Security and Risk considerations for outsourced IT Services

EA InfoSec Conference, 14/08/2013, version 1.0
Overview

- What is IT Outsourcing
- Why companies outsource IT
- Security and risk considerations
- Ensuring Information Security when Outsourcing
- Conclusion
What is Outsourcing?

IT outsourcing involves sub-contracting all or part of information technology functions to independent, third-party companies or individuals, instead of keeping those functions in-house.

- off-shoring
- home-shoring
- blended-shoring
### E.g’s of outsourced IT functions

- Application support
- Service desk / Support desk
- Datacenter services
- Backup and restore
- Incident management
- Anti virus / patch management
- IT security
- Printing
- MS Active Directory support
- Database / ERP support, etc
Why companies outsource IT

- Reduce operating costs
- Business focus
- Resources unavailable in-house
- Service improvement
- Reduce risk
Why companies outsource IT

Reduce operating costs

- Benefit from lower labour costs in countries like India. (Follow the sun). Processes outsourced to these locations are done at much lower rates and at the same quality levels as in the donor location. Eliminate the costs associated with hiring, training and retaining an employee, etc.

Business focus

- Focus on your core competencies. Redirect your organization’s internal resources toward mission-critical activities.
Resources not available in-house

- Get access to world-class capabilities and infrastructure. Have processes delivered by dedicated teams that have operational expertise in the outsourced process. Their experience in the field translates into greater operational efficiencies.

Service Improvement

- Can easily migrate to new technology with minimal downtime. Productivity and quality will be enhanced.
Reduce risk

- Protect your business from natural disaster. Get access to a service provider with adequate disaster recovery mechanisms.
- Reduce the risk of implementing a costly wrong decision.
Security & Risk Issues

- Strategic Risk
- Threat to information confidentiality
- Compliance Risk
- Logical Security
- Administrative risks
- Hidden costs
Security & Risk Issues

- **Strategic Risk**
  - Risk to the reputation of the business. Eg failure to resume operations for a financial institution could have serious repercussions
  - Not clearly defining the goals and objectives before starting to outsource

- **Threat to information confidentiality**
  - No control over company intellectual property

- **Compliance Risk**
  - Failure to abide by the customer’s contractual requirements resulting in penalties, e.g. transborder flow of data, etc
Security & Risk Issues

- Logical & physical Security
  - Unauthorized access to sensitive information, eg 3rd, 4th, 5th party
  - Datacenters – unauthorized access to business assets

- Administrative risks
  - Lack of or improper document control, eg. Runbooks used by service desk, use of outdated security policies, etc
  - Poor / lack of a change management system

- Hidden costs
  - Pay for any services out of scope
Security & Risk Issues

- Business Continuity
  - Continuity of services in case of a disaster - Service provider may not have an adequate BC plan
Ensuring Information Security when Outsourcing

- Having a good security policy
- Individuals dealing with sensitive information should sign confidentiality agreements.
- Selecting the right outsourcing vendor
- A sound privacy and intellectual property policy
- Protecting your data
- Providing Education on handling data
- The rule of least privilege
What the contract should include

Scope of Service

The contract should clearly describe the rights and responsibilities of the parties to the contract. Considerations should include:

- Clear scope of the contracted activities
- Clear Service Level Agreements (SLA’s)
- Exit Clause
- A penalty clause in the event of an incident
- Right to audit clause
- Security and confidentiality agreements
THANK YOU!