Who is responsible for privacy ?
Companies or Individuals

Anish Shaikh

- **Privacy** can be defined an individual's ability to restrict or eliminate the collection, use and sale of confidential personal information.

- **Data Protection** as we know security of the Data, Personally identifiable, Sensitive or proprietary in nature.

India Inc. in news over PDP

- Data Leakage more prevalent in India, China, reveals Cisco
  - Loss of company data and other sensitive information due to breach in company rules by employees, is more likely to happen in enterprises in emerging countries like China, India and Brazil, revealed a Cisco study.
- BPO pulls out after data theft case
  - Hit by data theft, Acme Tele Power Limited, a top business process outsourcing (BPO), has decided to shut its operations in India and annul a $10-million investment earmarked for research and development.

The need for Privacy and Data Protection

- Rapid Advances in technology raising privacy concerns
- Easy to get details on somebody
- Information sharing between parties*
  - Banks sharing with Banks / Agents (Tracking defaulters)
  - Cellular companies selling your details

Impact of Data Privacy

- Brand Name
- Privacy will make you change how you handle Data
- Regulatory, Legal, National and International requirements
  - Meet global requirements, Data Export law, Data Transfer law.
- Financial impact
  - Software's, Encryption Tools, Implementation costs.
- Consequences of PDP failure
  - Loss of projects, Loss of revenue, civil and criminal impacts

---

Breach of Data Protection Principles

- Authority to collect, lawfully, fairly and legitimate purpose*
  - Cellular company executives adding you credit card information in system when you make an offline payment
  - Chain of Medical Store, Buy a anything and they add it in their database.
- Excessive collection of data should be governed.*
  - Google collects data from everywhere they can, they profile you very well.
- Data collected should be disposed properly when not required or when purpose accomplished, retention period should be taken into consideration.*
  - Data mishandled by Stock Broker. Including person contact and investment amount of Portfolio management services clients.
- Proper safe guards should be in place to avoid disclosure of a person / organisation*
  - System admin mistakenly gives access to secret server to everyone.
  - Contractor email still in Company Distribution list.
  - Income Tax India Website, Password Reset Flaw.
- Stop the misuse of PII.
  - IT Employee misusing inventory software to look up files on clients network.

Action items for Service Providers

‣ Get a Plan and implement it
‣ Think Privacy at the design level while creating the architecture an application or a network.
‣ Integration with the Enterprise Policy and SOW
‣ Monitor incidents. Top-down Approach
‣ Data Classification
‣ If anybody wants any details about himself, he should be provided with it. Banks, Agencies, etc.
‣ Use of Data Masking while giving access to Contractors

privacy
policy

Questions ?

Anish Shaikh