Developing and Maintaining a World-Class Third Party Risk Assessment Program

Presented by:
Tom Garrubba, Senior Director, The Santa Fe Group/Shared Assessments Program

Monday, September 15, 2014 - IIA Pittsburgh
Agenda

- Why the “sudden” focus on third party risk?
  - Increased regulatory and standards focus
  - Increased targeting of service providers

- How a “Premier integrated pharmacy services provider” built their TPR Management Program

- Laying the ground work for using vendor questionnaires
  - Vendor identification
  - Vendor classification

- TPR Program Lifecycle
  - Phase I – Pre-assessment
  - Phase II – Assessment
  - Phase III – Post-Assessment
  - Phase IV – Criteria Evaluation
Agenda

- Discussion of Tools to Use
  - The VRMMM (Vendor Risk Management Maturity Model)
  - The SIG and SIG Lite (Standard Information Gathering) Questionnaires

- Key take-aways
Regulatory Pressure Increasing

Protected Data Types
- Intellectual Property (IP)
- Personally Identifiable Information (PII)
- Payment Card Industry (PCI)
- Protected Health Information (PHI)

Source: Prevalent http://www.prevalent.net/
Mega Breaches

<table>
<thead>
<tr>
<th>Breaches</th>
<th>2011</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identities Exposed</td>
<td>232M</td>
</tr>
<tr>
<td>Breaches &gt;10M</td>
<td>5</td>
</tr>
</tbody>
</table>

2013 was the Year of the Mega Breach
Breaches by Sector

Data Breaches by Sector, 2013
Source: Symantec

Healthcare, education and the public sectors accounted for 58% of all data breaches

But, the retail, computer software and financial sectors accounted for 77% of all identities exposed in 2013
Costs Associated with a Breach…

“…companies had to spend more on their investigations, notification and response when their sensitive and confidential information was lost or stolen. As revealed in the 2014 Cost of Data Breach Study: Global Analysis, sponsored by IBM, the average cost to a company was $3.5 million in US dollars and 15 percent more than what it cost last year (2013).”

- Source: Ponemon Institute; Cost of Data Breach: Global Analysis; (May 5, 2014)
Case Study: How a “Premier integrated pharmacy services provider” build their TPR Management Program
Case Study: How a “Premier integrated pharmacy services provider” build their TPR Management Program

Program Initiation and Alignment

Use this formula for a successful implementation…

\[ P = p_1(p_2 + p_3) \]

* **Garrubba-Mortensen Theorem**

* the-ərəm/ THēərəm/
1. Noun: A general proposition not self-evident but proved by a chain of reasoning; a truth established by means of accepted truths.
2. A rule in algebra or other branches of mathematics expressed by symbols or formulae.
Case Study: How a “Premier integrated pharmacy services provider” build their TPR Management Program

**Program Initiation and Alignment**

Use this formula for a successful implementation…

\[ P = p_1(p_2 + p_3) \]

**Process** - series of *documented* actions or operations; *streamlined!*
- Questionnaires, audit steps, internal & external resources; documentation to review; Turnaround times;
- Communication protocol, reporting

\[ P = p_1(p_2 + p_3) \]

**Practices** - your way of “doing things”
- *Daily tasks:* must be *consistent* and *understood* by your management!
- \( p_2 + p_3 = \) your *operating procedures* to execute assessments!

\[ P = p_1(p_2 + p_3) \]

**Policy** – Written and Communicated by the C-suite; may even be an executive “Proclamation”
- *Must have* in first position!
Case Study: How a “Premier integrated pharmacy services provider” build their TPR Management Program

Program developed to ensure vendors that collect, store, transmit, use, process, interface, or destroy data on behalf of CVS Caremark have an adequate information security program and privacy controls in place to protect confidential information:

- Protected Health Information (PHI)
- Personally Identifiable Information (PII)
- Payment Card Industry - Data Security Standard (PCI) - Cardholder Data (aka, “CHD”)
- Strategic (proprietary), operational or financial information of CVS Caremark

©2014 The Shared Assessments Program. All Rights Reserved.
Case Study: How a “Premier integrated pharmacy services provider” build their TPR Management Program

- The CVS Caremark VAP is based on the BITS Shared Assessment framework
- Covers both existing vendors and potential new vendor relationships if they are to have access to confidential or strategic information:
  - Any of their subcontractors that may have access to CVS Caremark data
  - Off-Shore vendors/subcontractors
  - Vendors with MED-D impact
Case Study: How a “Premier integrated pharmacy services provider” build their TPR Management Program

- Assesses Business Partners who associate with CVS Caremark to address an objective of CVS Caremark:
  - Clinical research partners
  - Universities (healthcare studies)
Case Study: How a “Premier integrated pharmacy services provider” build their TPR Management Program

- **Quantified our risk** with Third Party Service Providers via…
  - Exposure Ranking (performed *before* a new assessment)
    - Number of Records
    - Type of Data (Basic PII, Sensitive PII, PHI, CHD, IP)
    - Annual Spend (in $$$)
  - VARR (Vendor Assessment Risk Rating) Score (performed *after* a net-new assessment for the purposes of scheduling a reassessment)
    - Exposure Ranking
    - SIG Score
    - Assessor Score
Types of Implementation

TPRP Operations can be implemented in one of two structures:

Centralized  Decentralized
Centralized Structure

- Centralized operations tend to have the following:
  - Contained within a single business unit reporting to a CxO
  - Is known to all stakeholders (i.e., BU’s) across the enterprise
  - Offers a one-stop shop for other stakeholders to go to
  - Applies consistent assessment methodologies and execution strategies
  - Tend to have more structure in their processes and practices…
  - Tends to apply the $P = p_1(p_2+p_3)$ formula
  - More smoothly run operationally
Centralized Structure (Challenges)

- It’s often difficult for VAP assessors to know all that is going on with larger third party service providers (i.e., multiple scopes, project, applications being supported, etc.)
- Getting timely participation by smaller TPSP’s who are managed by large business partners/vendors to cooperate, that is; the assessment tends to get “lost in the shuffle” by the parent vendor overseeing the relationship
- May not truly understand the needs of every BU and why they have selected or are using a particular TPSP
  - If an assessment doesn’t go well “bad blood” may occur to have to force the BU to cut the TPSP off!
Example: Centralized Structure

CISO/ CPO/ CIO/ CCO/ COO/CRO/CA

VP/ Managing Director

Director/Manager
Third Party Risk Program
(Administration)

VAP Analyst
VAP Analyst
VAP Analyst

Director/Manager
Third Party Risk Program
(Security Assessments)

Security Assessor
Security Assessor
Security Assessor

External Assessment Augmentation
Decentralized Structure

- TPR Assessors reside in multiple business units, reporting up to multiple Business Unit VP’s; silo-ed operations
  - *Solid-line* up to the BU VP
  - *Dotted-line* to a VAP Manager/Director
- Stakeholders (i.e., BU VP’s) want *control* over their TPSP’s, thereby handling the assessment of the TPSP gives them a form of control
- BU’s who tend to maintain an IT services team in their group usually have someone dedicated to TPR tasks
Decentralized Structure (Challenges)

- Tend not to have a centralized *policy* and apply inconsistent assessment *methodologies* and execution strategies (that is; not utilize $P = p1(p2+p3)$)

- Inconsistent assessment methods likely occur as assessors tend to use *different tools* for assessments (i.e., using tools other than the SIG)

- May pose little knowledge sharing outside of the BU with respect to their TPSP’s or the results of the assessments

- May have inconsistent report distribution of assessments to appropriate levels of management

  - Assessment reports do not always get to other Stakeholders who may utilize the TPSP for other projects
Example: Decentralized Structure
Types of Implementations

What Method is right for your organization?

Centralized  Decentralized

YOU NEED TO DECIDE!
Laying the Groundwork for Using TPSP Questionnaires

Know your TPSP

- **Identification** – who are they and want do they do?
  - Who are your third party service providers?
  - What services do they provide?

- **Classification** – what risk do they present to your organization?
  - Vendor risk rating and classification
TPSP Identification

- Who are your third party service providers?
  - Shared services
  - Software providers
  - Cloud providers and other “hosted” services
  - Outsourced services (e.g., certain HR functions)
  - Vendors
  - Any entity who provides you with goods/services
TPSP Classification

- Define your TPSP’s by what they do (i.e. scope of work) and what they can access (e.g., data):
  - What data/systems do they have access to?
    - PII?
    - PHI?
    - CHD (PCI)?
    - Corporate confidential/intellectual property?
  - What is the risk to that data/system?
    - What is the risk exposure (or “ranking”) to that data?
    - What is your tolerance of risk?
    - How is it calculated? Is it the same across the board (i.e., same for PII, PHI, CHD, IP/strategic, etc.)?
TPSP Classification

- TPSP risk classification/rating
  - Established standards for risk tiers/classifications based on corporate risk tolerance
    - Contract requirements
    - Level/type of assessment
    - Frequency of assessment
  - Consistent assignment of vendor risk classifications
  - Validation of TPSP risk classification included in periodic assessment
TPSP Assessment Program Lifecycle
TPSP Self-assessments

- Define scope
- Define data in use
- Distribute SIG

Phase 1: Pre-Assessment
- TPSP risk rating
- Change(s) in services
- Risk scoring

Phase 2: Assessment
- Perform kickoff
- Obtain BU and vendor docs
- Acquire SIG responses

Phase 3: Post-Assessment
- Update BU and vendor management
- Track CI’s (“issues”)
- BU/vendor docs
- Remediate CI’s

Phase 4: TPSP Criteria Evaluation
- TPSP self-assessments
Phase 1  Pre-Assessment

- **Who?**
  - *Who exactly do we assess?*

- **What?**
  - *What are we to assess?*

- **Where?**
  - *Where should we assess them (i.e., what locations?)*

- **When?**
  - *When do we assess? When do we re-assess?*
Who Do We Assess?

- Any vendor that performs the following to our data:
  - Collect
  - Store
  - Transmit/transport
  - Use
  - Process
  - Interface
  - Destroy
What are we to Assess?

- At what level do we look at the vendor?
  - Enterprise?
  - Geographic?
  - Business line (i.e., service)?
  - Scope/solution specific?
  - Combination of one or more of the above?
What are we to Assess?

- Determine the scope of the assessment
  - TPSP risk rating
  - Standard corporate requirements
  - Type of services provided
  - Type of data
  - Periodic or event triggered
- Determine appropriate assessment questionnaire to be utilized
- Provide instructions to TPSP
  - Specific requirements
  - Assessment timeline
Where do we Assess them?

- State-side:
  - Any place handling your sensitive information that if a breach occurs it could result in significant damage or unnecessary costs to your organization

- Offshore:
  - *Any country*; but certainly one that is not bound by a safe-harbor agreement
When do we Assess and Re-assess?

**Assess:**
- When you are notified of:
  - A new TPSP or an existing TPSP that experiences a change to their business
  - An existing vendor with a *modification* of their current scope of work
  - An existing vendor with a *new/different* scope of work

**Re-assess:**
- When you are notified of:
  - A scheduled point in time for the reassessment to begin based on predetermined criteria
Phase 2 - Conducting The Assessment

Who should conduct the assessment?

- Type of Governance
  - Centralized
  - Decentralized

- Business Unit
  - TPSP management organization
  - TPSP relationship manager(s)
  - Risk management
  - Corporate compliance
  - Procurement
  - IT security
  - Training
Phase 2 - Conducting The Assessment

- Who should conduct the assessment?
  - Resource considerations
    - Training
    - Budget
    - External
Phase 2 tasks

- Kickoff meeting with vendor
  - Contacts? Deliverables? Timelines?
- Request/review pertinent documentation:
  - Documentation
    - Contracts, SOW’s, NDA’s
    - TPSP internal docs
- Follow up on any discrepancies regarding services/locations
- Identify any potential critical items/contingent items (CI’s) i.e., audit issues/findings
- Have exit interview to ensure CI’s are accurate
- Compose the assessment report
  - Report presented to vendor and internal business owner
Phase 2 - Conducting The Assessment

How to effectively use assessment results

- Use your assessment results
- Prioritize – risk rank areas and/or specific questions
- Establish a process to define and identify TPSP performance issues
- Report vendor performance issues to appropriate levels of management
Phase 3 - The Post-Assessment

- Remediating vendor performance issues
  - All issues should be risk ranked and prioritized for corrective action
  - Assign appropriate individual(s) responsible for closing issues
  - Timeline for closing issues should be established and communicated to vendor
    - Monitor prioritized issues to ensure corrective action is taken in a timely manner
    - Escalate to management if timelines not met
  - When termination is unavoidable
Phase 4 – Criteria Evaluation

- TPSP termination without business interruption
  - Well defined termination/exit strategy – must be fair to both parties
    - Ongoing services during winding down period
    - Work product and IP transition
    - Same TPSP team to remain in place (unless they are the issue)
    - Cooperation with new vendor
    - Parallel services
    - Cost
    - Data security and transfer/destruction (with applicable assertion)
    - Recovery/destruction of data from subcontractors
    - Ability to audit/validate requirements met
How *frequently* should a TPSP be assessed?

- Scheduled/periodic review schedule should be developed during requirements phase and based on the TPSP risk rating, and other prioritized factors

- Event triggered reviews/assessments are based on specifically identified events
  - Data breach/incident
  - Merger/acquisition
  - “Act of God”
  - Contract breach
  - Performance “failure”
  - Location changes
Discuss: the Full SIG Lite and SIG Lite

- Full SIG
  - When to use the full SIG
- SIG Lite
  - When to use it in lieu of the full SIG
The focus of the VRMMM is to provide third party risk managers with a tool they can use to evaluate their program against a comprehensive set of best practices. Using governance as the foundational element, the model identifies the framework elements critical to a successful program.
The Shared Assessments Vendor Risk Management Maturity Model (VRMMM)

- High-level components are broken down into subcomponents in a manner that makes the model adaptable across a wide spectrum of industry groups.

- Being able to identify specific areas for improvement the VRMMM allows companies to make well-informed decisions on how to spend limited resources to most effectively manage vendor related risks.
The Finish Line…

Your Take-Away’s

1. Have a general understanding what it takes to implement and maintain a TPR assessment program
2. Make sure you have developed a thorough framework for using vendor questionnaires
3. Know your W’s – the who, what, where and when of vendor assessment
4. Make sure that completed TPSP questionnaires are properly reviewed and mitigation plans are developed and tracked for completion

©2014 The Shared Assessments Program. All Rights Reserved.
For More Information

- www.sharedassessments.org
  - Resources
    - FAQs and tips for getting started
    - Case studies
    - Enterprise Cloud Computing Guide
  - Members
  - Partners

Contact:
- Julie Lebo; VP of Member Relations: 703-533-7256; julie@santa-fe-group.com
- Tom Garrubba; Sr. Director, Shared Assessments Program: 412-720-4248; tom@santa-fe-group.com

©2014 The Shared Assessments Program. All Rights Reserved.