Issues</td>
</tr>
<tr>
<td>Backup and Recovery</td>
<td>Prone to Attack</td>
</tr>
<tr>
<td>Easy Access to Information</td>
<td>Easy Access to Information</td>
</tr>
<tr>
<td>Quick Deployment</td>
<td></td>
</tr>
</tbody>
</table>
Keeping information Safe on the Cloud

- Strong password controls
  - Length
  - Complexity
  - Expiration
  - Limits on re-use
  - Etc.

- Backup your data (off the Cloud)
Performance of a Vendor Risk Assessment

Is this Vendor ‘worthy’ to provide services to us?
Technical Risk Office (TRO)

Different types of Assessments:

- Cyber Security Assessment
- Application Assessment
- Vendor Risk Management
- Compliance Assessment
- Vendor Risk Assessment
Vendor Risk Assessment Process

- Request for Assessment
- Service Risk Assessment Questionnaire
- Determination of Inherent Risk
- Report on Inherent Risk
- Applicability Analysis/Controls Assessment
- Cloud Applicability Analysis
- Report on Residual Risk
Request for Assessment

- A single point of access to submit a request for TRO Services
  - Recommend that a Business Associate Agreement be in Place

A business agreement governs the relationship between two parties who are exchanging information and services. The agreement serves as a guideline for how the information may be used so that both parties are properly protected in case of legal problems. A business associate agreement is a particular kind of document used primarily to regulate how health information is treated.

- Project Manager request one or more of the services from the TRO.
  - The Project Manager will act as the liaison between the person performing the Vendor Risk Assessment and the Vendor.
A Service Risk Assessment (SRA) Questionnaire is provided to the Project Manager who will work with the Vendor for determine the Inherent risk associated with the service or software the Vendor would like to provide. The SRA will calculate the Inherent Risk determining on the responses to the questions.
What about “Sub”-Vendors?

Vendors may sub-contract other vendors to help with the delivery of their services. These sub-vendors must also be taken into consideration when performing an assessment. Check with your legal department in order to gain comfort whether or not the sub is bound by your agreements with your primary vendor.
Determination of Inherent Risk

The completed SRA provides:

- Background information related to the vendor including contact information, whether or not the vendor is an existing vendor, estimated cost of the project, project timing.

- Data and Systems Security information (will PHI, PII, PCI be involved)

- How will the vendor access data on our network? (Using our hardware or their hardware)

- How will the vendor use our data?

- Are the services provided within the US or Outside of the US?
Determination of Inherent Risk cont’

- Business Continuity – if the vendor service or software were to become unavailable, would there be impact to our business? (Member/Patient, Compliance, Financial)

- Reputation – Would the vendor interact directly with our customers? Will our customers be providing data to the vendor? Will the vendor be providing branded products or services?

- Regulation – Will there be impact to any of the following regulations?
  - HIPAA
  - PCI
  - SOX
Report on Inherent Risk

- If the Inherent Risk is determined to be:
  - Very Low, Low, or Medium
    The Project Manager and the Technology Risk Program Manager (TRPM) are notified. A short report is included with this notification indicating how the Inherent Risk was determined. Generally Vendor Agreements may be finalized at this point.
  - High or Very High
    The Project Manager and the (TRPM) are notified and efforts are begun to determine the Residual Risk that may potentially exist related to the Vendor engagement. A recommendation is made to further investigate the Vendor’s internal IT control environment.

Note: The role of the TRPM is to advise Corporate Senior Management as to risks associated with taking on a vendor project or service and not to determine whether to.
What to do if the Risk is determined to be High or Very High?

More extensive work must be performed if the Inherent Risk is determined to be High or Very High.

We need to determine what controls the vendor has in place to mitigate risks that may impact the delivery of services or product.
Applicability Analysis/Controls Assessment

It is important to emphasize that this is not an audit.

In an audit, you have a "standard" and an explanation of how the activity should be performed (normally a process or procedure). The auditor is there to check firstly whether the described process conforms to the standard and secondly whether the operators are following the described process. An audit is therefore a control to check whether people are doing what they are told they should be doing.

In an assessment, there is no "standard". This is replaced with a set of concepts and principles. These describe desirable outcomes but not the specifics on how they should be achieved; that's up to the organization to decide. The Assessors are there to find out why people have chosen to do things the way they do and what other options have been considered. The objective is therefore learning.
Applicability Analysis/Controls Assessment cont'

Areas Covered:
- Data Security and Privacy
- Physical and Environmental Security
- User Access and Privilege Management
- Continuity of Operations
- Security Strategy and Policy
- Infrastructure Security
- Asset Management
- Monitoring and Incident Management
Cloud Applicability Analysis

Areas Covered include:

- Business Disruption and Disaster Recovery
- Critical Asset Inventory with Ownership defined and documented
- Data Security Controls
- System Availability, quality, and capacity
- Information Security and Personnel
- Information Security Management
- Network Security Management
- Physical Controls
- Presence of an Enterprise Risk Management Framework and Policy
- Program for systematic monitoring
Preliminary Report on Residual Risk

Purpose:
To share Control Assessment Risk Findings with the Project Manager and Other Critical team members and collectively decide if an Onsite Vendor Review should be recommended. Ensure the project team understands the Overall Vendor Risk level and specific Risks that will be included in the Final Assessment Report.
On-site reviews

- If the vendor cannot or will not complete the Control Assessment questionnaire
- The Project Team specifically requests that an on-site review be performed
- Judgmental concerns of the person performing the Assessment
Final Report on Residual Risk

The Final Assessment Report provides an overall and detailed summary of Vendor Inherent, Residual and Future Risk and also itemizes Risk/Findings that require follow-up.
Unresolved Control Issues – A Quiz

What if the Vendor cannot resolve the identified control issues before the contract start date?

a. Ignore the identified controls issues.

b. Tell the vendor that all bets are off, “Go pound sand!”

c. Put off the “go live” date because our business is not as important as that of the vendor.

d. Proceed with signing the contract and begin the implementation plan with the mutual understanding that the vendor will address all identified issues before the “go live” date.
Corrective Action Plan (CAP)

- The Corrective Action Plan is a plan that is initiated if there are unresolved risks that exist after the Control Assessment process has been completed.

- Per the CAP the vendor will be given 90 days to resolve/remediate identified risks to the satisfaction of the TRO.

- Progress on the CAP is closely monitored.
Who is Responsible for the CAP

After the Final Report has been issued, the report and associated findings are passed on to the Vendor Risk Management Group. The Vendor Risk Management Group is responsible for monitoring on-going Vendor Relationships (aka Sustainment).

The issuance of the Final Report marks the completion of the Vendor Risk Assessment process.
The End

Questions?

Jennifer F Alfafara
Consultant, RGP
(949) 584 – 7053
jenniferalfafara@me.com