Imagine a business that doesn’t rely on any third parties. Would that mean:

No Vendors?
No Business Partners?
No Customers???
No Regulators?
No Suppliers?
SINCE THAT SCENARIO IS HARD TO IMAGINE….

- Do you have an accurate inventory of all third parties that you rely upon?
- Which third parties are critical to your business?
- Which third parties pose the highest risk?
- Which third parties have access to your data?
- What are you doing about it now?
• **Education**
  – University of Notre Dame: B.B.A. Management Information Systems
  – University of Denver: Masters of Business Administration

• **Certifications**
  – Certified Information Systems Security Professional (CISSP)
  – Certified in Risk and Information Systems Control (CRISC)
  – Certification in Risk Management Assurance (CRMA)

• **Experience**
  – 14 years as consultant in information security, risk management, IT strategy
  – All major industries, emphasis on Financial Services
  – Broad spectrum of Fortune 1000 clients, emphasis on Fortune 500
• **What is Third Party Risk Management ("TPRM")?**
  – Definitions
  – Concepts
  – General management approach

• **Who Cares?**
  – Your customers do
  – Your stakeholders do
  – Your regulators do

• **Third Party Risk Management ("TPRM") & Associated InfoSec Practices**
  – Good practices
  – Quick wins
  – Goals: value
  – Maturity
  – Best practices
  – Key questions

Please Ask Questions At Any Time!
WHAT IS A THIRD PARTY?

Fourth parties are sub contracted to third parties (i.e., third parties of third parties)

Which type of third parties are significant in your business model?
## FOR WHAT PURPOSE ARE THIRD PARTIES USED?

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Supply raw materials</td>
</tr>
<tr>
<td>2</td>
<td>Deliver materials and product</td>
</tr>
<tr>
<td>3</td>
<td>Reduce costs</td>
</tr>
<tr>
<td>4</td>
<td>Enhance performance</td>
</tr>
<tr>
<td>5</td>
<td>Obtain access to specific expertise, or make up for general resource constraints</td>
</tr>
<tr>
<td>6</td>
<td>Offer products / services directly to customers</td>
</tr>
<tr>
<td>7</td>
<td>Develop and offer additional products / services to customers</td>
</tr>
</tbody>
</table>
WHAT IS RISK?

IT Benefit/Value Enablement
- Technology enable for new business initiatives
- Technology enable for efficient operations

IT Program and Project Delivery
- Technology enable for new business initiatives
- Technology enable for efficient operations

IT Operation and Service Delivery
- Technology enable for new business initiatives
- Technology enable for efficient operations

Business Value
- Fail to Gain
- Gain

Lose
Preserve

Risk of loss is NOT the whole picture!

ISACA: RiskIT
WHAT IS RISK MANAGEMENT?

ISACA: RiskIT
WHAT IS RISK MANAGEMENT IN INFORMATION SECURITY?

As suggested by ISO 27001...

<table>
<thead>
<tr>
<th>ISO 27001 ISMS Process&lt;sup&gt;3&lt;/sup&gt;</th>
<th>Information Security Risk Management Process</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Plan</strong></td>
<td>• Establishing the context</td>
</tr>
<tr>
<td></td>
<td>• Risk assessment</td>
</tr>
<tr>
<td></td>
<td>• Developing risk treatment plan</td>
</tr>
<tr>
<td></td>
<td>• Risk acceptance</td>
</tr>
<tr>
<td><strong>Do</strong></td>
<td>• Implementation of risk treatment plan</td>
</tr>
<tr>
<td><strong>Check</strong></td>
<td>• Continual monitoring and reviewing of risks</td>
</tr>
<tr>
<td><strong>Act</strong></td>
<td>• Maintain and improve the Information Security Risk Management Process</td>
</tr>
</tbody>
</table>

<sup>3</sup> ISACA: RiskIT
SO THEN, THIRD PARTY RISK MANAGEMENT IS…?

**OPERATIONAL** Encompasses cost, efficiency, and contracting issues but also business disruption risk and misalignment of supply chains. In one recent survey, 73 percent of respondents had experienced at least one disruption in their supply chain during the previous 12 months.

**FINANCIAL** Takes into account foreign exchange, currency risk, tariffs, and taxes, as well as product price, markup, and rebates.

**TECHNOLOGY** Closely related to information risk but also includes the risks associated with new types of technology. The risk associated with smartphones, tablets, social media and cloud computing are still being defined, even as the next generation of technology is being developed.

**INTEGRITY** Concerns extend beyond fraud to include risk associated with regulatory compliance, conflicts of interest, brand, and reputation. An organization’s brand is tied closely to the collective acts of its suppliers or service providers, and today’s rapid flow of information can result in an almost instant reaction to adverse events.

**INFORMATION** Addresses the accuracy, timeliness, relevance, and security of data shared by multiple parties. As privacy rules around the world continue to expand in scope, the protection of information in the hands of third parties in an increasingly important concern.

**STRATEGIC** Includes the effect third-party relationships could have on the organization’s business models and market positioning as well as their even larger potential impact on society, the environment, and the economy.
OR, IS THIRD PARTY RISK MANAGEMENT THIS?

- Transparency
- Capability to manage suppliers
- Capability to manage business
- Alignment of sourcing strategy

- Stability and complexity of process design
- Description of inputs/outputs
- Alignment of process
- Efficiency and effectiveness of process

- Expectations versus contract
- Customer satisfaction rating
- Flexibility
- Stakeholder Buy-in

- Governance Risks

- Business Risks
- Financial Risks

- Process Risks

- Technology Risks

- Service Provider Risks

- Environmental Risks
  - Market pressures
  - Laws and legislation
  - Disaster

- Alignment of IT environments
- Audit ability of data
- Quality of data
- Technology refresh
- Complexity of IT environment

- Turnover key employees
- Subcontractors
- Knowledge and skills
- Absenteeism employees
- Country

- BPO Risk Model

- Business case
- Hidden costs
- Budgeted - actual volume
- Contracted - actual liabilities
- Contracted-actual exit costs
OR WAIT, IS THIRD PARTY RISK MANAGEMENT THIS?

**Performance Management**
Service levels – monitoring, Reporting
Schedule management, Issues in quality,
Offshore workload management,
Process flow for onsite/offshore delivery

**Resource Management**
Retention, Buffer, Training,
Vacation, Holidays,
On-boarding, Resource transitions,
Conserve knowledge transfer,
Skills update

**Financial Management**
Invoice review, Budget to actual,
Expense allocation, Invoicing procedure,
Change management to base model

**Relationship Management**
Client of choice initiatives, One team,
Track issues to closure, Bridge culture gaps

**Contract Management**
Key personnel, Staffing, Attrition,
Background checks, Insurance
DR/BCP plans, Readiness,
Reformulate service levels for relevancy
## WHO IS RESPONSIBLE FOR TPRM?

<table>
<thead>
<tr>
<th>Organizational Area</th>
<th>All Respondents n = 164</th>
<th>Financial Sector n = 47</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Business unit/functional leadership</strong></td>
<td>32%</td>
<td>40%</td>
</tr>
<tr>
<td><strong>Individual business unit or operational managers</strong></td>
<td>20%</td>
<td>9%</td>
</tr>
<tr>
<td><strong>Decentralized risk management in the business unit</strong></td>
<td>14%</td>
<td>17%</td>
</tr>
<tr>
<td><strong>Not clearly defined</strong></td>
<td>12%</td>
<td>4%</td>
</tr>
<tr>
<td><strong>Procurement</strong></td>
<td>7%</td>
<td>0%</td>
</tr>
<tr>
<td><strong>Centralized, enterprise-wide risk management</strong></td>
<td>6%</td>
<td>17%</td>
</tr>
<tr>
<td><strong>Others</strong></td>
<td>5%</td>
<td>9%</td>
</tr>
<tr>
<td><strong>Corporate Leadership</strong></td>
<td>4%</td>
<td>4%</td>
</tr>
<tr>
<td><strong>Don’t Know</strong></td>
<td>1%</td>
<td>0%</td>
</tr>
<tr>
<td><strong>Internal audit</strong></td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>
WHAT IS THE BUSINESS PROCESS VIEW OF TPRM (COMMON PROGRAM VIEW)?

Figure 8—COBIT 5 Implementation Life Cycle

Source: ISACA, COBIT 5, USA, 2012
WHAT IS THE BUSINESS PROCESS VIEW OF TPRM (EXAMPLE OF REGULATORY VIEW)?
WHAT IS THE BUSINESS PROCESS VIEW OF TPRM (RISK MANAGEMENT VIEW)?

Risk Centric View

1. Understand Inherent Risk Profile
2. Determine Residual Risks & Exposure
3. Stratify & Prioritize
4. Design & Implement
5. Monitor & Re-Assess

Relationship Centric View

1. Initiation of relationship / RFP
2. Risk Assessment
3. Due diligence
4. Contract
5. Monitoring & Oversight
6. Retirement

Risk Centric View

1. Understand Inherent Risk Profile
2. Determine Residual Risks & Exposure
3. Stratify & Prioritize
4. Design & Implement
5. Monitor & Re-Assess

Relationship Centric View

1. Initiation of relationship / RFP
2. Risk Assessment
3. Due diligence
4. Contract
5. Monitoring & Oversight
6. Retirement
HIGH RISK LIFE CYCLE STAGES

• **Major organizational or structural change**
  – Information security measures are not necessarily keeping up the pace with new technologies
  – Distracted employees can forget or discard security measures and protocols
• **Mergers and acquisitions**
  – New systems, policies, and procedures can create gaps in information security systems, measures and protocols
  – Headcount reductions may activate disgruntled ex-employees familiar with the organizations’ systems, processes and security measures
• **Entering new markets**
  – New markets mean new processes, vendors, buyers, systems, languages, etc., with varying levels of security risk
  – Unfamiliar governmental regulations on privacy, communications and data security complicate the security environment
• **Headline grabbers**
  – Hackers and cyber attackers use public relations disruptions to target companies whose attention is focused elsewhere
  – Reactive “emergency” actions designed to solve a short-term problem run the risk of actually creating openings and issues that can pose long-term risks

SO WHO CARES ABOUT TPRM?

Your customers do!
Customer churn following a breach – by industry

<table>
<thead>
<tr>
<th>Industry</th>
<th>Customer Churn</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial Services</td>
<td>4.5%</td>
</tr>
<tr>
<td>Healthcare</td>
<td>4.5%</td>
</tr>
<tr>
<td>Pharmaceutical</td>
<td>4.2%</td>
</tr>
<tr>
<td>Services</td>
<td>3.8%</td>
</tr>
<tr>
<td>Transportation</td>
<td>3.3%</td>
</tr>
<tr>
<td>Consumer</td>
<td>2.9%</td>
</tr>
<tr>
<td>Industrial</td>
<td>2.7%</td>
</tr>
<tr>
<td>Technology</td>
<td>2.6%</td>
</tr>
<tr>
<td>Hospitality</td>
<td>2.5%</td>
</tr>
<tr>
<td>Media</td>
<td>2.0%</td>
</tr>
<tr>
<td>Communications</td>
<td>1.5%</td>
</tr>
<tr>
<td>Retail</td>
<td>1.3%</td>
</tr>
<tr>
<td>Public</td>
<td>0.3%</td>
</tr>
</tbody>
</table>

PwC, Sep 2013: fs viewpoint
SO WHO CARES ABOUT TPRM?

Stakeholders do!

2012
- National Mortgage Settlement issued $25B in fines and actions against leading mortgage servicers, in part for missteps by their suppliers

2013
- Capital One pays $210M to settle charges of deceptive marketing practices by some third party suppliers

2013
- Discover Card settles similar charges for a similar amount

2013
- American Express settles a CFPB action for $112M

2013-2014
- Target Corp breach cost estimated $60M+ and growing
Regulators do! For example:

- Consumer Finance Protection Bureau (CFPB): holding financial institutions responsible not only for their own actions, but for those of their vendors and suppliers
- Federal Reserve
- Federal Deposit Insurance Corporation (FDIC)
- Health Information Technology for Economic and Clinical Health Act (HITECH)
- Office of Thrift Supervision – Third Party Arrangements (TB82a)
- Gramm-Leach-Bliley Act (GLBA)
- HIPAA
- FFIEC Guidelines
- State-specific Privacy laws
- Security Breach Disclosure Requirements (state specific)
- Model Audit Rule
- Red Flag Rules
- EU Data Protection Directive
- PATRIOT Act / Homeland Security
TYPES OF RISK ASSOCIATED WITH A BREACH


- Operational Risk
- Compliance Risk
- Reputation Risk
- Strategic Risk
- Credit/Financial Risk
- Cascading Risk
  - Market Loss
  - Recovery Continuation
  - Sustainability Questions

Third-Party Issues of greatest concern

- Monitoring third-party risk management practices
- Evaluating technology control to protect data
- Identifying or aggregating risks
- Gaining assurance on compliance with laws and regulations
- Determining protection of our intellectual property
- Obtaining internal audit coverage of key risk areas
- Collecting financial, performance, or other information
- Monitoring financial viability
- Evaluating quality of products

TPRM: GOOD PRACTICE SUGGESTS...

1. A comprehensive *inventory of all third parties* with whom the firm has a relationship. Many firms find it difficult to build this list; enterprise-wide surveys and data algorithms to reconcile data are effective tools that can help.

2. A comprehensive catalog of *specific customer risks* to which third parties can expose the firm. Many institutions don’t fully understand all the risks their third parties run. A master risk register, tied to important issues, can help track them down.

3. A *risk-based segmentation* of the supplier base. Not all suppliers carry the same amount of risk. Firms need to better triage their suppliers to make sure the most effort is devoted to the highest risks.

4. *Rules-based due diligence* testing. Treating every supplier the same doesn’t make sense. Carefully designed rules can help firms focus their investigation of suppliers.

5. A disciplined governance and escalation *framework*. At many firms, third-party risk management does not have a natural owner. Establishing one and giving that group the right decision-making powers is essential.

6. *Integrated technology* and MIS workflow process and tools. Adapting current risk IT applications to third-party management is tricky, and building a new one is even harder. A purpose-built off-the-shelf application is the right answer for many.

McKinsey, May 2013: Managing third-party risk in a changing regulatory environment
TPRM – INFORMATION SECURITY: GOOD PRACTICE SUGGESTS...

1. A comprehensive inventory of what data types and volumes third parties have access to. Corporate, consumer, or employee confidential information? Some records or all?

2. A comprehensive catalog of specific data based customer risks to which third parties can expose the firm. Loss or exposure of sensitive customer information, channels of transmission, integrity and security of information, etc.

3. A risk-based segmentation of third parties, based on data risks. Firms need to better triage their third parties’ Information Security practices to make sure the most effort is devoted to the highest risks.

4. Rules-based due diligence testing. Treating every supplier the same doesn’t make sense. Carefully designed rules can help firms focus their investigation on suppliers’ risks.

5. A disciplined governance and Information Security escalation framework. When an vendor has a security incident, who is responsible for doing what?

6. Integrated technology and MIS workflow process and tools. Organizing third parties’ relevant InfoSec information so that it’s referenceable is a challenge on its own. Integrating security monitoring tools to effectively monitor 100’s or 1000’s of data connections and report actionable information is critical to managing the overall third party environment.

McKinsey, May 2013: Managing third-party risk in a changing regulatory environment
TPRM – INFORMATION SECURITY: QUICK WINS

• **Rules Based Information Security and Data Privacy Screenings**
  – Use of surveys and questionnaires during due diligence and follow-up
  – Identification and gathering of control environment documentation prior to contract
  – Diligence commensurate with InfoSec risk profile

• **Service Organization Control (SOC) Reports, and similar attestation reports**
  – PCI Reports on Compliance (“ROC”), ISO 27001 Certification, Network penetration assessments, SysTrust, WebTrust, etc.

• **Standard action plan to work with third parties to mitigate identified risks**
  – Who communicates, what is communicated, what are the expectations?

• **Third Party Risk Management is a life cycle, not just a one time event**
  – How are changes to third parties’ risk / control environments identified?
  – After contract, how are risk levels and SLA’s monitored?
  – When a third party contract is terminated, then what?
## TPRM GOALS: VALUE

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
</table>
| **Cost** | • Reduced cost of managing third-party risk through stratification, process of simplification, and use of technology.  
             • Greater transparency into the cost of third party risk management.                                                    |
| **Quality** | • Higher quality of third-party risk management throughout the third-party life cycle.                                               
                • Tighter controls over third parties that pose significant risk.                                                             |
| **Standardization** | • Improved quality, efficiency, timeliness and accuracy of TPRM stemming from automated workflows and reporting tools.        
                          • Streamlined and standardized processes for third-party onboarding, 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 (KRI’s). |
| **Risk** | • More effective monitoring on due diligence activities and their frequency, as now monitoring is 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 greater risk, now made possible through third-party stratification.
- Ability to redirect the efforts of staff based on identified organizational priorities.
- Enhanced ability to quickly undertake new initiatives when opportunity arise, such as launching new services.
- Ability to locate third-party 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.
TPRM: INFORMATION SECURITY AS BUSINESS PARTNER

<table>
<thead>
<tr>
<th>Cost</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
</tr>
</tbody>
</table>

- **Goal**
- **Actual**
- **Business Unit Perception**
- **Information Security ROI within 3rd Party Risk Management**
TPRM MATURITY

- **Clerical**
  - Basic systems
  - Focus on purchase price and delivery
  - Risk addressed as they occur
  - Manual process, no data or reporting
  - Order / Invoice Issue Resolution
  - No focus on risk

- **Transactional**
  - Impact: Bottom line neutral

- **Proactive**
  - Impact: Risk avoidance, Sustainable cost savings
  - Integrated systems
  - Foundation for Supplier Mgmt
  - Emphasis on process and performance
  - Basic risk profiling and categorization

- **Strategic**
  - Impact: Exploit Risk, Margin contribution, Strategic differentiator
  - New Generation of Supply Management / SRM
  - Focus on value, innovation and margin
  - Enterprise wide 3rd party risk management

- **Level of Maturity / Value Add**
  - Initial / Ad-hoc
  - Repeatable
  - Defined
  - Managed / Optimized

- **Impact**
  - Overhead
  - Bottom line neutral
  - Sustainable cost savings
  - Strategic differentiator

- **Value**
  - Performance

- **Strategic**
  - Impact: Exploit Risk, Margin contribution, Strategic differentiator

- **Performance**
  - Impact: Risk avoidance, Sustainable cost savings

- **Value**
  - Impact: Exploit Risk, Margin contribution, Strategic differentiator

- **Strategic**
  - Impact: Exploit Risk, Margin contribution, Strategic differentiator
## Maturity of information security management processes in surveyed organizations

<table>
<thead>
<tr>
<th>Security Operations (antivirus, IDS, IPS, patching, encryption, etc.)</th>
<th>Very mature</th>
<th>Mature</th>
<th>Developed</th>
<th>Not yet developed</th>
<th>Nonexistent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Testing (web applications, penetration testing, etc.)</td>
<td>14%</td>
<td>46%</td>
<td>33%</td>
<td>7%</td>
<td></td>
</tr>
<tr>
<td>Security Awareness, Training and Communication</td>
<td>6%</td>
<td>24%</td>
<td>41%</td>
<td>26%</td>
<td>3%</td>
</tr>
<tr>
<td>Security Governance and Management (E.g., metrics and reporting, architecture, program management)</td>
<td>5%</td>
<td>23%</td>
<td>41%</td>
<td>26%</td>
<td>5%</td>
</tr>
</tbody>
</table>

Results shown on a scale of 5 to 1, where 5 is very mature and 1 is nonexistent

Which information security areas do you define as “top priorities” over the coming 12 months?

Survey respondents were asked to mark five items showing their top priority with a 1, down to their fifth priority with a 5.
### TPRM – INFORMATION SECURITY: BEST PRACTICES

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Optimize outsourcing as a capability enhancement rather than cost reduction</td>
</tr>
<tr>
<td>2</td>
<td>Develop or source a capability to understand developing and trending external market information security issues</td>
</tr>
<tr>
<td>3</td>
<td>Create flexible resource arrangements that allow for increased focus during periods of need throughout the information security service spectrum</td>
</tr>
<tr>
<td>4</td>
<td>Develop or source a capability to monitor Internet and social media channels related to contracted third parties, so that response can be proactive</td>
</tr>
</tbody>
</table>
TPRM IN GENERAL: KEY QUESTIONS

1. Does the organization have a full inventory of its third-party relationships and agreements?
   - Does the organization know clearly which third parties are HIGH or CRITICAL risk?
   - Does the org have an accurate inventory of locations or jurisdictions where data resides currently?

2. Has an assessment of the risks to the business or the brand for each of the relationships been performed?

3. Who owns the assessment of risks? Is the assessment linked to the organization’s ERM approach?

4. What are the primary relationship risks, and what processes are in place to manage them? Who is responsible for managing and monitoring these risks?

5. How do you know that your relationships are complying with the agreements in place?

6. How do you know your relationships are complying with various laws and regulations?

7. What are the organization’s policies related to auditing agreements for compliance?

8. Which significant relationship agreements or statements of work have not been reviewed by legal counsel in the last three to five years?

9. What procedures are followed to reassess the risks associated with a relationship prior to the renewal of a contract?

10. What types of risks are considered in the selection or renewal process? Are any significant risks not considered?

11. What types of monitoring are performed on third parties?

12. Do standard agreements address the most important risks of a majority of relationships?
TPRM – INFORMATION SECURITY: KEY QUESTIONS (1/2)

• **Data protection**
  – How will data be protected?
  – What controls does the vendor have in place for intrusion detection, perimeter security, physical security, timely application of security patches, and data leak prevention, among other safety measures?

• **Data access**
  – Who will have access to our data, and how can we confirm this?
  – Does the vendor have the right security controls to protect our data? How will the provider ensure that others (e.g., those whose data resides on the same server as ours) are not able to view our data?

• **Data security**
  – What policies and procedures are in place to detect, prevent and mitigate incidences of identity theft?
  – Have there been any instances of identity theft experienced by the third-party vendor within the last two years?
  – Does the vendor scan employee email and company social media platforms for potential breaches of customer data?
  – How are incidents and breaches reported?
  – Will we receive notification if a breach to our data occurs?
TPRM – INFORMATION SECURITY: KEY QUESTIONS (2/2)

• **Disaster recovery and business continuity planning**
  – Does the third party have a disaster recovery plan?
  – In the event of a disaster, how will the vendor protect our information assets?
  – Can we get our data back if the vendor goes out of business?

• **Contract and controls compliance verification**
  – Does the potential vendor allow third-party verification or provide such verification on its own?
An effective risk management process throughout the life cycle of the relationship includes:

- A comprehensive inventory of all third parties
  - “Tiering”
  - A disciplined governance and escalation framework
- Rules-based due diligence testing
- Written contracts that outline the rights and responsibilities of all parties
- Clear roles and responsibilities for overseeing and managing the relationship and risk management process
- Ongoing monitoring of the third party’s activities and performance
- Documentation and reporting that facilitates oversight, accountability, monitoring, and risk management
- Independent reviews that allow management to determine that the organization’s process aligns with its strategy and effectively manages risks
- Contingency plans for terminating the relationship in an effective manner
- **Shared value with the third party (win / win)**

CASE STUDIES

• **Several large, multinational credit card institutions** recently discovered that a group of hackers had successfully executed a multiyear campaign to steal prepaid debit card information from Indian- and US-based third-party. By the time they were arrested they had fraudulently withdrawn a total of $45 million from ATMs worldwide since 2012.

• **Nortel Networks Inc.**, an optical networking company, was compromised by Chinese hackers for nearly a decade, including computer systems and senior management’s emails (including the CEO’s). An employee had alerted Nortel’s executives that there was a breach in 2004, according to *The Wall Street Journal*, but outside of changing passwords, his warnings were largely ignored. This ongoing breach resulted in costly and complex litigation during Nortel’s asset sale after it declared bankruptcy in 2009. Companies that acquired Nortel’s intellectual property—Ciena Corp., Avaya Inc. and Ericsson Inc.—found out that their organizations might not have “exclusive rights” to the sensitive information.

• **Global Payments Inc.**, a payments processor, had been breached, exposing an estimated 1.5 million accounts. Just three years earlier, Heartland Payment Systems, another processor, was breached, impacting 130 million cards. The common factor among each of these incidents: They occurred at third-party entities, yet adversely affected the healthcare providers and financial institutions that relied on them for services. The hard lesson: Any organization can be victimized by a breach, even when the breach occurs outside its control. Responding to such an incident requires understanding, due diligence, risk mitigation and preparation.

• **Target Corp.**, a multinational retailer, had implemented a risk management framework for third parties, but may have simply failed to follow the defined processes. Approximately 110 million credit cards were compromised.

---

Key questions

An initial level of due diligence starts by asking management to ensure it understands if the vendors have the proper security controls in place to protect organizational data by, at a minimum, addressing the following key questions:

1. Who will have access to our data, and how can we confirm this?
2. Does the vendor have the proper security controls to protect our data?
3. How will the vendor ensure that its other clients (for example, other companies whose data resides on the same server) won’t have access to our information?
4. What subcontract or affiliation arrangements does the vendor have that involve our information? And what assurance is the vendor providing in this regard?
5. How will data be transmitted between the vendor and the organization, and for what part of the transmission process are the vendor and our organization responsible/at risk?
6. What control does the vendor have for intrusion detection, physical security, data leakage prevention, timely application of security patches and other safety measures?

“Third-party relationships and your confidential data.” Grant Thornton
7. Does the vendor allow third-party verification of controls compliance, or does it provide verification on its own?

8. Does the vendor have a disaster recovery plan, and if yes, when was it last tested? Can the vendor provide the latest results and any related remediation plans?

9. In the event of disaster, how will the vendor protect information assets?

10. Can we get our data back if the vendor goes out of business or when the contract ends, and how much will it cost to get it back?

11. What policies does the vendor have to detect, prevent and migrate incidents of identity theft?

12. Has the vendor had any incidents of identity theft within the past two years?

13. Does the vendor scan employee email and company social media platforms for potential breaches of customer data?

14. How are incidents and breaches reported?

“Third-party relationships and your confidential data.” Grant Thornton
<table>
<thead>
<tr>
<th></th>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>How quickly will we receive notification if breach of our data occurs?</td>
</tr>
<tr>
<td>16</td>
<td>How is the communication chain of command managed and monitored?</td>
</tr>
<tr>
<td>17</td>
<td>What are the plans for reviewing procedures and notifying of any issues identified?</td>
</tr>
<tr>
<td>18</td>
<td>Does the vendor conducted internal auditing of its controls and safeguards? How often are audits conducted, and will the vendor provide the latest reports and any related remediation plans?</td>
</tr>
<tr>
<td>19</td>
<td>Does the vendor engage an external auditor to perform review procedures and issue an application Service Organization Control (SOC) or Statement on Standards for Attestation Engagements (SSAE) No. 16 report?</td>
</tr>
</tbody>
</table>

"Third-party relationships and your confidential data." *Grant Thornton*