India

Building a New Ecosystem for Cyber Security & Data Protection

Vinayak Godse
Sr. Manager- Security Practices, DSCI

3rd International Conference
ICEB 2010

4th – 5th Jan 2010

DSCI
PROMOTING DATA PROTECTION

A NASSCOM® Initiative
Indian Economy: becoming e-economy

Continuing story of growth
Increased thrust on e-Governance
  About $10 billion investment
  Mission mode projects- Income Tax, MCA21, Passport, UIDA etc
  Government@ 24 x 7

E-Commerce growth- 30%
  Travel, downloads & e-tailing
  Becoming an important driver of Internet

Mobile
  More than 490 million subscribers
  Cross 1 billion by 2014

Internet Penetration
  Low at 7.1%, will be 3rd by 2013 (Forrester)

Internet is replacing other channels to execute banking transaction
About 100,000 railway e-Tickets by IRCTC
Retail epayment likely to grow by 70%,
  $180 billion by 2010
E-transaction currently account for 37% total transactions. However, total 75% payment value in electronic
Card circulation (credit & debit) will hit 210 million by 2010
Mobile banking transaction allowed, and expected grow faster
Outsourcing industry-
  $225 billion by 2020 from current $50 billion

Cyber security and data protection is critically important for securing growth of Indian economy
E-economy: Rising concerns of end users

Transformation from Joint to Nuclear family structure
Fast climbing individualism ladder
New emerging segment: 25-35 years
Increasing usage of Internet services
Emergence of personalize services
Improved understanding about security and privacy in cyber space

Annoyance over telemarketing calls & messages
Increased awareness of personal information being collected
Rising concerns over computer & internet security
Media coverage of national & international data breaches
Increased exposure of IT/ITES industry to global data protection regulations
An ecosystem for cyber security and data protection

**Legal Framework**
- Competent legal model for security and privacy?
- Current legislative ecosystem understand new age complexities?
- Special legislation for governing Information Technology?
- Benchmark or conform with international practices

**Government Initiatives**
- Government proactive in policy enablement?
- Investment and attention to increasing challenges?
- Programs, initiatives and partnership with industry, academia and other stakeholders?

**Important Projects**
- Flagship projects that affect cyber space and privacy?
- Their status and likely benefits?

**Industry Initiative**
- Industry is participation and collaboration?
- Special purpose mechanisms established?

**Law Enforcement**
- Law enforcement effective enough?
- Initiatives for the improvement?
India- Data Protection & Privacy Legal Model

A Spiral of Myths

- No supportive legislation
- No special legislation
- No Constitutional guarantees
- No data protection & privacy legal model

Data Protection & Privacy Model

Fundamental Rights (Art.21)
- Supportive Legislation(s)
  - The Indian Penal Code, 1860
  - The Indian Telegraph Act, 1885
  - The Indian Contract Act, 1872
  - The Specific Relief Act, 1963
  - The Public Financial Institutions Act, 1983
  - The Consumer Protection Act, 1986
  - Credit Information Companies (Regulation) Act, 2005

Special Legislation(s)
- The Information Technology Act, 2000
- The Information Technology (Amendment) Act, 2008

International Conventions
- International Covenant on Civil and Political Rights, 1966
- Universal Declaration of Human Rights, 1948

Ref: Vakul Sharma, Advocate, Supreme Court

A NASSCOM® Initiative
IT (Amendment) Act, 2008


- **Intermediaries:** Chapter XII on network service providers has been renamed as “Intermediaries not to be liable in certain cases”

- **Data protection new section 43A; existing section 43 strengthened source code**

- **Penalty for breach of confidentiality and privacy:** new section 72A

- **Cyber crimes:** new sections for 66A to 66F; 67A to 67C – unauthorized access, offensive messages, identity theft, impersonation, violation of privacy, and cyberterrorism; transmitting obscene material, child pornography

- **Interception and blocking:** 69A and 69B

- **Retention and preservation of traffic data and information by intermediaries,** and other computer resources— 67C, 69B

- **Critical information infrastructure protection** – sections 70A and 70B on a nodal agency, and for CERT-In to respond to incidents including notifying breach of incidents

- **Electronic contract formation:** Section 10A provides for validity of contracts formed through electronic means.

- **Encryption:** Section 84 A enables the central government to prescribe the modes or methods of encryption for secure use of the electronic medium and for promotion of e-governance and e-commerce
New Section 43A: Data protection has now been made more explicit through insertion of a new clause 43A that provides for “compensation to an aggrieved person” whose personal data including sensitive personal data may be compromised by a company, during the time it was under processing with the company, for failure to protect such data whether because of negligence in implementing or maintaining reasonable security practices.

Section 72 A: Penalty for breach of confidentiality and privacy: - punishment for disclosure of information in breach of a lawful contract is prescribed.

 Explicit new clause 43 A – for Data Protection-

“Compensation to an aggrieved person” whose personal data including “sensitive personal data” may be compromised because of “negligence in implementing or maintaining reasonable security practices”

72 A- “Punishment for disclosure” of information in breach of a lawful contract

“Disclosure without the consent“ of the subject person “will constitute a breach”
IT (Amendment) Act, 2008

IT Act and amendments include provisions on digital signatures, e-governance, e-commerce, data protection, cyber offences, critical information infrastructure, interception, cyber terrorism...etc.

‘Avoiding legal Multiplications’

....45 U.S. Federal enactments
....About 598 U.S. State enactments
....16 UK enactments
Government Initiatives

CERT-In
Department of IT

- Legal entity, nodal agency for incident response
- Policy enablement and regulations
- Threat monitoring, response planning, incident tracking
- Critical infrastructure protection
- Guidelines, standards, testing, security drills and certification
- Awareness: outreach & awareness, survey, security portal, training
- Collaboration: work with industry, international CERTs, network of security & privacy professionals, and academia

Important Projects

- UIDAI- primarily for economic benefits, will contribute to securing transactions
- NATGRID- Intelligence grid, transaction monitoring
- CCTNS- Networking all police stations in the country

Cyber Labs

- DFS- Director of Forensic Science, under Ministry of Home Affairs
- CFSLs- 3 Central Forensic Labs
- GEsQD- 3 Examiner of questioned document laboratories
- SFSLs- 28 State Forensic Labs

A NASSCOM® Initiative
Industry Initiatives

IT Industry

IT Services Industry
- Securing client data
- Providing security solutions

Presence of all major security vendors
Preferred destination of security research
Niche security players

Contributing of growth of security profession
No dearth of security skills

Industry Initiative

NASSCOM 4 E Framework

Setting up Data Security Council of India

Cyber Labs: NASSCOM DSCI initiative for training of law enforcement
National Skills Registry

A NASSCOM® Initiative
## Data Security Council of India

**DSCI - Data Security & Privacy Protection**

Set up by NASSCOM as a non-profit company

<table>
<thead>
<tr>
<th>Outsourcing</th>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low-cost resources</td>
<td>Consistent data security</td>
</tr>
<tr>
<td>Quality &amp; diversity</td>
<td>Security at Affordable cost</td>
</tr>
<tr>
<td>Scale up &amp; expanding</td>
<td>Privacy for customer confidence</td>
</tr>
</tbody>
</table>

- Establishment of rules & standards
- Promote ethics, quality and best practices

<table>
<thead>
<tr>
<th>Self-Regulation:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adoption of best global practices</td>
</tr>
<tr>
<td>Independent Oversight:</td>
</tr>
<tr>
<td>Focused Mission:</td>
</tr>
<tr>
<td>Enforcement Mechanism:</td>
</tr>
</tbody>
</table>

- “Connected Endeavour” -
  - Industry + Government + clients + international bodies + knowledge sources

- “Continuous Engaged” for the cause of data protection

- Building “Ecosystem for enhanced security and privacy” culture

- Proactive role for “policy enablement” that affect ICT

- “Collaborate” with multi-stakeholders and interest groups at national and international forums

- Approaches, “Frameworks and Practices” to align security and privacy practices to recent trends

- “Repository of knowledge” and content for benefit of industry

---

**Data Security Council of India**

- Low-cost resources
- Quality & diversity
- Scale up & expanding
- Consistent data security
- Security at Affordable cost
- Privacy for customer confidence
- Establishment of rules & standards
- Promote ethics, quality and best practices

- Self-Regulation:
  - Adoption of best global practices
  - Independent Oversight:
  - Focused Mission:
  - Enforcement Mechanism:

---

**A NASSCOM® Initiative**
DSCI- Data Protection Practices

DSCI Security Framework
- DSCI Security Framework (DSF©)
- 16 Best Practice areas
- Based on ISO 27001
- Draws upon the tactical recommendations
- Takes note of new approaches, technology and tactical mechanisms evolved

DSCI Security Practices

DSCI Privacy Framework
- DSCI Privacy Framework (DPF©)
- 9 Best Practices and 12 Privacy Principles
- Privacy Policy Guidelines
- Privacy Impact Assessment

DSCI Privacy Practices

A NASSCOM® Initiative
National Skills Registry: Ensuring Personnel Security

- Database of pre-verified resumes.
  - Data ownership with IT Professional.
  - Fingerprint for unique identification.
- Web based secure interface
- Subscriber
  - Pool of country’s IT Skills
  - Safer & Efficient Recruitment
  - Standard Verification Process
  - Cost & Time Saving
- IT Professionals
  - Reduced Recruitment Time
  - Transparent Verification Process

National Level initiative for Personnel Security - Central database

Identity assurance: One person – One Profile, Finger prints of professionals

Technology platform connecting Companies – Professionals – Background Checkers

Factual and objective data-source confirmation

Data ownership & Privacy

Deterrence for professionals faking details

Standard Processes and reporting

Current Status
70 large employers have pledged to recruit through NSR
Enrolments till Dec, 2009: 561,000
Fingerprinting: 344,000
Law Enforcement: Tackling of new age crimes

“Lack of reporting” by individuals, commercial organizations due to fear of adverse publicity and loss of reputation and share prices.

“Transnational nature” and the associated “jurisdictional problems” that contribute to the complexity of investigation.

“30 million policemen” to train apart from “12,000 strong Judiciary”

“Delay in investigation and prosecution” affect the spirit of bringing criminal to justice.

Cyber Crime Case Investigation

The 7 stage continuum of a criminal case starts from perpetration to registration to reporting, investigation, prosecution, adjudication and execution.
Law Enforcement: Tackling of new age crimes

- Separate authority for Critical Infrastructure protection
- CERT-In- nodal agency for Incident management
- Cyber Appellate Tribunal
- Delegation of instigation power to lower level officer
- Cyber Forensic Labs
- Cyber Crime Investigation Cells.
- Cyber Police Stations major Cities
- C-DAC: Home grown forensic tools
- Awareness Programs
- NASSCOM-DSCI Cyber labs: training of law enforcement officials

Rationalization of Internal Security Department

National Intelligence Grid (NATGrid)
- Connecting more than 21 public databases
- Quick and secured access to desired information
- Store, digest and disseminate actionable information

Crime and Criminal Tracking Network and Systems (CCTNS)
- Connecting 14,000 police stations
- Central visibility of crime records

A NASSCOM® Initiative
Thank You