Vendor Risk Management Best Practices

February 13, 2015

weaver
Assurance • Tax • Advisory
Agenda

• Introduction
• Who are the Players?
• Third Party Risk
• Becoming a **Target**
• Risk Identification
• Risk Assessments
• Risk Response
• Takeaways
Key Trends

General Trends
- Outsourcing
- Regulation
- Transparency
- Contractual

Audit Trends
- Risk Based
- Focus on Vendors/Partners
- Creating Insight and Value
- Risk Responsibility
Where’s the Stolen Data
DARKNET
Where is Your Data

• Stolen Data – most likely sold on the **Darknet** - a computer network with restricted access that is used chiefly for illegal peer-to-peer file sharing

• Short for dark Internet
  – In file sharing terminology, a darknet is a private network where information and content are shared by darknet participants anonymously
  – Users cannot be traced, tracked or personally identified. Usually, darknets are not easily accessible via regular Web browsers

• Extensions end in “.Onion”
• 1 HVAC Vendor with network access
  – Refrigeration/heating company near Pittsburgh whose data connection to Target was for billing, contract submission, and project management
  – Accessed system using stolen credentials from third-party vendor

• Impact:
  – 40 Million credit / debit cards accessed
  – 46% Drop in profit 4Q 2013
  – $200 Million lost by banks reissuing cards
  – $100 Million planned by Target to upgrade to Chip and Pin cards

• Would your risk management program identify this vendor as high risk?
Data Recovery

• Can data be recovered – very difficult and typically through cyber-counterintelligence professionals
• Prevention is the best alternative
  – Insurance coverage is beginning to be addressed
Risk Identification
Risk identification seeks to identify and address risks here... instead after they have impacted the company of reacting to risk events here.

**Stage 1 - Root Cause Event Signal**
- Factors that create a high risk environment
- Identified through monitoring Key Risk Indicators

**Stage 2 - High Risk Environment**
- High risk environment resulted from signals identified in Stage 1
- High potential for root cause event

**Stage 3 - Root Cause Event**
- Event occurs that creates potential for risks to be realized

**Stage 4 - Risk Realization and Consequence**
- Significant risk event occurs, impacting the company
- Snowball effect occurs causing risks to multiply:
  - Reputation risk
  - Fraud risk

**Stage 5 - Management / Mitigation**
- Management evaluates outcome and establishes mitigation strategy to avoid future risk.
Lifecyle of a Risk Event

Stage 1 - Root Cause Event Signal
- Tire pressure is low

Stage 2 - High Risk Environment
- Flat tire

Stage 3 - Root Cause Event
- Car Accident

Stage 4 - Risk Realization and Consequence
- Increased insurance cost
- Placed into high risk pool
- Inability to negotiate terms

Stage 5 - Management/Mitigation
- Switch insurance providers
- Wait for accident to clear from record
- Take defensive driving
- Check tire pressure regularly

If the risk had been identified here through monitoring of Key Risk Indicators…

... the cause event may never have occurred...

... and the risk may never have been realized.
Risk Identification

• Identify risk upfront during due diligence

• Build a program for risk identification
  – For example, vendor profiling

• Biggest challenge is getting the data!
  – Create a process to obtain it
Risk Assessment
Risk Definitions

Risk Assessment is **not** the same as Risk Management.

**Risk Assessment:**
Identify and evaluate individual risks in order to determine risk responses.

**Risk Management:**
Identify, assess and respond to risk on an ongoing basis — requires building a processes to manage risk.
Typical Risk Assessment Methods

Methods for Assessing Risk: Choose one of the four effective data collection methods for collecting information about significant risks.

**Self-Assessment**
- **Advantages**
  - Participants generally close to the process and can easily identify exposure areas.
- **Disadvantages**
  - Self-Assessment may miss key areas due to lack of involvement of others.
  - May not be objective.

**Questionnaire**
- **Advantages**
  - Specific questions asked.
  - Works well if decentralized operations.
- **Disadvantages**
  - No opportunity for discussion. Required extra effort for follow up if responses are not clear.

**Participatory / Open Forum**
- **Advantages**
  - Involves many perspectives. Creates "buy in" & awareness of RA importance.
  - Discussion format, healthy for the organization.
- **Disadvantages**
  - Some may hesitate to speak out in a group.

**Internal Audit**
- **Advantages**
  - IA has the ability to ask probing questions of participants.
  - IA personnel have expertise.
- **Disadvantages**
  - IA may have pre-determined opinions based on prior internal audit areas, may miss new areas of exposure.
Risk Assessment - How?

• Risk profile on existing third parties - rating methodology

• Establish risk factors and evaluate vendor against relevant risk factors

• Further due diligence based on risk assessment

• Establish more detailed risk assessment based on investigations (not just a rating)
Direction of Risk

- Direction or trend in risk:
  - Stable
  - Increasing
  - Decreasing
Risk Response
Management’s Risk Responses:

- Considers alternative responses
- Evaluates costs/benefits of available risk responses
- Analyzes whether risk responses appropriately reduce risk to tolerable level
- Selects most appropriate risk response based on risk appetite, risk tolerance, and evaluation of portfolio risk
Third Party Assurance

- What is the specific scope of each type of report?
- What are the areas of overlap?
- What are the unique areas for each audit type?
- What are some other third party IT audits?
## Standards and Names

### Trust Services Principles and Criteria

<table>
<thead>
<tr>
<th>SERVICE ORG CONTROL 1 (SOC 1)</th>
<th>SERVICE ORG CONTROL 2 (SOC 2)</th>
<th>SERVICE ORG CONTROL 3 (SOC 3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSAE16 - Service auditor guidance</td>
<td>AT 101</td>
<td>AT 101</td>
</tr>
<tr>
<td>Restricted Use Report (Type I or II report)</td>
<td>Generally a Restricted Use Report (Type I or II report)</td>
<td>General Use Report (with a public seal)</td>
</tr>
<tr>
<td>Purpose: Reports on controls for F/S audits</td>
<td>Purpose: Reports on controls related to compliance or operations</td>
<td>Purpose: Reports on controls related to compliance or operations</td>
</tr>
</tbody>
</table>

Note: The SOC 3 report is the SystTust for Service Organizations.
Report on controls at a service organization relevant to a user entity’s internal control over financial reporting

- Contents of report package:
  - Description of service organization’s system
  - CPA’s opinion on fairness of description, suitability of design, operating effectiveness of controls
SOC 2SM Report – 5 Trust Services Principles

Security
• The system is protected against unauthorized access (both physical and logical)

Availability
• The system is available for operation and use as committed or agreed

Processing integrity
• System processing is complete, accurate, timely and authorized

Confidentiality
• Information designated as confidential is protected as committed or agreed

Privacy
• Personal information is collected, used, retained, disclosed and disposed of in conformity with the commitments in the entity’s privacy notice, and with criteria set forth in Generally Accepted Privacy Principles (GAPP) issued by the AICPA and Canadian Institute of Chartered Accountants
SOC Reports - Type 1 versus Type 2

Both report on the fairness of the presentation of management’s description of the service organization’s system, and...

- **Type 1** also reports on the suitability of the design of the controls to achieve the related control objectives included in the description as of a specified date (i.e. as of June 30, 2013)

- **Type 2** also reports on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives included in the description throughout a specified period (6 to 12 months)
Service organizations have many uses and reasons for obtaining SOC reports which all achieve the same result; reporting on internal controls.

- Can a SOC 1 be used by a data center?
- Can a SOC 2 be used by a financial statement auditor?
- Can you post a SOC 2 report on the service organization website with a disclaimer?
- If a TSP criteria in a SOC 2 is not met, does it automatically preclude an unqualified opinion?
- What assurance is received from a SOC 3?
- What should you look for in evaluating an SOC report?
What should you look for in evaluating a SOC report?

- Auditor’s opinion – unqualified or if qualified does it impact the use of the report or your conclusion
- Services covered
  - All relevant services used
  - Locations used
  - Exceptions
- Date of the report coverage period – how much time has elapsed / bridge letter
- Service auditor credibility – peer reviewed, state board, professional organizations
- Is the SOC report enough to mitigate your risk?
• Federal Risk and Authorization Management Program (FedRAMP)
• Conflict Minerals Disclosure
• What audits/reviews does the contract require the vendor to obtain?
Relying on an Audit

Considerations for relying on third party assurance:

• Confirm the type of report

• Evaluate coverage within the report – does it apply to your control environment

• Have the right personnel evaluate the reports

• Push back and insist on performing your own audit (when necessary)

• Validate the external audit or consulting firm performing the procedures
Vendor Internal Audits

How much of your plan is dedicated externally?
Risk response is an ongoing program that identifies, assesses and responds to third party risk:

- Vendor programs
- Evaluating and monitoring partner relationships
- Customer profiles

**Avoid**
Eliminate cause of risk

**Mitigate**
Reduce probability of impact of risk

**Accept**
Contingency plans for risk

**Transfer**
Have third party take on responsibility for risk (insurance)
Vendor Management Components
Best Practices in Vendor Management Policies

- **Security Policy** - Have the policies been approved in last 12 months that covers the company’s risks?

- **Organizational Security** - Do external parties have access to scoped systems and data or processing facilities?

- **Asset Management** - Is there a policy? Is insurance coverage for business interruptions?

- **Human Resource Security** - Is there a security awareness training program? Background screening for those with physical / system access.

- **Physical and Environmental Security** - Are there physical controls over building / data center access.
Best Practices in Vendor Management Policies (continued)

- **Communications and Operations Management** - System backups, anti-virus/malware policies, firewalls, vulnerability assessments, etc. in place?

- **Access Controls** - Are unique user IDs used for access, remote access permitted?

- **Information Systems Acquisition Development & Maintenance** - Is application development performed? SDLC process?

- **Incident Event and Communications Management** - Is there an Incident Management program?

- **Business Continuity and Disaster Recovery** - Is there an annual schedule of required tests? Understand what changes were made from the testing.
• **Compliance** - Is there an internal compliance and ethics reporting mechanism and training program for employees to report compliance issues?

• **Mobile** - Does the vendor allow Scoped Systems and Data to be accessed on Mobile Devices?

• **Privacy** - Is there formal privacy awareness training for employees, contractors, and third-party users to ensure confidentiality and privacy of Scoped Data?

• **Cloud** - Are Cloud Services provided? Are encryption and other security features in place and tested?
Key Takeaways

- Third Party Risk Management, like ERM, is a journey, not a destination

- Embed the process into the organization’s decision making

- Effective third party risk management is dependent on good data

- Good data requires a good process for collecting and analyzing third party profile data
Key Takeaways

• Third Party Risk Management is about better communication and collaboration within business units, senior management, operations and administrative.

• Organizations that identify risk, understand how the third party manages risk that impacts their control environment, will be better able to develop effective response plans.
About Weaver

Largest independent accounting firm in the Southwest, with seven offices across all major Texas markets

Nationally ranked as a top-50 firm – named a “BEST of the BEST” CPA firm by INSIDE Public Accounting (2014)

Ranked #41 by Accounting Today (2014) and #37 by INSIDE Public Accounting (2013)

FY 2014 revenues of approximately $87 million

Founded in 1950 in Fort Worth, Texas

Approximately 500 employees, including 72 partners

Member of the Baker Tilly International network of firms
Industries Served

- Financial Services
- Government Services
- Oil and Gas
- Technology
- Renewable Energy
- Manufacturing, Distribution & Retail
- Real Estate
- Construction
- Healthcare
- Nonprofit
- Insurance
Speaker Profiles

Bruce Zaret, CPA, CRMA

bruce.zaret@weaver.com
(972) 448-9232

Bruce is a Partner with more than 25 years of experience in public accounting. He specializes in providing internal control, risk management and due diligence services to the financial institutions and oil & gas industries.

Neha S. Patel, CPA, CISA

neha.patel@weaver.com
(972) 448-9804

Neha is a Senior Manager with more than 11 years of experience in public accounting. Neha specializes in performing IT audits (like SOX) and is one of the firm’s leaders in third party assurance like SOC audits.
Thank You!