Cyber Security Ecosystem in India

Data Security Council of India
September 18, 2018
New Delhi
Our Mission and Key areas

Our Mission

To **develop capabilities, capacities and norms**, in collaboration with all the stakeholders including the government, required to advance towards a **safer, more secure and trusted cyberspace** for enhancing trade and commerce by increasing global data flows and promoting innovation; **strengthening national security, protecting individuals’ rights** in cyber space and addressing such global issues while safeguarding national and industry interests.

Key Areas

- Public Advocacy
- Thought Leadership
- Capacity Building
- Outreach & Awareness
- Assurance ecosystem
- Global Trade Development

Vision

To be the premier industry body for making cyberspace safe, secure and trusted.
### Aggregated Level Capabilities

**DSCI’s Cyber Forensics Initiative**
- Cyber Lab in Bengaluru
- **67,000** officers trained

**Actions at Industry level**
- Helped set up Banking ISAC
- Structural Mechanism for sharing Information

**Skill Building**
- Sector Skill Council for Cyber Security
- Job Roles, Qualification Packs, Content & Training

**Industry Development**
- Security product development
- Security Service industry
- Resolution of Trade issues, data flow

### Collective Learning & Actions

**Cross Sectoral Platform**
- Membership Program (IT/BPM, BFSI, Oil & Energy, Telecom, Manufacturing)
- Cross-Sectoral Interactions
- Platforms for Ideas & learning

**DSCI Chapters**
- 13 Chapters
- 2000+ Privacy and Security professionals

### Policy & Thought Leadership

**Policy Enablement**
- IT Act & Rules
- Various policy matters
- Global Cyber Norms
- Internet Governance

**Credentials & Trust Mechanism**
- Privacy Certification
- DCPLA & DCPP
- DPC, Privacy Assessment

**Security Standards**
- ISO standards
- Participation & hosted meeting of SC 27

**Thought Leadership**
- Security & Privacy framework
- Cyber Security
- Cybercrime Investigation
- Study, survey and reports
- E-Security Index Model

<table>
<thead>
<tr>
<th><strong>70+</strong> Reports &amp; Papers</th>
<th><strong>250+</strong> CISOs</th>
<th><strong>13</strong> Chapters</th>
<th><strong>500+</strong> DCPLA, DCPP</th>
<th><strong>240+</strong> Colleges</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>450+</strong> Corporate Members</td>
<td><strong>67K+</strong> LEA, Judiciary, Defence officials</td>
<td><strong>7500+</strong> Professionals</td>
<td><strong>100+</strong> Start ups</td>
<td><strong>18K+</strong> Students</td>
</tr>
</tbody>
</table>
Digital Wave in India

Technology Trends

Digital Payments

- Internet users: 500 million + (June’18, expected)
- Telephone users: 1175 million + (March’18)
- Digital transactions: Volume: 1.11 Bn, Value: INR 131.95 Tn (Jan’18)
- Mobile wallet transactions: Increased 40 times in 5 years, INR 24 bn to 955 bn (2013-2017)
- Aadhaar authenticated transactions: 177 Crores (March 2018)
- IoT Devices: 200 million + (Draft IoT Policy, 2015)

Digital Transformation

- Smart cities
- Industry 4.0
- e-Governance

Establishing Cyber Security Baseline

Cloud

- Artificial Intelligence
- Cryptocurrencies
- Mobility

A NASSCOM® Initiative
Changing Digitization Paradigm

Imperatives of “Digitization” are “increasingly opening up orgs to external interfaces & entities”

“Increasing exchanges of calls with cloud” are slowly leading to “full blown adoption of the cloud”

Design for “always on” are bringing many “devices in operations & transaction processing”

“Data centric business innovations” driving “unprecedented collection & processing of PII”

“Protocols & interfaces” designed for one environment are increasingly used in “new environments”

“Data Poor to Data Rich Nation”
Nation with Data Centric Risks

Digital Payments Emergence & Digitization of Banking
...DBT, AEPS, PPI Wallets, Identity based banking

“Ease of on boarding” (one hand) & “National ID scheme” (other hand) making “Biometrics central to authentication”

“Information’s role” is shifting from “measurement & monitoring” to “aiding automated decision making”

“Adoption of digital channels”, and with advanced analytics the role of organizations are moving towards customer advisory & models of self-help

Globalization of Organizations & their supply chains

A NASSCOM® Initiative

Changing Digitization Paradigm

Globalization of Organizations & their supply chains

“Data Poor to Data Rich Nation”
Nation with Data Centric Risks

Digital Payments Emergence & Digitization of Banking
...DBT, AEPS, PPI Wallets, Identity based banking

“Ease of on boarding” (one hand) & “National ID scheme” (other hand) making “Biometrics central to authentication”

“Information’s role” is shifting from “measurement & monitoring” to “aiding automated decision making”

“Adoption of digital channels”, and with advanced analytics the role of organizations are moving towards customer advisory & models of self-help

Globalization of Organizations & their supply chains

A NASSCOM® Initiative
## Existing Cyber Security Initiatives—India

### National Cyber Security Framework
- Amendment to Information Technology Act, comprehensive provisions for cyber crimes: 2008
- National Policies on IT, Telecom and Electronics
- Joint Working Group for PPP on Cyber Security: 2011
- Recognition of country as ‘authorizing nation’ under CCRA product certification scheme: 2012
- National Cyber Security Policy: 2013
- NCIIPC- Critical Infrastructure Protection: 2014
- National Information Security Policy and Guidelines (NISPG)
- National Cyber Security Coordinator: 2015
- Security Framework for Smart Cities
- SEBI Cyber Security Guidelines
- State Cyber Security Policies – Telangana, AP
- IRDAI Cyber Security Framework: 2017

### Data Protection
- IT (Amendment) Act
- Privacy clauses: 2008
- Notification of privacy rules under Sec 43A of ITAA 2008
- A P Shah Expert Group on Privacy; DoPT draft law
- Aadhaar Law and Regulations focusing on Privacy
- New Data protection law in making

### Institutional Mechanism
- NCSC (NSCS-NSA); NCIIPC (NTRO)
- CERTs (CERT-In; Fin-CERT and Power Sector CERT announced)
- Joint Working Group (PPP)
- Sector Skill Council (Skills)
- IB-CART (Information Sharing)
- ISEA (Capacity Building and Awareness)
- Cyber Forensic Lab (Capacity Building)
- LITD 17 Committee of BIS (Standards)
- Industry – Setting up focused entity, DSCI (Policy, Assurance, Capacity Building and Awareness)

A NASSCOM® Initiative
Indian Cyber Security Ecosystem

Government Departments and Agencies

- NSA
- NSCS
- NTRO
- MHA
- MeitY
- MoC
- MEA
- MoD
- MoC
- Regulators

- ICERT
- NIC
- STQC
- CCA
- DoT
- C-DoT
- TEC
- CIRT Navy
- CERT Army
- CERT Air Force
- DIARIA
- CSG-DDP
- RBI
- TRAI
- SEBI
- IRDA

Additional
- IB-CART
- Fin-CERT

Intelligence - IB, RAW, NIA

Based on info. in public domain & for listing purposes only; doesn’t represent hierarchy of any sort
Penalties, Remedies and Offences

Penalties ranging from five crore rupees or two per cent of total worldwide turnover to fifteen crore rupees or 4% of the total worldwide turnover.

The Data principle under section 75 has the remedy to claim compensation for harm suffered as a result of any violation of any provision in the bill from the data fiduciary or the data processors.

The bill inscribes certain offences under chapter XIII of the bill, which are punishable with imprisonment.
Cyber Security: India Advantage

Destination of Global SoCs

Mature Security Practice of Indian IT Services

Security Services Operations set up by MNCs

Destination for Security R&D

GIC security operation centres

Competitive IT Product Ecosystem

100 + Indian Security Companies

150,000 + people working in Security

Preferred Investment Destination

Cyber Security

Experience

Trust

Ecosystem

Services

IP Led Services

Research

Product

Capabilities

Trust

Ecosystem

Acquisitions of Indian Security Product Companies by Global Leaders

Funding into Product Companies on the rise – Seed, Series A, B....

Cyber Security Task Force [CSTF]
Set up NASSCOM-DSCI

By 2025

$35 billion market for Indian Cyber Security products & services;

1 million security jobs

1000 security startups

Technology

Industry

4 Dimensional Approach

Skills

Policy

A NASSCOM® Initiative
## Domestic Market

### Public Sector

<table>
<thead>
<tr>
<th>Reserve specific budget</th>
<th>Reporting of cyber security incidents</th>
<th>Public private partnership</th>
<th>Specific policy intervention</th>
<th>Define and advocate frameworks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor and evaluate investments</td>
<td>Promote and advocate cyber security</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- 10% IT budget reserved for cyber security
- Andhra Pradesh, Telangana and Haryana have announced a policy of reserving budget for cyber security
- Development of Cyber Security Framework for Smart Cities under guidance of National Cyber Security Coordinator, in association with the industry
- MHA developed National Information Policy Guidance (NISPG), which set up requirements for protection of information generated in government departments and bodies
- Developed security and privacy frameworks that serve as a reference in security and privacy initiatives
- Government of India working for ‘data protection regulation’, which will open up new opportunities for cyber security market
Focus on Cyber Security by Regulators

Cyber Security Framework in Bank

Guidelines for Information and Cyber security for Insurer

Cyber security & cyber resilience framework for registrars to an issue share transfer agents
Cyber Security Industry – India View

Cyber Security – India’s current Landscape

- ~ 100 + start-ups
- ~ 150K security professionals
- ~ USD 4 Bn+ Security Market (FY16)
- ~ USD 1.4 Bn Domestic Market

Cyber Security – India’s Vision 2025 | NASSCOM-DSCI CSTF

- ~ 1K focused start-ups
- ~ 1 Mn security professionals
- ~ US$ 35 Bn Security market

Development of Capabilities for Future

- Consolidated view of Current Capabilities and policy Landscape
- Skills and Expertise for Future
- Emerging Use Cases/Whitespaces
- Research and Development of Technologies

DSCI
PROMOTING DATA PROTECTION

A NASSCOM® Initiative
Product Industry Capability Map

- DDoS Mitigation Solution
- Cloud and SaaS Security Solution
- Big Data Analytics Solution
- Social Engineering Solution
- Data Loss Prevention Solution
- Mobile Data Protection Solution
- Advance Authentication Solution
- Governance, Risk and Compliance Solution
- Threat Management Solution
- Antivirus/Antimalware Solution

- Data Security Solution
- Data Classification Solution
- Identity Management Solution
- Fraud Management Solution
- Application Testing Solution
- Program Analysis Solution
- Email Forensics Solution
- Endpoint Security Solution
- Other Network Security Solutions
- IoT Security Solutions
Indian Security Product landscape - A Snapshot

Security landscape

Network security
- Firewall
- Threat management
  - Secure Web Gateway

Identity and access management
- Advanced authentication
- User Provisioning (UP)
  - Web access management

Data loss prevention

Data security
- Mobile data protection
- Cloud access security
- Application security and endpoint protection
- Antivirus/Antimalware
- Testing/Secure email gateway (SEG)
- Enterprise platform
  - Asset security
- Server security
Indian Cyber Security Services Industry

Security Services Industry in India

- Expansion of Services Vertical
- IP Led Services
- New Lines of services
- Closely working with Start-ups
- Security as separate vertical of Business

Examples
- KPIT
- TCS
- Wipro
- Happiest Mind
- Paladion
- Aujas
- HCL
- Infosys
- Tech Mahindra
- Mindtree
- Cognizant
- Persistent

Existing Capabilities Meeting Global requirements

- Cyber Security Advisory
- Governance, Risk and Compliance
- Managed Cloud Security
- Threat Intelligence
- Cyber Crisis Management
- Incident Response
- Managed Security Services
- Identity Services
- Product R&D for Global Majors

Managed SOC Services | Cyber Defence Centre | IP Led Services

A NASSCOM® Initiative
Global In-house Centre (GIC) in India

- 1100 GICs in India
- 800K Employees
- $23 B Revenue
- ~1% of India’s GDP

**Drivers**
- Cost arbitrage
- Access to talent pool

**Move up the Value chain**
- Digital Disruption
- Domain Knowledge
- Leadership – New Business avenues
- Talent attraction and retention
- Distributed Development
- Acting as cost centre – no revenue focus
Digital Payments Security Program

Digital Payments Security Alliance
Bringing a variety of players and stakeholders together on the agenda of securing digital payments and building the national ecosystem

~ 25 Industry members from varied sectors
Banks & Financial Services, Payment systems, service providers, Technology Provider, Industry associations, ecommerce, Institutions like RBI, NPCI, IDRBT etc.

Functions
RTs/Conferences Policy deliberations, Industry Submissions

Online banking and card schemes
BHIM/UPi, AEPS and USSD
Digital wallets and Mobile Banking

Digital Payments Security Campaign
Engage with various communities that will be influenced and impacted by fast paced transition to digital payments and make them aware of the security issues emanated from it

Target Segments
End User Traders Small and Medium Businesses

Functions
Campaign Plan Content Creation Outreach

COMMUNITY AWARENESS
BEST PRACTICES
INDUSTRY DELIBERATIONS
Building Innovation ecosystem at state level with appropriate partnerships & associations, investment opportunities and Policy engagements,

Build and align with existing start up incubators and,

Capability building at start up, university and state level.
DSCI Cyber Forensics Initiative

• Trained 67,000 personnel from
  – Police, prosecution, judiciary and other departments trained in basics of Cybercrime investigation.

• Partnership with:
  – (ISC)2 for localization & development of CCFP credential.

• Capacity building programs for:
  – Indian Defense forces (Army/Navy/IAF), Income tax, Vigilance depts, law schools and financial sector.
  – Designed and delivered specialized training program for banks.

• Assistance to LEA & Industry
Cyber Security – Skill Building

The gap between supply and demand of skilled cyber security professionals is rising steeply. Global Information Security Workforce Study (GISWS) conducted by (ISC)2 has revealed that the world will face a shortfall of 1.8 million cybersecurity workers by 2022.

In line with the vision of **NASSCOM-DSCI Cyber Security Task Force** of having a million Cyber Security professionals in the country by 2025. DSCI & NASSCOM Sector Skills Council (SSC), under the aegis of National Skill Development Corporation (NSDC) are developing Career Map, Standardised Curricula (Qualification Packs) and courseware for upcoming job roles, which is being rolled out in nation wide colleges and universities. Key tracks of courseware are as follows:

1. Network Security
2. Application Security
3. Data Protection and Privacy
4. Identity and Access Management
5. Cyber Assurance / GRC
6. Digital Forensics
7. Incident Management
8. BCP/DR
9. End Point Security
10. Security Operations
11. Industrial Control Security

Numerous universities and institutions are offering PhDs and Master’s degree specializing in Cyber Security/ Information Security. Vocational training program on cyber security have been introduced by Ministry of Skills Development and Entrepreneurship, and also universities like IGNOU.
Thank You!