RISK MANAGEMENT FOR THIRD-PARTY RELATIONSHIPS

Webcast Series - Part I
February 18, 2016
THE POWER OF BEING UNDERSTOOD

AUDIT | TAX | CONSULTING
Experience the Power of Being Understood

- On October 26, 2015 McGladrey LLP changed its name to RSM US LLP and united with fellow firms in its global network under the common brand – RSM

- We remain an independent member of the RSM International network globally, which encompasses:
  - 110 countries
  - 730 offices
  - 37,500 people internationally

- This is accelerating our vision to be the first-choice advisor to middle market leaders globally
INTRODUCTION
Presenters

Dan Ramey
RSM US LLP
Director, Risk Advisory Services

Tauseef Ghazi
RSM US LLP
Director, Risk Advisory Services

Rick Shriner
RSM US LLP
Principal, Risk Advisory Services
Agenda

• Define third-party relationships
• Discuss how the Three Lines of Defense model applies to third-party relationships
• Highlight the third-party relationship lifecycle and provide a point-of-view on characteristics of an effective third-party relationship management (TPRM) program
• Review current issues around TPRM and share perspectives on two critical risks impacting TPRM today:
  ▪ Anti-bribery compliance
  ▪ Security & privacy
A third-party relationship is any business arrangement between an organization and another entity, by contract or otherwise.

<table>
<thead>
<tr>
<th>Examples of Third-Party Relationships</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendors</td>
</tr>
<tr>
<td>Distributors</td>
</tr>
<tr>
<td>Customers</td>
</tr>
<tr>
<td>Subcontractors</td>
</tr>
<tr>
<td>Contract Manufacturers</td>
</tr>
<tr>
<td>Brokers</td>
</tr>
<tr>
<td>Agents</td>
</tr>
</tbody>
</table>
The Three Lines of Defense Model

1st Line of Defense:
- Management Controls
- Internal Control Measures

2nd Line of Defense:
- Financial Control
- Security
- Risk Management
- Quality
- Inspection
- Compliance

3rd Line of Defense:
- Internal Audit

Governing Body / Board / Audit Committee

Senior Management

External audit

Regulator

Image used with permission by the Institute of Internal Auditors
TPRM Maturity Continuum

<table>
<thead>
<tr>
<th>Weak</th>
<th>Sustainable</th>
<th>Mature</th>
<th>Integrated</th>
<th>Advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ad-hoc processes</td>
<td>Problem driven</td>
<td>Inconsistent outcomes</td>
<td>Rework</td>
<td>Reactive</td>
</tr>
</tbody>
</table>
The Increasing Importance of TPRM

The following factors contribute to the need for a strong, demonstrable TPRM:

• Recent business changes:
  ▪ Mergers
  ▪ Acquisitions
  ▪ Enterprise-Wide Technology Deployment (i.e. ERP software)
• Increased importance of global sales and supply chains
• High turnover in third-party relationships
• Known third-party data breaches or breach of contract
• Increased offshoring / outsourcing activity
• Off-shoring of key data (financial, operational, sensitive)
• Lack of a solid baseline for third-party risks
THIRD-PARTY CONSIDERATIONS RELATED TO ANTI-BRIBERY RISK
Third-parties are frequently involved in the perpetration of bribes to foreign government officials

“Funding for those [illicit] payments came from funds generated by discounts provided to Company’s network of distributors.”

“…Company made the payments to Official through the Freight Forwarding Agent who had previously paid bribes on behalf of Company”

Source: Department of Justice, company names redacted

Governments have made it increasingly clear that companies are responsible for the activities of their third-parties with respect compliance with the Foreign Corrupt Practice Act (FCPA)
Overview of the FCPA

Antibribery provision

Prohibits U.S. person, U.S. company or any other person in the U.S. from corruptly paying or offering to pay anything of value directly or indirectly to a foreign official to:

- Secure an improper advantage
- Influence a foreign official in his official capacity
- Induce him to violate the law
- Assist in obtaining, directing or retaining business

Proof of actual knowledge of a payment or promise to pay is not required

Accounting provision

Books and records component requires companies to maintain its books and records in a reasonable level of detail.

Internal controls component requires that companies devise and maintain a system of internal accounting controls that can reasonably prevent and detect corrupt or unauthorized transactions

Who is covered

The accounting provision of the FCPA applies only to public companies, but all companies must adhere to the Act’s anti-bribery provisions.
Corruption Challenges throughout the TPRM Lifecycle

How and why a company’s third-party management programs often fall short in preventing or detecting corruption schemes:

- Third-party ownership, qualifications, and justification for retention were never sufficiently vetted (or documented)
- A third-party risk management plan was not developed as part of due diligence

- Many contracts pre-date the current management team, lack key provisions, or are incomplete
- Combination of personnel turnover, contract addenda, and off-contract agreements create fragmented and conflicting expectations of third-party responsibilities
How and why a company’s third-party management programs often fall short in preventing or detecting corruption schemes:

- Intimate knowledge of third-party existence and activities are limited to comparatively few employees
- Pricing and discounting approval processes are poorly controlled, allowing for abuse
- High-risk third-party responsibilities such as licensing, marketing, or customs clearance are often not considered adequately in company internal control programs (e.g. Sarbanes-Oxley)
- Monitoring efforts are often relegated to annual online training or certification activities
- Representations by sales, marketing, and other management are accepted with little or no independent verification
Third-Party Corruption Risk Realized: An Example

What: Previously unknown consultant serving as intermediary to local Latin American government agency

How found: Review of local payment records using analytic: recurring transaction amount, subsequent inquiries and review of supporting materials

What we learned: Consultant was hired by Company in 2012 to provide consulting services and administrative procedures in connection with the Ministry of Public Health and related entities in connection with the opening of laboratories and other activities on behalf of the company.

Summary of red flags:

- No company affiliation. Although internet/background searches connect Consultant with several organizations, Consultant is not associated with either in connection with her services to Company.

- Vague nature of consulting services. Acquired company had hired Consultant to “provide consulting services and handle administrative procedures and other related activities on behalf of Company.”

- Lack of anti-bribery contractual provisions. Consultant’s contract does not include prohibitions against bribery or breaches of ethical behavior.

- One-time payment. A contract between Company and Consultant states that a one-time payment of $100,000 will be made when a license or permit to open a laboratory is obtained.
What: Previously unknown consultant serving as intermediary to local Latin American government agency

How found: Review of local payment records using analytic: recurring transaction amount, subsequent inquiries and review of supporting materials

What we learned: Consultant was hired by Company in 2012 to provide consulting services and administrative procedures in connection with the Ministry of Public Health and related entities in connection with the opening of laboratories and other activities on behalf of the company.

Summary of red flags (cont.):

• Monthly fixed payments with no contractual end-date. The contract also specifies other payments to Consultant that include a monthly fixed amount of $800. According to electronic records Consultant has received a total of approximately twenty payments.

• Payments to Consultant are made inconsistently. Two payments of $800 appear to have been made to Consultant in January 2014, in addition to one made the month prior and one the month after.

• US management was unaware of the consultant.

As a result...

The company launched a formal investigation into the activities of the third-party, and consequently terminated the contract.
Bribery schemes involving third-parties have often been in place for several years or more – often making detection difficult.

A third-party review can be an effective pilot for identifying systemic weaknesses in your overall third-party risk management program.

The ability to demonstrate real evidence of your commitment to address compliance with the FCPA is critical in an investigation.
THIRD-PARTY CONSIDERATIONS RELATED TO SECURITY & PRIVACY
In the current economic, political and social landscape, addressing security has becoming a core necessity for most organizations:

- Customers are demanding higher levels of security assurance as concerns about privacy and identity theft rise.
- Business partners, suppliers, and vendors are requiring assurance from one another, particularly when providing mutual network and information access.
- Espionage through the use of networks to gain competitive intelligence and to extort organizations is becoming more prevalent.
- National and international regulations are calling for organizations to demonstrate due care with respect to security.
Businesses are demanding technological solutions to create value and efficiencies in the current processes to stay competitive.

The complexity and breadth of technology is increasing to support the evolving business needs.

Complexity is increasing the role of security and making it more strategic.

Therefore, the security organization needs to evolve from a fragmented state to an enabler for business:
- No longer a first step in asset protection
- Critical role in the exchange of sensitive data
- Essential for compliance

Deliver strategic cost savings for businesses while addressing security comprehensively.
Security Statistics – Third-Party Risk

PII was the most frequently exposed data (45% of claims), followed by PCI (27%) and PHI (14%).

Hackers were the most frequent cause of loss (31%), followed by Malware/Virus (14%). Staff Mistakes and Rogue Employees tied for third (11%).

Healthcare was the sector most frequently breached (21%), followed closely by Financial Services (17%).

Nano organizations experienced the most incidents (29%), followed closely by Small organizations (25%). Extremely large breaches occurred in Nano, Small and Large organizations.

Third parties accounted for 25% of the claims submitted.

The largest breaches occurred in the Retail sector, followed by Healthcare.

There was insider involvement in 32% of the claims submitted.

Data compiled from the NetDiligence - 2015 Annual Cyber Claims Study
# RSM’s Security Governance Framework

<table>
<thead>
<tr>
<th>Over Sight</th>
<th>People</th>
<th>Process</th>
<th>Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Understanding of Cyber Threats</strong></td>
<td><strong>Security Awareness &amp; Training</strong></td>
<td><strong>Identity &amp; Access Management</strong></td>
<td><strong>Security Architecture &amp; Design</strong></td>
</tr>
<tr>
<td><strong>Board &amp; Executive Oversight</strong></td>
<td><strong>Organizational Culture</strong></td>
<td><strong>Incident Management</strong></td>
<td><strong>Security Monitoring</strong></td>
</tr>
<tr>
<td><strong>Security Governance &amp; Strategy</strong></td>
<td><strong>Communications</strong></td>
<td><strong>Vulnerability &amp; Malware Management</strong></td>
<td><strong>Threat Modelling</strong></td>
</tr>
<tr>
<td><strong>Regulatory &amp; Legislative Compliance</strong></td>
<td><strong>Security Organization Structure</strong></td>
<td><strong>Sourcing &amp; 3rd Party Risk Management</strong></td>
<td><strong>Intrusion Detection &amp; Prevention</strong></td>
</tr>
<tr>
<td><strong>Public Relations</strong></td>
<td><strong>Roles &amp; Responsibilities</strong></td>
<td><strong>Information Asset Management</strong></td>
<td><strong>Configuration Management</strong></td>
</tr>
<tr>
<td><strong>Cyber Insurance</strong></td>
<td><strong>Security Skills &amp; Competency</strong></td>
<td><strong>Application &amp; System Development</strong></td>
<td><strong>End Point Security</strong></td>
</tr>
<tr>
<td><strong>Litigation &amp; Investigation</strong></td>
<td></td>
<td><strong>Business Continuity</strong></td>
<td><strong>Data Loss Prevention</strong></td>
</tr>
<tr>
<td><strong>Coordination with Law Enforcement</strong></td>
<td></td>
<td><strong>Physical Security</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Effective Management of Cyber Risk</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Establish a Disciplined Approach

Security and privacy programs are only as strong as their weakest links as demonstrated by recent cyber attacks.

A disciplined approach to Third-Party Risk Management can yield demonstrable progress toward key organizational metrics, including:

- Accurate response time for third-party data breach inquiries
- Decreased costs associated with third-party data breaches
- Better control of data shared
- Reduced customer turnover (due to third-party data breaches)
- Increased understanding of higher-risk third parties and specific outsourced processes / data

Sample Standards, Regulations and Considerations

- NERC CIP
- Smart Grid
- NIST
- ISO 2700x
- Sarbanes Oxley
- GLBA
- FFIEC
- PCI DSS
- FISMA
- FTC/CPNI
- HIPAA/HITECH
BUILDING A FRAMEWORK TO ASSESS TPRM RISKS
Overview of Approach

- Develop a framework for the assessment program, not just a questionnaire.
- Develop a workflow and process for conducting surveys, evaluating responses, weighting responses, compliance audit requirements and having the right information on which business decisions are made. These decisions include which third parties should provide additional information, those that would require an in-depth audit, or spot audit, and those where completion of the survey is satisfactory.
- The next step is the deployment of the surveys to the third parties in a tiered and practical approach.
- Risk areas to audit:
  - Operational Performance
  - Security (Information Privacy and Protection)
  - Regulatory Compliance
  - Personnel
  - Financial
    - Total spend analysis
    - Tax analysis
    - Self reporting accuracy
    - Other financial clauses (MFN, SLAs, etc.)

Step 1: 3rd Party Prioritization
Step 2: Refine the 3rd Party Risk Assessment Framework
Step 3: Deploy the 3rd Party Risk Assessment Survey
Step 4: Compliance Audit

Continuous Monitoring
Third-party risk areas and third parties themselves can be prioritized based on factors such as:

- Third-party impact on enterprise-level risks
- Operational performance including software quality, incident management, etc.
- Third-party access to critical business information
- Impact to the nature of the relationship (strategic, significant, considerable, insignificant)
- Contract language (specificity, operational versus financial, etc)
- Complexity of contracts (number of agreements, calculation of costs, complexity of pricing models)
- Evidence of potential errors or manipulation
- State of the relationship (new, ending, short-term, long-term)
- Geographic considerations (location of Vendor, multi-regional agreements)
- Strength of contract audit clause
- Financial strength of vendor
- Third-party reliance on sub-contractors or other third parties
- Regulations
Incorporate the knowledge gained through similar privacy and security program assessment engagements at industry leaders.

High-Level Third-Party Risk Assessment Program

Perform the following key tasks in developing the framework for a Third-Party risk assessment:

- Define roles and responsibilities for project team.
- Define the project plan, project charter, and communication plan.
- Determine and agree on the questionnaire format, quantity of questions, target audience, and delivery format.
- Develop workflow for risk assessment
- Develop weighting criteria
- Develop decision making criteria
- Strengthen Third-Party Security Standard
- Develop compliance audit program

BEST PRACTICES & STANDARDS
- INDUSTRY FOCUS
- REGULATORY REQUIREMENTS
- BUSINESS NEEDS
- GEOGRAPHY

DESIGN 3RD PARTY RISK FRAMEWORK

CURRENT STATE

GOVERNANCE & RISK
- POLICIES & PROCEDURES
- BUSINESS PROCESSES
- CRITICAL ASSETS
- CONTROLS
The goal of the third-party risk assessment workflow is to assess the level of risk the third-party relationships present to your organization.

- The third-party criticality is determined from the Prioritization Data evaluation.
- The control state is determined from the questionnaire scorecards.
- These two data points contribute to the combined third-party risk rating, which drives the level of focus and attention the third-party needs to be given from a security perspective.
Example Scorecard

- Responses to survey questions from each selected third-party are assessed and ranked using a scoring model customized for the organization.
- The example scorecard shows mapping to the ISO framework however this can be provided in a wide variety of security frameworks.

Take Away

- Develop and enforce process to identify, understand, and monitor all third-party relationships
- Address risk throughout the third-party relationship lifecycle
- Document organizational risk profile, risk tolerance, and risk acceptance
- Exercise due diligence to minimize risks (including regulatory fines and reputation damage)
- Treat Third-Party Risk Management holistically: Changes to sourcing models, program management, technology, regulations, and staff can all have a ripple effect.
- Be innovative and flexible: Program and processes should allow for incorporation of changes due to business, industry, and regulatory drivers.

Vendor Information Security Domain Scores

<table>
<thead>
<tr>
<th>Domain</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Assessment</td>
<td>2.2</td>
</tr>
<tr>
<td>Information Security Policy</td>
<td>3.3</td>
</tr>
<tr>
<td>Organization of Information Security</td>
<td>1.0</td>
</tr>
<tr>
<td>Asset Management</td>
<td>1.5</td>
</tr>
<tr>
<td>Human Resources Security</td>
<td>4.7</td>
</tr>
<tr>
<td>Physical &amp; Environmental Security</td>
<td>3.0</td>
</tr>
<tr>
<td>Communication and Operations Management</td>
<td>3.2</td>
</tr>
<tr>
<td>Access Control</td>
<td>2.7</td>
</tr>
<tr>
<td>Information Systems Acquisition, Development, and Maintenance</td>
<td>2.0</td>
</tr>
<tr>
<td>Information Systems Incident Management</td>
<td>1.0</td>
</tr>
<tr>
<td>Business Continuity</td>
<td>3.0</td>
</tr>
<tr>
<td>Compliance</td>
<td>2.0</td>
</tr>
</tbody>
</table>
THANK YOU FOR YOUR TIME AND ATTENTION
Wrap-Up

• Please join us for Part II of the webcast series on Thursday, February 25 at 1:00 pm EST

• Shortly after the webcast series concludes, the recording and slides will be sent to all webcast registrants and participants

• For further information on this topic, please contact:
  ▪ Dan Ramey - dan.ramey@rsmus.com
  ▪ Rick Shriner - rick.shriner@rsmus.com
  ▪ Tauseef Ghazi - tauseef.ghazi@rsmus.com