

Business Outsourcing to Asia: Security Challenges and Response

FIST CONFERENCE - BARCELONA

Presented By

Anup Narayanan, CISA, CISSP

anup@firstlegion.net

Agenda

- Domains of Outsourcing
- Security Concerns
- What International Customers demand ?
- The answers
 - Business Perspective on Security
 - Government Perspective on Security
 - Comparison on Global Scale
- Scope for Improvement

Domains of Outsourcing

Businesses that outsource to Asia

- Software Engineering
- Support Services
 - Call Centers
 - Back Office Processing
- Health Insurance
- Finance Services

- Increased international interactions
- Exchange of Intellectual Property
 - Source Code
 - Designs
- Exchange of personal information
 - Finance Data
 - Health Data
- Impact of International Laws (Information Security) on Indian Business,
- Opening of new channels of Information Exchange
 - Extreme Reliance on Internet

Security Concerns

The spheres of concern

- Protection of Intellectual Property
- Protection of Privacy
- Technical Threats
 - Related to Information Exchange
 - Related to communication channels
- Legal Aspects

Initial Roadblocks

- The advent of International Business initiated new work cultures.
- Most Asian countries did not have
 - Framework for Intellectual Property Protection
 - Privacy Protection
- Awareness of Privacy was and is not as advanced in Asian Countries.
- **What is the status today ?**

What American and European customers demand ?

Information Security – Customer Requirement

- Mature customers demand,
 - Detailed Information Security Framework
 - Management Understanding and Commitment to Information Security
 - Most of them stress on good Physical Security
 - Understanding of International Standards – SoX, GLBA, HIPAA Security Rule
 - Good Technical Infrastructure for Information Security – Encryption, Firewall and the works....

The answers

How Asian Companies have adopted Information Security ?

Overview of Information Security in Asia

- Asian companies (Especially India and Japan) have been on the forefront of ISMS implementation.
- For example
 - Japan is the largest adopter of BS7799 in the world.
 - India is at the 3rd largest adopter of BS7799 in the world.
- Apart from this many companies voluntarily adopt SoX, COBIT, HIPAA Security Rule etc.

Status of ISO 27001 (BS7799-2:2005)

- Most widely adopted ISMS in Asia, especially India
- Out of 2600 companies certified worldwide, approximately 2000 are in Asia.
- The scope is normally the critical business processes of the organization.
- More focus on,
 - Ownership and accountability of Information Security
 - Management commitment
 - Periodic review

What are the motivating factors ?

- Though the law does not demand it, compliance is often voluntary because,
 - Business survival often depends on security compliance
 - Management realizes the importance of the same.
- For example, Asian companies have,
 - Voluntarily complied to SoX and COBIT
 - Also, HIPAA Security Rule

Do we have incidents ?

- Yes we do,
- But the good factor is that there is maturity in resolution
- Companies are coming out and sharing incident reports with government and other companies
- Example -
 - A major outsourcing company in India with a major American Bank as it's customer had an incident. The company reported the same and their security levels were reviewed.
 - The level of security was reviewed and was found to be better than that of the customers'.

How the Government has approached Security ?

Government Initiatives

- Major initiatives have been through CERT.
- Initiation of Privacy Laws – Example Indian Privacy Act
- Apart from this many associations are active
 - ISACA
 - eISSA

Government and IT Laws

- Indian enacted the IT Act in 2000
- All police stations in India are centers for reporting Cyber Security Thefts
- Cyber Crime is slowly gaining recognition and there is regular training for Police on Cyber Security

Incident Handling and Reporting

- Govt. of India has a good framework
- CDAC – Center for Development of Advanced Computing, has released an open version of Forensic Analysis kit, which is recognized by the Government,
- This tool has been used for convicting Cyber Criminals.

A perspective on Business Continuity and Pandemic Flu

What was the reaction to Avian Influenza?

- Most Asian countries have a good Emergency Management framework for mitigating Pandemic Flu.
- For example in India
 - The NDRC (National Disaster Recovery Coordination) Committee coordinated with corporate companies to create recovery plans.
 - Businesses tested their DR plans through drills.
 - Industry meetings were arranged to discuss the possible impact of Pandemic Flu
- The positive – There was a common sharing of knowledge and best practices.

Comparison on Global Scale

Approach

- As far as ISMS goes, Asian companies are up there with the best or even leaders.
- On Technological Aspects of Security, may be we do not have the latest geek devices.
- There is immense improvements on
 - Management framework
 - Management commitment on regular investment in Information Security

The professional side

- Though my stats are not accurate, Asia, especially India is a leader in number of CISSP's, CISA's
- Security Professionals are amongst the best paid in India
- Some of the major security service providers (Nokia) have their Global Security Support services in India.
- There is a demand for Risk Management and Business Continuity Management Professionals.

The challenges

We share some of the global challenges

- The Human Aspect of Information Security
 - Social Engineering
 - Fraud
 - Theft
 - Corruption
- Environmental Factors – Tsunami, Floods etc.

Specific Challenges

- Too much focus on certification
- This puts stress on small businesses to adopt ISMS's and certify them – Not economically viable.
- Slow adoption of privacy laws.
- Compliance by users by fear and not real understanding.

Improvements ?

- A more holistic approach to Information Security.
- The aim of security should be achieving business goals and not just Confidentiality, Integrity And Availability.
- Too many companies (managers) adopt Information Security out of fear and not understanding it really.
- There is no clear understanding on how much to invest and what to expect in return.

Thank You

Anup Narayanan
Sr. Consultant and Founder

First Legion Consulting