Third Party Risks

Mick Atteberry

Nebraska CERT Conference

August 2006

Disclaimer

Views expressed in this presentation are those of my own and do not reflect those of my employer.

Examples given in this presentation are not all inclusive and will be different for each organization. The examples are intended to demonstrate a thought process.

Objectives

- Develop an understanding of third party business risk.
- Establish a list of risk areas for prioritization.
- Establish methodology for assigning priorities.

Definition

Third Party Risk

The possibility of adverse impact from a dependent resource to a primary supplier or service provider.

Example: We, the first party, contract with a second party to provide a service. The second party is dependent on a third party in the provision of that service. A third party can affect the success of the second and first party or present downstream liabilities.

Issues List for Discussion

	Issue	Effect	Action
01			
02			
03			
04			
05			
06			
07			

Mind Set - Business

- Impact area: Every business is dependent on someone else.
- Background: Using examples from others will always support the issues you are presenting.
- Fact: A basic statement that is irrefutable to the issue.
- Effect: A negative effect on the organization that will require a mitigation plan.

Case Study 01: Electrical Power

- Impact area: Business Continuity - Shutdown
- Background: In July 2006, record high temperatures were reported across the United States resulting in peak demands for electricity.
- Fact: Some electrical providers announced and enforced rolling blackouts within their service areas.
- Effect: A corrugated box manufacturer reported the time required for structured production restart procedures to take two days for each blackout. The control of glue through pipes affects quality of the end product. Unexpected expenses take away from net income.

Case Study 01 - Utility Notes

- Every utility represents a third party risk scenario.
- We contract for their services, and in return they are dependent on a number of downstream third parties to provide that service.
  - Electricity
  - Water
  - Sewer
  - Telecommunications
- Third party risk management is a business issue that can affect business operations.

Case Study 02: Alaska Oil Pipeline

- Impact area: Operational Costs Increase
- Background: On August 7, 2006, British Petroleum announced they will shut down the Alaskan pipeline for an unknown period of time to fix a sixteen mile section of corroded pipe.
- Fact: The Alaskan pipeline carries 8% of total U. S. oil production, or 2% of total U. S. oil consumption.
- Effect: Supply decreases while demand remains the same. Cost of oil and oil products will increase during the shutdown as downstream refineries search and compete for additional oil resources to draw from.

Case Study 02 - Commodities

- Every provider of commodities represents a third party risk scenario.
- We contract for their services, and in return they are dependent on a number of downstream third parties to provide that service.
  - Fuel and oil
  - Basic process inputs
  - Paper
  - Office supplies
- Virtually nothing in a modern day enterprise is exempt from the third party risk management evaluation process.

Mind Set - Information

- Impact area: Interaction with dependent businesses require an exchange of information, some of which is protected by law.
- Background: The press and Internet have given us multiple examples of how information can be unintentionally lost or disclosed.
- Fact: Example, the Nebraska Privacy law quietly went into effect on July 13, 2006 affecting all citizens of Nebraska and those doing business with citizens of Nebraska.
- Effect: Improper handling of “private” data will result in negative consequences and unexpected expenses to the organization.

Case Study 03: Theft of Credit Card Data

- Impact area: Downstream Liability - Litigation
- Background: Multiple examples of credit card information loss disclosures in the past twenty four months.
  - (lost laptops, lost backup tapes, web sites hacked, fraud)
- Fact: Credit card issuers sue companies for the recovery of costs to issue new credit cards to individuals whose credit card information was compromised.
- Effect: Unexpected expenses take money and labor resources away from planned activities - reducing net income or budget.
  - $ x to cover costs for each new card issued
  - $ x to cover costs to prove liability of the first party
  - $unknown for individual credit monitoring costs

Case Study 03 – Credit Card Data

- Every provider of credit card services represents a third party risk scenario.
- We contract for their services, and in return they are dependent on a number of downstream third parties to provide that service.
  - Merchant license
  - Bank
  - Internet service providers
  - Telecommunications lines
  - Online stores
- Privacy laws in multiple states and countries require the protection of “private” data associated with an individual.

Case Study 04: Background Checks

- Impact area: Downstream Liability - Litigation
- Background: Choice Point announced that multiple parties accessed information on individuals through fraudulent means.
  - (these individuals used social engineering tactics)
- Fact: Choice Point collects information through methods they declare to produce high quality information on individuals.
- Effect: Decisions must be made from possible high quality derogatory information must be validated from a second source.

Case Study 04 – Background Checks

- Every provider of background services represents a third party risk scenario.

- We contract for their services, and in return they are dependent on a number of downstream third parties to provide that service.

  - Credit services
  - Court services
  - Internet content providers

- Privacy laws in states and countries require the protection of “private” data associated with an individual. Most foreign countries require “consent” before storing the data, the U.S. does not.

Case Study 05: Expense Reports

- Impact area: Downstream Liability – Litigation
- Scenario: Inadvertent loss of information associated with an expense report may result in identity theft of the individual submitting the report.
- Fact: Many expense reports require the name of the individual and the credit card number used for paying the expenses.
- Effect: (1) Identity theft will cause unexpected expenses to the individual, and possible costs to the company if the inadvertent loss is attributed to the company. (2) The credit card company may charge the attributed company for replacement costs and credit monitoring services for the individual.

Case Study 05 – Expense Reports

- Every organization processes expense reports for their employees.
- Follow the process flow, the real one. Where does that report really go – e-mail approvals – external payment services.
  - Private data
  - Credit cards or bank accounts
  - External processors for payment
- Privacy laws in states and countries require the protection of “private” data associated with an individual. Most foreign countries require “consent” before storing the data, the U.S. does not.

Case Study 06: U. S. V. A. Lost Laptop

- Impact area: Downstream Liability, Abnormal Expense
- Background: In May 2006, The United States Veterans Administration (VA) announced they lost a lap-top computer containing the identity information for 24 million veterans.
- Fact: The VA offers a $50,000 bounty for recovery of the lap-top. This value sets a new public threshold for the value of information.
- Effect: Unexpected expenses to budget take money and labor resources away from planned activities.
  - $15 million in investigative expenses
  - $50,000 bounty offered for recovery of lap-top
  - $unknown for individual credit monitoring costs

Case Study 06 – Hardware Thefts

- Every organization must be prepared for physical loss of equipment.
- The hardware is trivial today – the information is paramount. A process is required to profile the lost equipment for possibility of lost private data.
  - Prevent negative press scenarios from third party disclosure on findings.
- A police report is frequently required for lost or stolen equipment. But they do not ask about the contents of the device.

Case Study 07: Disposal of Equipment

- Impact area: Downstream Liability, Abnormal Expense
- Background: Most of today's machines contain from 0GB to 80GB+ of end user data in file format or cache format. The time to determine what the data is not warranted compared to the time required to run an overwrite utility against the machine.
- Fact: End users or applications will store a multitude of information on the local hard drive.
- Effect: Litigation, publicity, and investigative expenses take money and labor resources away from planned activities.
- Note: Watch dog groups will require large organization to have an environmentally friendly disposal process.

Case Study 07 – Disposal of Equipment

- Every organization must dispose of equipment with data eradication procedures and environmental cognizance.

- Almost every piece of hardware has local storage – the proper eradication of information is key to protect the perception of unintentional loss of information.

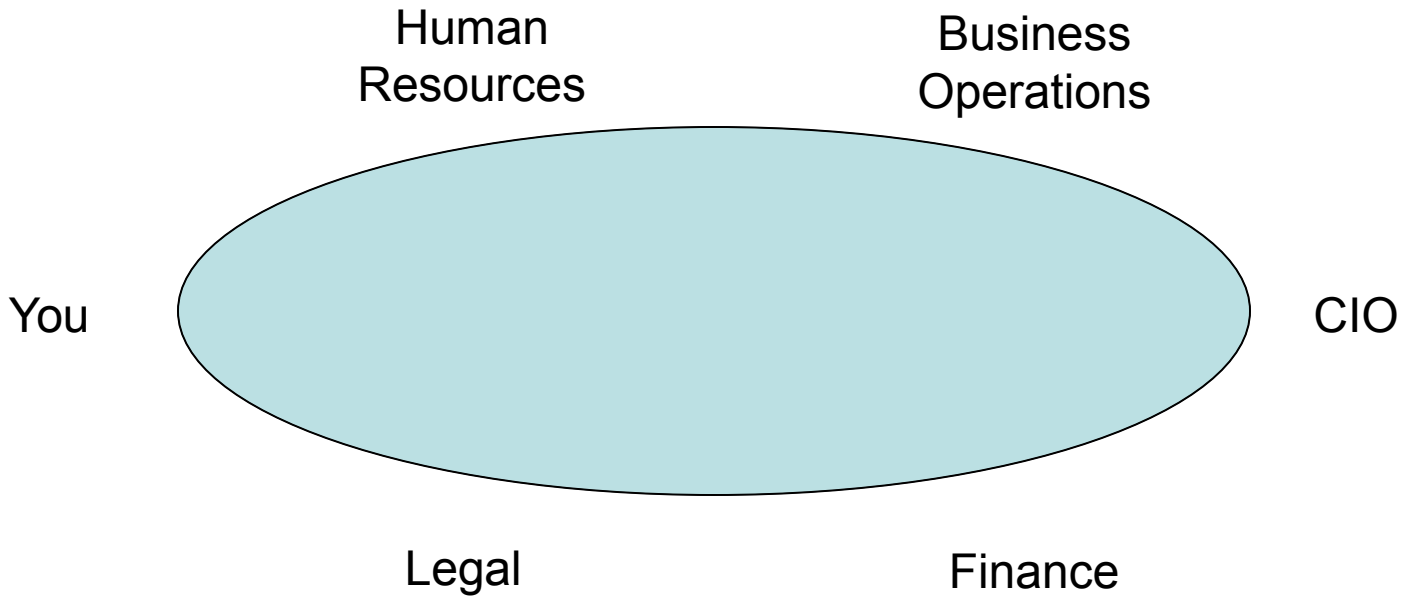
  - Prevent negative press scenarios from third party disclosure on findings.

- Most third party recycling firms will offer a procedure for data eradication at additional cost; while also being environmentally friendly with the disposal process. Documentation is a must for each asset.

Issues List for Discussion

	Issue	Effect	Action
01	Electrical Power - Rolling Blackouts	Downtime and recovery time are unexpected expenses that take away from revenue.	Recommendation for or against backup power supplies or generators, or both.
02	Alaska Oil Pipeline	Supply decreases while demand remains the same will result in higher prices.	Determine near term actions to absorb price increase or avoid consumption.
03	Loss or Theft of Credit Card Data	Unexpected expenses take money and labor resources away from planned activities - reducing net income or budget.	Review business process data flow for possible leakage or loss points.
04	Background Checks	Decisions made from possible high quality derogatory information must be validated from a second source.	Review business process with human resources to determine secondary validation process.
05	Expense Reports	The credit card company may charge the attributed company for replacement costs and credit monitoring services for the individual.	Review business process with finance to determine possible leakage or loss points.
06	Hardware Theft	Unexpected expenses to budget take money and labor resources away from planned activities.	Develop process to profile the lost machine for possible "private" information loss.
07	Disposal of Equipment	Litigation, publicity, and investigative expenses take money and labor resources away from planned activities.	Develop process to assure each machine is overwritten to prevent loss of "private" data.

Prioritization Meeting



Note: The issues list only starts the discussion. The meeting will take a life of it's own and the issues list will grow during the meeting. The objective is to have a top priority, an action item for resolution or mitigation, and a next meeting date.

Questions

Issues List for Discussion

	Issue	Effect	Action
01			
02			
03			
04			
05			
06			