PwC Viewpoint on Third Party Risk Management

**Significant others:** How companies can effectively manage the risks of vendor relationships

November 2013
Are vendors more trouble than they’re worth? For companies, that’s a multibillion-dollar question. Data breaches at vendors and other third parties are costlier than in-house breaches, and the number of incidents is rising.

Data breaches at vendors and other third-parties continue to have a high profile in the news.

A customer service software provider recently suffered a data breach when hackers gained access to information stored on its system by three prominent social media sites. The hackers downloaded emails from users who had contacted the social media sites’ support departments. This and other recent hacks point to a larger problem with infrastructure cybersecurity.1

In today’s environment, it would be nearly impossible to find a company that doesn’t contract with a vendor. But the convenience and flexibility of outsourcing to third parties comes with significant risks, including the potential for regulatory penalties related to vendor incidents—penalties that have soared in recent years, costing institutions billions of dollars.

Preventing risk events at third party service providers has always been a challenge, but now the stakes are far higher. Over the past three years, the number of security incidents at companies attributed to partners and vendors has risen—increasing from 20% in 2010 to 28% in 2012 (see Figure 1).²

The most recent PwC Global State of Information Security Survey shed some light on the problem. Although 71% of companies expressed confidence that their security activities are effective, only 32% require third parties to comply with their policies.

1 Bank security weaknesses led to cyber looting of $45M from ATMs, CSO Online, March 10, 2013
3 PwC Analysis based on PwC 2013, 2012, and 2011 Global State of Information Security Surveys. (Not all factors shown. Totals do not add up to 100%.)
Customers are voting with their feet. Research shows that companies experience customer turnover following a security breach.

When reputations are tarnished after a security event, customers tend to bolt. They don’t really care whether the breach originates within the institution itself or within a vendor organization. Financial and reputational damage ensues regardless of the source. As customer attrition grows, revenue shrinks, and the pinch is felt at the bottom line.

Looking beyond just the significant financial penalties, institutions that suffer security breaches open the door to other serious consequences:
- The resulting reputational damage can nibble away at an institution’s customer base—and, eventually, take a bite out of its bottom line
- Additional consequences can include increased vulnerability to litigation, depressed market value and share price, and the possibility of regulatory enforcement actions

As shown in Figure 2, certain industries are more susceptible to customer churn, causing their data breach costs to be higher than the average.

Figure 2: Customer churn following a breach—by industry

1 Symantec and Ponemon Institute, “2013 Cost of Data Breach Study United States,” May 2013

Significant others: Managing the risks of vendor relationships
**Market drivers**

- Substantial reliance on third parties
- Vendor sourcing decisions that often overlook key risks
- Incomplete populations of vendors or vendors with sensitive data
- Inconsistent risk assessment and review practices across organizations
- Complexities in managing third party risk, such as:
  - Identifying what risks really matter
  - Selecting which third parties to review
  - Taking effective action when an issue is found

**Regulatory drivers**

- GLBA Gramm-Leach Bliley Act
- HITECH Act Health Information Technology for Economic and Clinical Health Act
- California Privacy Bill SB 1386
- PCI-DSS v2.0 Payment Card Industry Data Security Standard
- NRS 603A NV Data Security Law
- 201 Mass. Code Regs. 17 MA Data Security Law
- OCC 2013-29 Third Party Relationships
- Omnibus HIPAA Rule
- CFPB Bulletin 2012-03
- May '07 H.F. 1758 MN Plastic Card Security Act
- Aug '03 California Privacy Bill SB 1386
- May '02 OCC Bulletin 2002-16 (Foreign-Based Third-Party Service Providers)
- Nov '01 OCC Bulletin 2001-47 (Oversight and Management of Third-Party Relationships)
- July '01 GLBA Gramm-Leach Bliley Act
- 1996 HIPAA Health Insurance Portability and Accountability Act

Significant others: Managing the risks of vendor relationships
Adding to the challenge of effectively managing vendor-related risk, we see today’s companies also struggling with:

- Implementing formal enterprise-wide TPRM governance (Compliance and Enterprise risk management, etc.)
- Maintaining an accurate and complete inventory of vendors
- Incorporating other third party relationships into their TPRM programs (e.g., business partners, joint ventures, distribution channels, attorneys, utilities, etc.)
- Establishing standard operational risk methodologies and policies
- Identifying/using TPRM key risk indicators
- Implementing and using technology to adequately support the TPRM program, taking some of the burden from the business
- Staying ahead of, and effectively complying with, changing regulatory requirements

Our observations are underscored by the results of PwC’s Global State of Information Security Survey 2013:

- **69%** of the surveyed companies lack an accurate inventory of locations or jurisdictions where data is stored¹
- **74%** of companies do not have a complete inventory of all third parties that handle personal data of its employees and customers¹
- **73%** of companies lack incident response processes to report and manage breaches to third parties that handle data¹


Types of data that typically need to be protected:

- Intellectual Property (IP)
- Personally Identifiable Information (PII)
- Payment Card Industry (PCI)
- Protected Health Information (PHI)
Here are some of the comments our clients have shared with us regarding their TPRM challenges. With careful planning, each can be overcome.

We don't have a program to continuously evaluate and re-classify vendor based on assessment results.

I have operational staff focused on TPRM and they aren't risk and controls specialists.

We don't centrally manage our TPRM.

My vendors have vendors. How do we address the risks associated with those “Fourth party” vendors?

We have no pre-contract TPRM process in place.

We have inadequate resources to assess our high risk population on an ongoing basis.

We were told by our vendor that their SSAE16 is enough. Is that sufficient?
All too often, companies fail to adopt vendor stratification.

We observe many organizations applying the same level of risk analysis to all of their vendors, rather than identifying those vendor services deemed to carry the greatest risk and then prioritizing their focus accordingly.

The first step in the stratification process is to understand which vendors and services are in scope from an active risk management perspective. Once this subset of vendors has been identified and prioritized, due diligence assessments are performed for the vendors, depending on the level of internal versus vendor-owned controls. The results of these assessments help establish the appropriate monitoring and control requirements that should be maintained for each vendor.

This stratification approach focuses resources on the vendor relationships that matter most, limiting unnecessary work for lower-risk relationships.

Illustrative risk factors included in a vendor stratification program

Service risks:
- Volume of financial transactions processed
- Concentration associated with service
- Sensitivity risk of the data to which the vendor could potentially have access
- Compliance and regulatory risks related to the service
- Customer and financial impact

Vendor risks:
- Location of the vendor (subject to multinational laws, regulations, Safe Harbor, etc.)
- Previous data or security breaches
- Extent of outsourcing performed by the vendor
- Performance history

Vendor stratification prioritizes higher-risk services and vendors

1. Remove categories that don’t pose risk
2. Stratify third parties into risk categories
3. Prioritize high risk vendors for review

Level of due diligence and active risk monitoring

- Higher risk: on-site reviews
- Moderate risk: desktop reviews
- Lower risk: vendor self assessments

significant others: Managing the risks of vendor relationships
An effective and efficient TPRM program may provide benefits to various facets of the enterprise.

<table>
<thead>
<tr>
<th>Cost</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Reduced cost of managing vendor risk through stratification, process simplification, and use of technology</td>
<td>• Greater transparency into the costs of Third Party Risk Management</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Quality</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Higher quality Third Party Risk Management throughout the vendor lifecycle</td>
<td>• Tighter controls over vendors that pose significant risk</td>
</tr>
<tr>
<td>• Enhanced ability to quickly undertake new initiatives when opportunities arise—such as launching new services</td>
<td>• Consistent approach to assessing vendors and risks they present</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Standardization</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Improved quality, efficiency, timeliness and accuracy of TPRM stemming from automated workflows and reporting tools</td>
<td>• Streamlined and standardized processes for supplier on-boarding, risk profiling, and ongoing monitoring and oversight</td>
</tr>
<tr>
<td>• Greater benefits realized from scorecards and dashboards through use of standardized key performance indicators (KPIs) and key risk indicators (KRIs)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Risk</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• More effective monitoring of due diligence activities and their frequency, as now driven by both inherent and residual risks</td>
<td>• Greater agility in responding to changing regulatory requirements and other TPRM challenges as they arise</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Flexibility and efficiency</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Tighter focus on specific controls associated with those relationships found to pose the greatest risk, now made possible through vendor stratification</td>
<td>• Limited resources now able to be refocused based on identified organizational priorities</td>
</tr>
<tr>
<td>• Enhanced ability to quickly undertake new initiatives when opportunities arise—such as launching new services</td>
<td>• Ability to locate vendor replacements more rapidly as needed</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Shareholder value</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Improved compliance with Federal laws and regulations, thereby reducing or eliminating altogether any fines and penalties that could prohibit services and impact the bottom line</td>
<td>• Less intense scrutiny by the regulatory community</td>
</tr>
<tr>
<td>• Appropriately trained and placed resources</td>
<td></td>
</tr>
</tbody>
</table>
PwC offers a range of services with various entry points through the TPRM lifecycle, helping clients assess their current state programs and develop a roadmap for designing, building, and improving their current programs.

Program Diagnostic
Perform a high level assessment of the current TPRM function, identifying gaps against needs and leading practices.

Program Management Office
Outsource or co-source the TPRM program, including project planning, execution, and reporting.

Vendor Assessments
Using PwC’s global network of firms and service delivery centers, perform the following for specified vendors: on-site or remote reviews or development of self-assessments to be used by vendors.

Vendor Stratification
Perform a risk assessment and determine a risk score for all outsourced services and vendors. Help develop the client’s strategy to respond to that risk.

Technology Enablement
Integrate processes into new or existing technology platforms.

Function Build/Rebuild
Assist in building and implementing a new TPRM office, including the operating model, governance and structure, policies & procedures, processes and controls, and reporting framework.

Transformational Roadmap
Execute a comprehensive program review resulting in an end-state blueprint and roadmap to desired state, including anticipated level of effort and costs.
To have a deeper conversation, please contact:

<table>
<thead>
<tr>
<th>Name</th>
<th>Phone Number</th>
<th>Email Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shawn Panson</td>
<td>(973) 236-5677</td>
<td><a href="mailto:shawn.panson@us.pwc.com">shawn.panson@us.pwc.com</a></td>
</tr>
<tr>
<td>TR Kane</td>
<td>(216) 875-3038</td>
<td><a href="mailto:t.kane@us.pwc.com">t.kane@us.pwc.com</a></td>
</tr>
<tr>
<td>Dan Morrison</td>
<td>(415) 498-7066</td>
<td><a href="mailto:daniel.morrison@us.pwc.com">daniel.morrison@us.pwc.com</a></td>
</tr>
<tr>
<td>Garit Gemeinhardt</td>
<td>(704) 344-7757</td>
<td><a href="mailto:garit.gemeinhardt@us.pwc.com">garit.gemeinhardt@us.pwc.com</a></td>
</tr>
<tr>
<td>Nehal Sheth</td>
<td>(415) 498-7891</td>
<td><a href="mailto:nehal.sheth@us.pwc.com">nehal.sheth@us.pwc.com</a></td>
</tr>
<tr>
<td>Dean Spitzer</td>
<td>(917) 841-2976</td>
<td><a href="mailto:dean.v.spitzer@us.pwc.com">dean.v.spitzer@us.pwc.com</a></td>
</tr>
<tr>
<td>Rob Stouder</td>
<td>(317) 940-7501</td>
<td><a href="mailto:rob.stouder@us.pwc.com">rob.stouder@us.pwc.com</a></td>
</tr>
</tbody>
</table>