www.pwc.com

PwC Health Industries Viewpoint on Third Party Risk Management

Significant others: How companies can effectively manage the risks of third party 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 resulting from vendors and other third-parties continue to make news:

In January 2013, an orthopedic clinic contracted with a third party vendor to transfer old x-ray films into electronic format. The x-ray films, including full names and date of birth of over 17,000 patients, were provided to the vendor, but the clinic never received the electronic version of the films and discovered they were the victims of a scam. The clinic has recommended that the patients remain vigilant by reviewing their account statements and monitoring their credit reports, as they have no way of knowing whether or how patient information may have actually been used.[1]

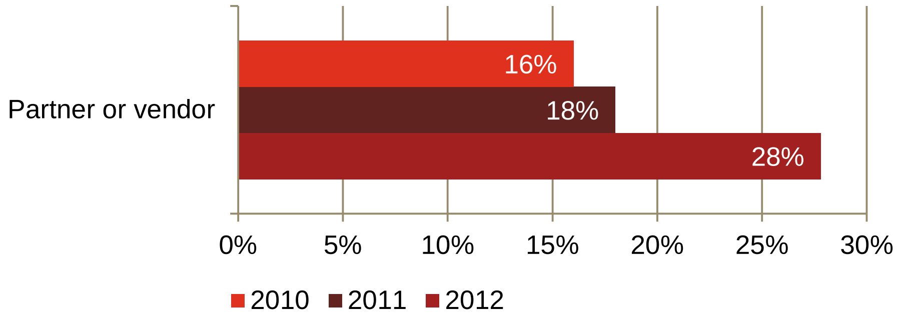
In today's environment, it would be nearly impossible to find a company that doesn't contract with multiple vendors and interact frequently with other third parties. But the convenience and flexibility of engaging third parties comes with significant risks, including the potential for regulatory penalties related to vendor incidents—penalties that have soared in recent years, costing companies 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 in the health industries attributed to partners and vendors has risen—increasing from 16% in 2010 to 26% in 2012 alone *(see Figure 1).*[2]

The most recent PwC Global State of Information Security Survey sheds some light on the problem. Although **68%** of companies in the health industries respondents expressed confidence that their security activities are effective, only **40%** 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] *Vendor Scam Results in Data Breach Involving 17k Patients,* Healthcare Informatics, 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 in the health industries experience higher-than-normal churn (customer turnover) following a security breach.

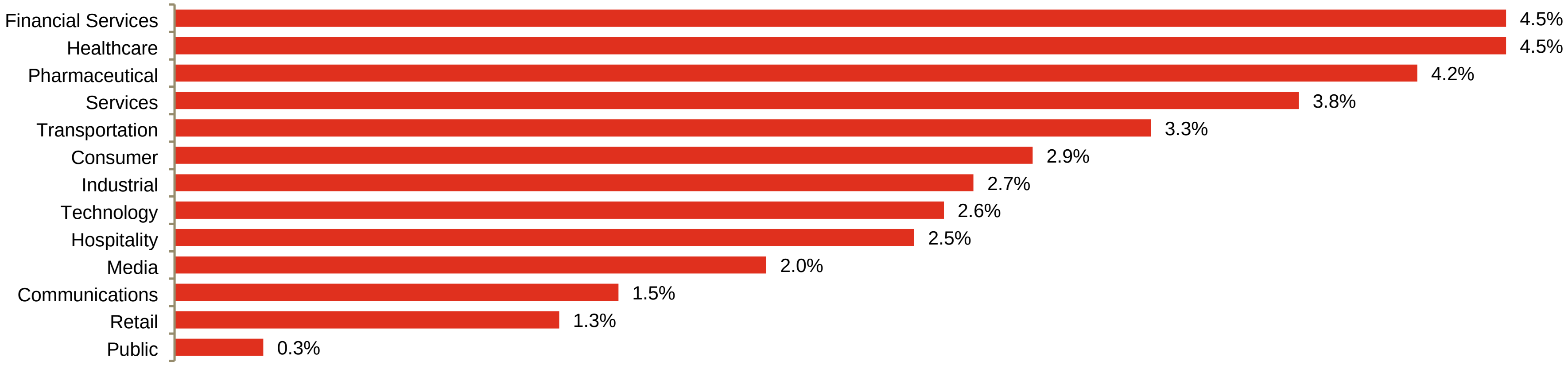
Looking beyond just the significant financial penalties, organizations that suffer security breaches open the door to other serious consequences:

- 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, Healthcare—with it's post-breach churn rate of 4.5 percent— is tied with Financial Services for highest turnover rate of the industries surveyed. This indicates that health industry companies are highly vulnerable to customer loss following a security breach.

Figure 2: Customer churn following a breach–by industry[1]



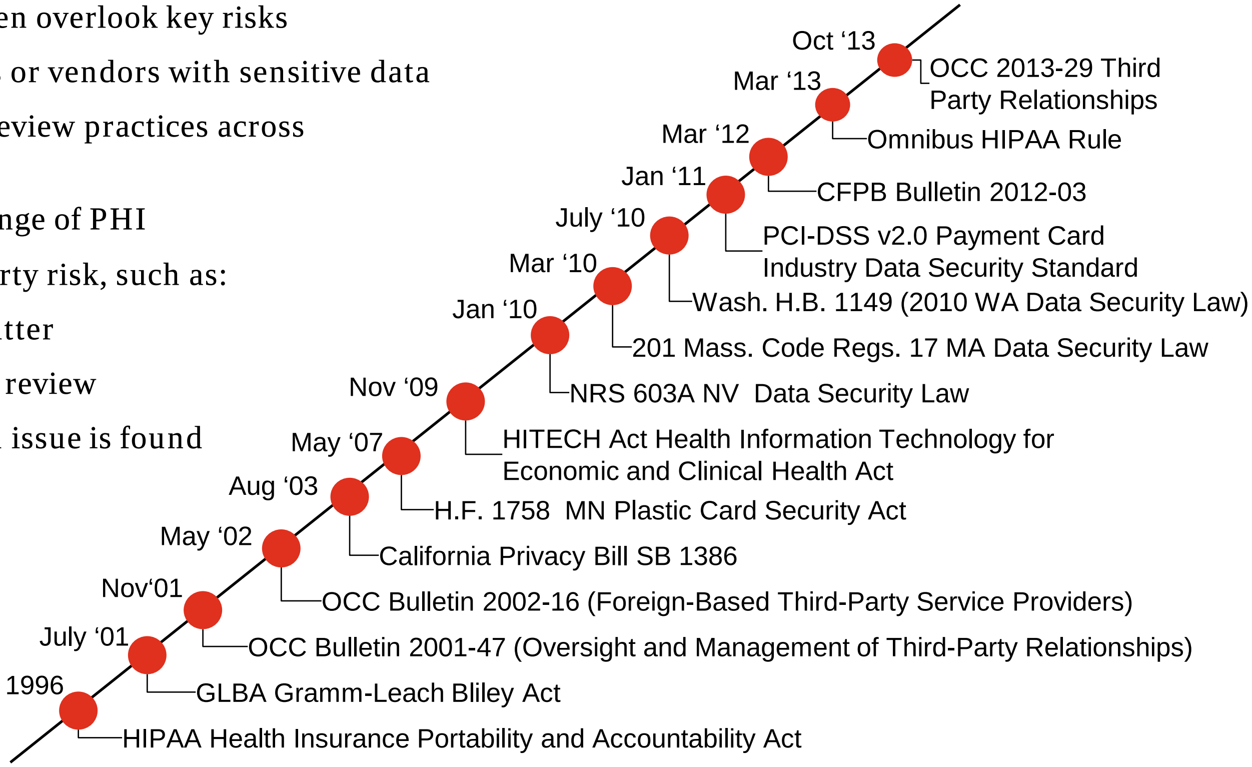
[1] Symantec and Ponemon Institute, "2013 Cost of Data Breach Study United States," May 2013

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
- Business model necessitates exchange of PHI
- 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



Oct '13 OCC 2013-29 Third Party Relationships

Mar '13 Omnibus HIPAA Rule

Mar '12 CFPB Bulletin 2012-03

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

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

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

Jan '10 NRS 603A NV Data Security Law

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

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

Following the release of the HIPAA "Final Rule" in January 2013, a cursory search finds references to "Business Associates" 1,358 times, evidencing a strong focus on vendor relationships.[1]

Companies in the health industries need to monitor their third party relationships for compliance with regulatory requirements, including

- **First Tier, Downstream, and Related Entities (FDR):** Payers must have a robust program in place to monitor their FDR relationships
- **Health Insurance Portability and Accountability Act (HIPAA):** Companies in the health industries can be held responsible for vendors' lack of adherence to HIPAA regulations related to Protected Health Information
- **Health Information Technology Act (HITECH):** Among other requirements, HITECH extended the liability of Covered Entities under HIPAA to their Service Providers
- **Food and Drug Administration (FDA):** Organizations regulated by the FDA are required to have strong vendor controls in place for a range of sectors including Drugs, Medical Devices, Food, Cosmetics and Tobacco Products
- **Stark Law:** Prohibits physician referrals of designated health services for Medicare and Medicaid patients if the physician has a financial relationship with that entity
- **Good x Practice(GxP):** A series of quality guidelines and regulations used in sectors such as pharmaceuticals, medical device, cosmetics and food. Manufacturers must establish and maintain procedures to ensure that all products conform to traceability and accountability requirements for all parties that contributed to the development and production of the products

[1] http://www.forbes.com/sites/danmunro/2013/05/01/hipaa-support-widens-in-cloud-vendor-community/

Although the industry is making strides to strengthen third party risk management (TPRM), we have observed that most organizations have not yet adopted stratification —a leading practice in managing third party 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 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 VRM 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, "subcontractor" vendors?

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

Program execution
Vendor stratification

All too often, companies in the health industries 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

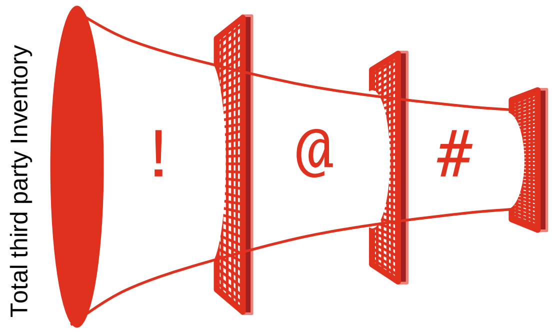
Service risks:

- 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



! Remove categories that don't pose risk

@ Stratify third parties into risk categories

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 third party 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 third parties that pose significant risk
- Consistent approach to assessing third parties 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

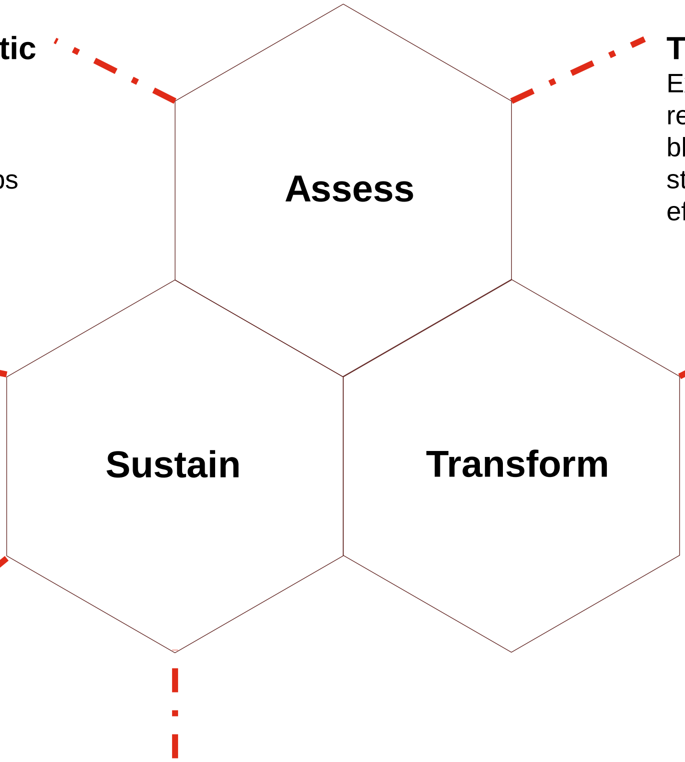
Flexibility and efficiency

- 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 road map 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.

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.

PwC Health Industries Practice

PwC's Health Industries Practice serves all segments of the healthcare industry, including providers, payers, entitlements, suppliers, and employers, helping them meet the challenges of today's changing environment. By understanding the needs and issues of each segment, as well as the complex interrelationships of these sectors, we are able to help our clients address issues and take advantage of opportunities.

We place a top priority on the continued growth of our healthcare industry practice. We invest heavily to develop the resources and services our clients need to prosper today and meet the challenges of the future. Along with audit, tax, and advisory services, we deliver a wide range of industry-focused services, including governance, risk and compliance, Medicare reimbursement consulting, medical management, actuarial consulting, network development, transaction consulting, and Digital Health. Our professionals include certified public accountants, tax professionals, physicians, nurses, information system professionals, management consultants, health policy analysts, actuaries, financial advisors, and data analysts. The Firm's professionals are recognized industry-wide for their innovation in analyzing, developing and implementing strategic options for clients.

PwC's Health Research Institute

Through PwC's Health Research Institute, we provide new intelligence, perspective and analysis on trends affecting health-related industries, including healthcare providers, pharmaceuticals, life sciences and payers. **PwC was the first of the Big Four firm to invest in a dedicated healthcare research unit.** The Institute helps executive decision-makers and stakeholders navigate chance through a process of research and collaborative exchange that draws on a network of more than 4,000 professionals with day-to-day experience in the health industries.

To have a deeper conversation, please contact:

Terry Puchley	(213) 356-6890 terry.puchley@us.pwc.com
TR Kane	(216) 875-3038 t.kane@us.pwc.com
Rob Stouder	(317) 940-7501 rob.stouder@us.pwc.com
Tiffany-Anne Gallagher	(973) 236-4646 tiffany-anne.gallagher@us.pwc.com
Dan Morrison	(415) 498-7066 daniel.morrison@us.pwc.com

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.