www.pwc.com

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]

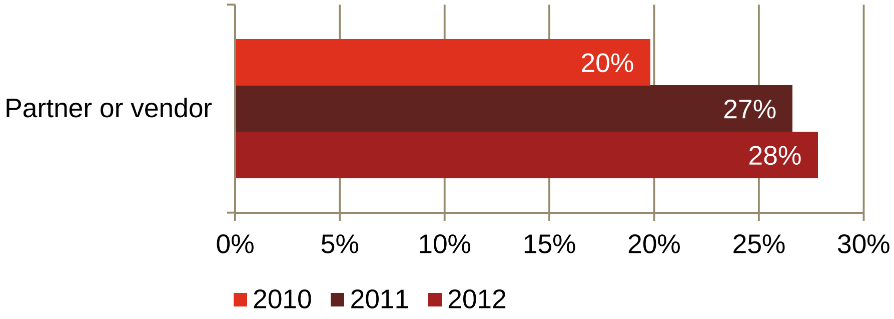
In today's environment, it would be nearly impossible to find a company that doesn't contract with a vendor. But the convenience and flexibility of outsourcing to third parties comes with significant risks, including the potential for regulatory penalties related to vendor incidents—penalties that have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

Over the past 36 months, the number of security incidents attributed to customers, partners, vendors, and other third parties has escalated.

Figure 1: Number of security incidents attributed to vendors[3]



[1] *Bank security weaknesses led to cyber looting of $45M from ATMs,* CSO Online , March 10, 2013

[2] PwC 2013 Global State of Information Security Survey.

[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.

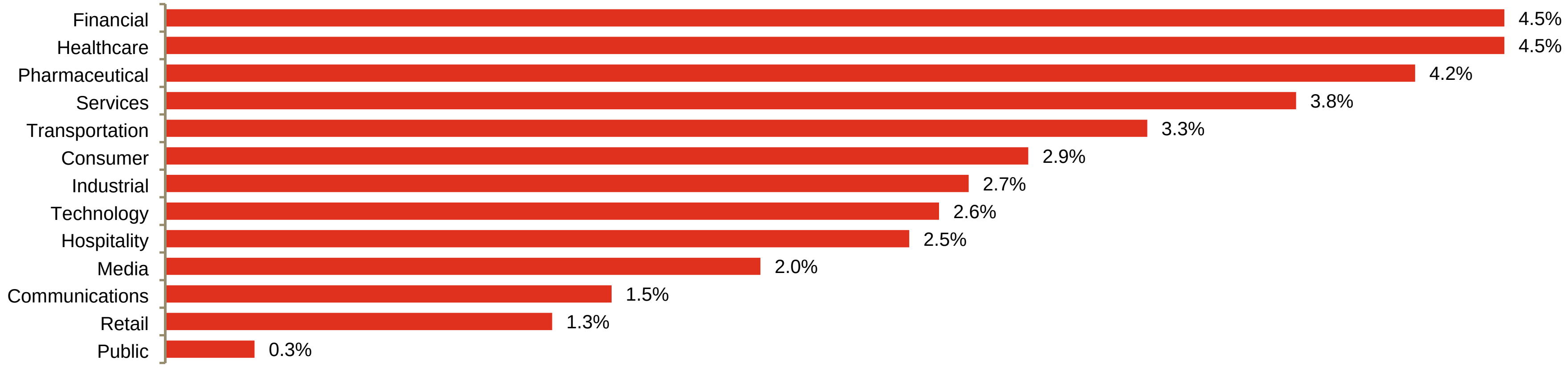
Looking beyond just the significant *financial* penalties, institutions that suffer security breaches open the door to other serious consequences:

- 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

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.

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]



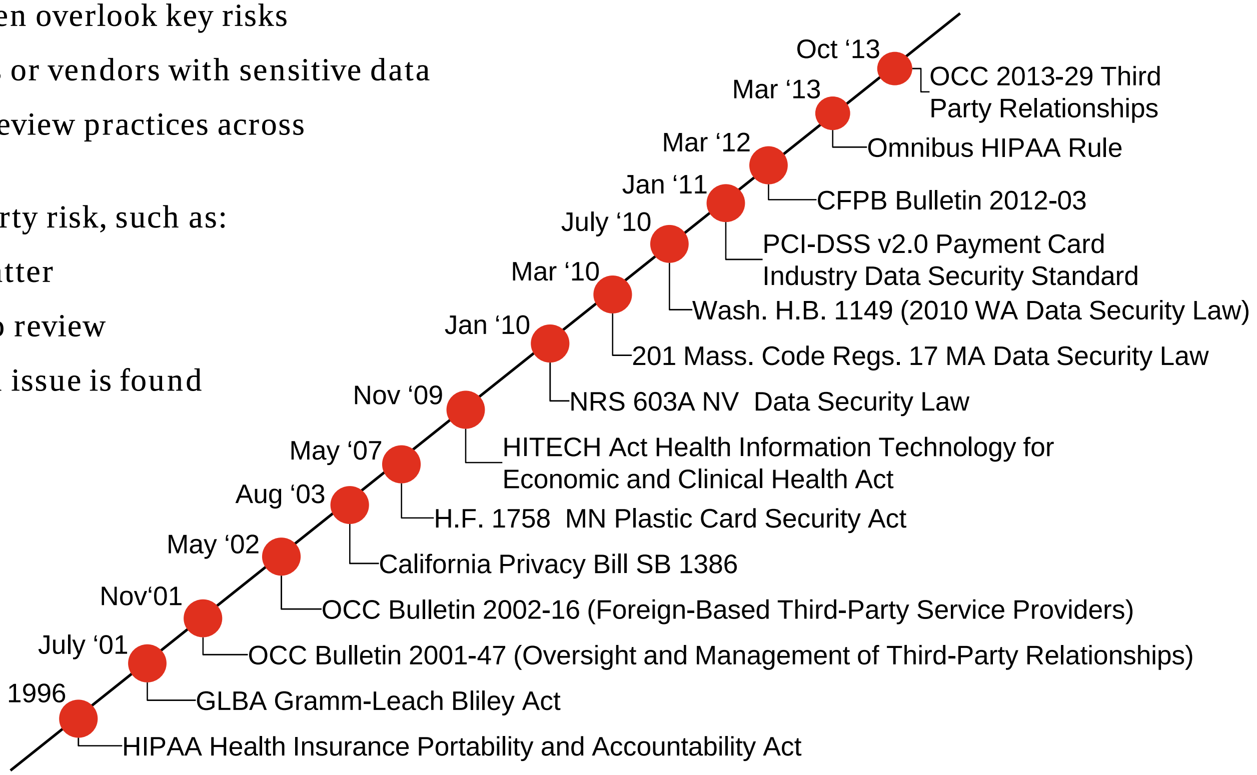
[1] Symantec and Ponemon Institute, "2013 Cost of Data Breach Study United States," May 2013

Drivers for Third Party Risk Management

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



1996 – HIPAA Health Insurance Portability and Accountability Act

July '01 – GLBA Gramm-Leach Bliley Act

Nov'01 – OCC Bulletin 2001-47 (Oversight and Management of Third-Party Relationships)

May '02 – OCC Bulletin 2002-16 (Foreign-Based Third-Party Service Providers)

Aug '03 – California Privacy Bill SB 1386

May '07 – H.F. 1758 MN Plastic Card Security Act

Nov '09 – HITECH Act Health Information Technology for Economic and Clinical Health Act

Jan '10 – NRS 603A NV Data Security Law

Mar '10 – 201 Mass. Code Regs. 17 MA Data Security Law

July '10 – Wash. H.B. 1149 (2010 WA Data Security Law)

Jan '11 – PCI-DSS v2.0 Payment Card Industry Data Security Standard

Mar '12 – CFPB Bulletin 2012-03

Mar '13 – Omnibus HIPAA Rule

Oct '13 – OCC 2013-29 Third Party Relationships

Although the industry is making strides to strengthen TPRM, we have observed that most organizations have not yet adopted stratification—a leading practice in managing vendor risk.

Types of data that typically need to be protected:

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

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 stored[1]
- ***74%*** of companies do not have a complete inventory of all third parties that handle personal data of its employees and customers[1]
- ***73%*** of companies lack incident response processes to report and manage breaches to third parties that handle data[1]

[1] PwC 2013 Global State of Information Security Survey.

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 vendors based on assessment results.

We have no pre-contract TPRM process in place.

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

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

We don't centrally manage our TPRM.

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

We were told by our vendor that their SSAE16 is enough. Is that sufficient?

Program execution

Vendor stratification

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

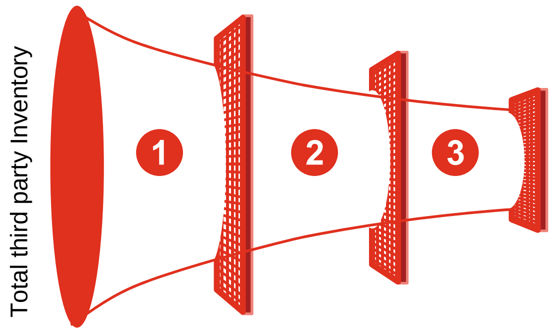
Service risks:

- 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

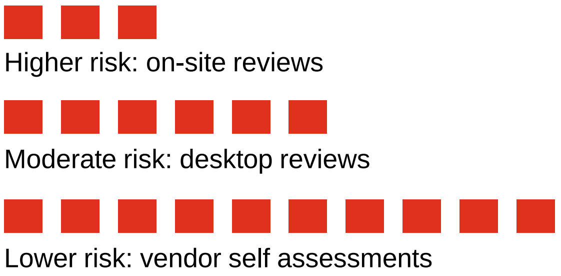


1 Remove categories that don’t pose risk

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

An effective and efficient TPRM program may provide benefits to various facets of the enterprise.

Cost

- Reduced cost of managing vendor risk through stratification, process simplification, and use of technology
- Greater transparency into the costs of Third Party Risk Management

Quality

- Higher quality Third Party Risk Management throughout the vendor lifecycle
- Tighter controls over vendors that pose significant risk
- Consistent approach to assessing vendors and risks they present

Standardization

- Improved quality, efficiency, timeliness and accuracy of TPRM stemming from automated workflows and reporting tools
- Streamlined and standardized processes for supplier on-boarding, risk profiling, and ongoing monitoring and oversight
- Greater benefits realized from scorecards and dashboards through use of standardized key performance indicators (KPIs) and key risk indicators (KRIs)

Risk

- More effective monitoring of due diligence activities and their frequency, as now driven by both inherent and residual risks
- Greater agility in responding to changing regulatory requirements and other TPRM challenges as they arise

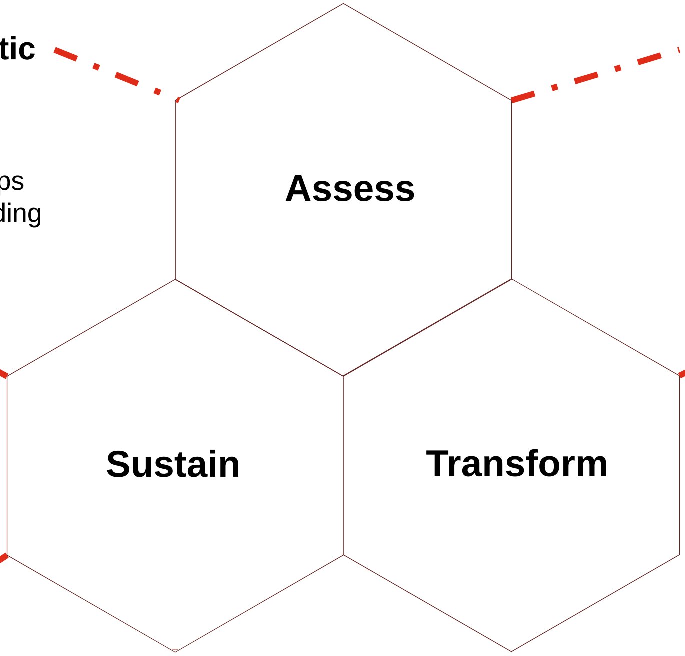
Flexibility and efficiency

- Tighter focus on specific controls associated with those relationships found to pose the greatest risk, now made possible through vendor stratification
- Limited resources now able to be refocused based on identified organizational priorities
- Enhanced ability to quickly undertake new initiatives when opportunities arise—such as launching new services
- Ability to locate vendor replacements more rapidly as needed

Shareholder value

- 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
- Less intense scrutiny by the regulatory community
- Appropriately trained and placed resources

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.

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.

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

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.

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.

Technology Enablement

Integrate processes into new or existing technology platforms.

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.

To have a deeper conversation, please contact:

Shawn Panson	(973) 236-5677 shawn.panson@us.pwc.com
TR Kane	(216) 875-3038 t.kane@us.pwc.com
Dan Morrison	(415) 498-7066 daniel.morrison@us.pwc.com
Garit Gemeinhardt	(704) 344-7757 garit.gemeinhardt@us.pwc.com
Nehal Sheth	(415) 498-7891 nehal.sheth@us.pwc.com
Dean Spitzer	(917) 841-2976 dean.v.spitzer@us.pwc.com
Rob Stouder	(317) 940-7501 rob.stouder@us.pwc.com