Managing 3rd Party Risks During a Crisis

“Are your business partners watching your back when you are watching your front?”

Danny Shaw
SE Practice Leader
IT Risk Advisory Services
Objectives:

Organizations frequently rely upon 3rd party service providers to deliver a wide variety of services and other activities.

The “What” is your responsibility

These arrangements may result in activities being outsourced in their entirety, but they do not relieve the ‘hiring’ organizations of the responsibility for managing the activities and identifying/controlling the risks associated with the relationships especially during an outage.

Learning Objective 1:
• Gain an understanding of the potential risks that may arise from the use of 3rd party service providers during a BCP exercise.

Learning Objective 2:
• Identify the basic elements of an effective 3rd party risk management program during an outage.
Why do we care ..... 
There’s a lot of $$$ involved!

• 95% of organizations buy or provide outsourcing services

• 75% of organizations spend upwards of 50% of their budgets on outsourcing
2011 Global Outsourcing Market for IT, BPO and call center services is $450B

– Who’s minding your assets?
U.S. Government spends $550 billion annually on outsourced products and services
CASE STUDY: Boeing 787 Dreamliner
A complex, integrated, interconnected environment

Supply chain issues + new technology + new approach = PROBLEMS

• Made of entirely new composite material

• 6,000 engineers

• 43 “top tier” suppliers on 3 continents

• 80% of production outsourced

• Exacting technological demands

• Overly ambitions production deadlines
The result?

- Plane delayed by 2+ years
- Upwards of $6 billion in lost profits
- Millions in contract penalties for late delivery
- Reputation took a “hit”

Without collaboration and measurement the 300 year old parable still applies:
of THE BLIND MEN AND THE ELEPHANT
Top 5 Reasons Organizations Outsource

- 75% Reduce and control operating costs
- 65% Focus on core competencies
- 59% Resources not available internally
- 52% Reduce internal headcount
- 51% Reallocate internal resources for higher value purposes
Top 5 Functions Outsourced

- 69% IT (all categories)
- 29% Operations and administration
- 26% Customer service
- 21% Other (wide variety)
- 20% Financial (payroll, etc.)
Third-Party Arrangements - WHY?

• Appropriately managed 3rd-party relationships can:
  – Enhance competitiveness,
  – Provide diversification and
  – Help organizations to attain key strategic objectives.
  – *FASCILITATE Business Continuity*
  – They can facilitate an increase in revenue or a reduction of costs.
  However, these business arrangements can also present risks to
the organization.

• The board of directors and senior management are ultimately
  responsible for
  – managing activities conducted through third-party relationships
  – as well as identifying and controlling the risks arising from such
    relationships.
Cloud Based Third-Party Arrangements

• Global cloud services revenue projected to reach
  - $149 billion by 2014 and
  - $241 billion by 2020.

• Information Security can either become a nightmare or an enabler for cloud adoption, with recent increases in highly publicized cloud security breaches.
Cloud Based Third-Party Statistics

• **$150 Billion:** *The size of the Cloud Computing Market by 2013.* (source – Gartner). Merrill Lynch’s research predicts the cloud computing market to be worth $160 B by the same year.

• **$750 Million:** *The Amount Amazon.com earnings in 2011.* Their offering, which started in 2006, hit revenue of around $500M in 2010.

• **7 of 10:** *Companies* using cloud services that will move new applications to the cloud.

• **54%:** of respondents citing Security as their top concern for transitioning to the cloud.

• **60%:** *Server workloads* that will be virtualized by 2014 in the cloud.
Potential risks arising from 3rd-party relationships

• 3rd party risk is not a simple, easily identifiable risk attribute, but rather a combination of risks ranging from the familiar to the highly complex.

• Such risks can vary greatly, depending upon the specific characteristics of each third-party arrangement.

• Risks Relationships are Associated as the following:
  – Strategic
  – Reputational
  – Operational
  – Transaction
  – Credit
  – Compliance
Strategic Risk

The risk arising from **adverse business decisions**, or the failure to implement appropriate business decisions in a manner that is consistent with the organization’s strategic goals.
Reputation Risk

The risk arising from **negative public opinion**.

- 3rd Party relationships that result in
  - dissatisfied customers,
  - inappropriate recommendations,
  - security breaches resulting in the disclosure of sensitive information and violations of laws and regulations are examples of situations that could create negative publicity and harm the reputation of the business.
Operational Risk

The risk of loss resulting from:

- inadequate or failed internal processes
- people, and systems, or from external events.

- 3rd Party relationships often integrate the process of other organizations with the internal processes of the business and can thereby increase the overall complexity of the operational environment.
Transaction Risk

The risk arising from problems with service or product delivery.

- A 3rd-party’s failure to perform as expected due to reasons such as inadequate capacity, technological failure, human error or fraud exposes the entity to transaction risk.

- Other forms of transaction risk include the lack of effective business continuity/disaster recovery plans and a weak IT internal control environment that threatens the integrity of systems and resources.
Credit Risk

The risk that a third party, or any other creditor necessary to the third-party relationship, is unable to meet the terms of the contractual relationship.

- **Solvency?** The basic form of credit risk involves the financial condition of the service provider itself.
- **Peak Demand?** A crisis can stress the abilities of your provider. Can they handle peak demands?
Compliance Risk

The risk arising from **violations of laws, rules or regulations**, or from noncompliance with internal policies, procedures or business standards.

- Compliance risk is exacerbated when the organization has inadequate oversight, monitoring or audit functions.

- Des your provided have an SSAE16 SOC1 or 2 that addresses BCP? “availability trust principle”
Risk Management Process

• The use of a 3\textsuperscript{rd} party service provider reduces management’s direct control over the activities at hand, but therefore increases the need for oversight of the activities from start to finish.

  – The key to the effective use of a 3\textsuperscript{rd} party in any capacity is for the organization to \textbf{appropriately assess}, measure, monitor and control the risks associated with the relationship.
Basic Elements of an Effective 3rd-Party Risk Management Program

- Risk assessment *(next page)*
- Due diligence in the selection of a service provider
- Contract structuring & review (including actionable SLAs)
- Oversight

While these elements apply to any 3rd party activity, the precise use of this framework is dependent upon the nature of the third-party relationship, the scope/magnitude of the activity, and the related risks that have been identified.
Risk Assessment Key Components

• Develop specific business requirements:
  • What do we need? – When do we need it? – How do we pay for it? – How will we know if we got what we paid for?

• Develop a thorough understanding of:
  • What the proposed relationship will accomplish and
  • Why the use of a 3rd party is in the organization’s best interest

• Analyze the benefits
  • costs, legal aspects & potential risks

• Perform a risk/reward analysis for significant matters,
  • Compare the proposed 3rd-party relationship to other methods of performing the activity: the use of other vendors, performing the activity in-house, etc.

• Identify performance criteria
  • internal controls, reporting needs and contractual requirements.
Due Diligence in Selecting a Third Party

- The scope and depth of the due diligence activity should be directly related to the significance and magnitude of the anticipated relationship with the third party.

- Not only should the due diligence be performed prior to selecting a 3rd party, but also periodically throughout the duration of the relationship.

- Comprehensive due diligence involves the review of all available information concerning a potential 3rd party,
  - focusing upon the entity’s financial condition,
  - its specific relevant experience, its reputation and
  - the scope/effectiveness of its operations & controls.
Due Diligence Review

- Audited financial statements
- Experience & capabilities in the proposed activity
- Business reputation
- Qualifications/experience of the company’s principals
- Existence of significant complaints, litigation or regulatory actions
- Use of other parties or subcontractors
- Scope of internal controls, systems & data security, audit coverage
- Business resumption strategy & contingency plans
- Adequacy of management information systems
- Insurance coverage
Contract Structuring & Review

• **Management expectations** should ensure that the specific obligations of both parties are outlined in a written contract prior to entering into the arrangement.

• **Board approval** should be obtained prior to entering into any significant third-party arrangements.

• **Legal counsel** should review significant contracts prior to finalization.

• **Contract should prohibit assignment, transfer or subcontracting of obligations to another entity.**
Content of the Contract

- Scope
- Cost/compensation
- Business reputation
- Performance standards
- Management information reports
- Right to audit
- Confidentiality & security
- Business resumption and contingency plans
- Default & termination
- Dispute resolution
- Indemnification
Oversight of 3rd-Party Activities

• Management should periodically review the 3rd party’s operations
  • Verify that they are consistent with the terms of the written agreement and that risks are being controlled.

• Management should consider designating a specific officer to:
  • coordinate the oversight activities with respect to significant relationships and, as necessary
  • involve other operational areas (audit, IT) in the monitoring process.

• An effective oversight program will generally include
  • the monitoring of the third party’s quality of service, risk management practices, applicable internal controls and reports
7 Steps to “Better” Third-Party Relationships

1. Conduct market research and “ask around”

2. Widely distribute your RFP/Bid/Tender

3. Have strong evaluation criteria and an experienced proposal review team

4. Google / Facebook “key personnel” offered

5. Perform due diligence on technical and financial capabilities to perform

6. Demand a demonstration

7. Meet the key executives
Did we meet our Objectives?

**Learning Objective 1:**
- Gain an understanding of the potential risks that may arise from the use of 3rd party service providers during a BCP exercise.

**Learning Objective 2:**
- Identify the basic elements of an effective 3rd party risk management program during an outage.
Thank You!

Any Questions?

Danny Shaw
SE Practice Leader, IT Risk Advisory Services
Experis
+1.404.586.2773 (o)
+1.678.910.4355 (m)
Danny.Shaw@experis.com