INFORMATION SECURITY ENVIRONMENT IN INDIA
NASSCOM ANALYSIS

Most Indian companies that are aiming to go global will require certifying their ability to maintain proper security levels when scouting for international clients. Information security is no more a mere legal requirement but it is fast becoming a factor for companies to compete on and grow businesses. A "secure and reliable" environment—defined by strong copyright, IT and cyber laws—is an imperative for the growth and future success of the ITS/BPO industries.

NASSCOM has been proactive in pushing this cause and ensuring that the Indian Information Security environment benchmarks with the best across the globe. ITS/BPO companies in India are taking as many precautions as possible to ensure that data and personal information of their customers is protected. That means following international best practices, getting procedures audited by independent parties and making sure that these procedures are up to date and are being closely followed.

Security Environment in India

Indian companies are known for their quality deliverables. International certifications like ISO 9000 went a long way in establishing this reputation. Likewise following international standards in information security will also help companies build credibility in the minds of their customers.

While most Indian BPO firms are recognized for high quality processes and services, information security orientation may become the Achilles heel if not attended to in time. Special focus needs to be given to the protection of customer data. Merely following good information security practices may not suffice; and it needs to be marketed. So while Indian BPO firms market their process efficiencies and cost savings, they also need to market their adherence to the prevailing international security and privacy standards.

Currently, the information security environment in India is:

- Indian companies have robust security practices comparable to those followed by western companies. Indian companies primarily comply with BS 7799 – a global standard that covers all domains of security
- Companies sign Service Level Agreements (SLA), which have very strict confidentiality and security clauses built into them at the network and data level. Such SLAs also cover all relevant laws that the companies want its offshore providers to comply with and actions that can be taken in case of breaches
- Laws such as the IT Act 2000, Indian Copyright Act, Indian Penal Code Act and the Indian Contract Act, 1972 provide adequate safeguards to companies offshoring work to US and UK
- Most of the BPO companies providing services to UK clients ensure compliance with UK Data Protection Act 1998 (DPA) through contractual agreements
- Companies dealing with US clients require compliance depending upon the industry served. E.g. Healthcare requires compliance with HIPAA, Financial services require compliance with GLBA. To ensure compliance with such laws, Indian vendors follow security practices as specified by clients such as security awareness, protection of information, non-disclosure agreements, screening of employees, etc. Further, clients conduct periodic audits to ensure compliance
- Many companies in India are undergoing/have undergone SAS 70 Audit. SAS-70 assignments helps service companies operating from India to implement and improve internal controls, ensure minimal disruptions to business from clients' auditors, and is potent marketing tool in the face of increasing competition.

NASSCOM's Security Initiatives

NASSCOM has been working closely with ITS/BPO industries to create an Information Security culture within these segments. The association has also been interacting with the Indian Government on the issue of creating a relevant regulatory environment that will further strengthen information security initiatives being rolled out within ITS/BPO organizations. Indian companies have raised their quality standards in recent years to meet international demands. NASSCOM, with the Indian government, has laid the foundation for the required legal framework. The IT Act of 2000 includes laws and policies concerning data security and cyber crimes. Other than the IT Act, the Indian Copyright Act of 1972 deals with copyright issues in computer programs.

The Indian IT industry under auspices of NASSCOM is working with the Government to introduce amendments to the existent Indian IT Act to make it more robust and relevant. The Amendments have already been taken cognizance of by the ministry and will be reviewed shortly and the industry is confident that these will be passed into law in the coming parliamentary session.

NASSCOM is endeavoring to build a robust Information Security environment within the ITS/BPO segments. The initiatives undertaken include the following:

Trusted Sourcing

NASSCOM launched the Trusted Sourcing initiative last year that seeks to re-inforce India as a secure and reliable technology partner. NASSCOM has also instituted the 4E framework to establish India as a trusted sourcing destination. This framework ensures highest standard of information security in the outsourcing industry in India.

As part of the trusted sourcing initiative, the following activities have been undertaken under the 4E framework till now:

4Es	Activities Planned	Status as of December 2005
Engage	▪ Creation of Global and National Advisory Boards on Security ▪ Meet all stakeholders in India and key markets	▪ National Advisory Board operational as of December 2005. ▪ Engaged with the following in 2005: • Department of Homeland Security • Treasury – Infrastructure Compliance • Federal Reserve Board – NewYork • Industry bodies – ITAA, FSTC, BITS • Think tanks – Heritage, CSIS, IPI • Academia – CMU
Educate	▪ Reports to members on model contracts, SLAs, security practices and standards, industry legislation like HIPAA, GLB, DPA ▪ Seminars to educate members, lawmakers and judiciary ▪ Create intellectual capital for members and other stakeholders	▪ Focus on NASSCOM members – created awareness about secure sourcing • Commissioned research reports on security • Educated members on Model contracts, SLAs, best practices through reports and meetings ▪ Educational collateral for judiciary and police in India • Set up training labs at Mumbai (March 2004) and Thane (July 2005), which have imparted one-week training module to about 1,063 officers • Organised/addressed awareness seminars for senior police leadership in six different states • Addressed workshops/seminars for trial judges, at Mumbai and Bhopal • Organised workshops for public prosecutors at Mumbai

		• Cyber Safety Awareness Week being organized in Mumbai every year since 2003
Enact	▪ Examine areas to strengthen legal framework in India ▪ Work with coalitions and regulators in key markets to identify relevant provisions ▪ Best security practices in member companies	▪ Working with Ministry of IT and Ministry of Law-IT Act 2000 being strengthened to bridge the gap ▪ US India Gap Analysis in place – areas ranging from hacking to credit card theft to health information to children's information ▪ Consensus that IT Act, Contracts Act, Specific Relief Act, Indian Penal Code, Consumer Protection Act, Arbitration & Conciliation Act, are largely sufficient to meet concerns ▪ Exploring concept of Self Regulatory Organisation (SRO) for the industry ▪ Working with members to enact secure practices • Physical security – access codes, security guards, fire suppression systems, etc. • Network security – technological solutions like firewalls, anti-virus at various levels, encryption methodologies, authentication and access controls, Intrusion Detection System, VPN etc • Information security –Employee background checks –No access to internet, cell phones, email, instant messaging, not even paper and pens –Stringent customer audits to ensure compliance with GLBA, HIPAA, and other regulatory provisions ▪ Few cases of infringement – inter-agency co-operation between FBI and CBI – cases in court • Liaised with law enforcement to follow up cases involving data security to ensure adequate and prompt response
Enforce	▪ Established Mumbai Cyber Labs – to be extended to other cities ▪ Security audit of members, security certification for employees ▪ Focus on personnel security	▪ NASSCOM has formed an alliance with Business Software Alliance (BSA), and recently launched toll-free numbers to report software piracy ▪ Organised workshops for public prosecutors at Mumbai ▪ Meetings with all India police officers to educate on cyber-security and how to recognize and prosecute cybercrime ▪ NASSCOM and Mumbai Police jointly launched a Cyber cell in Mumbai Police with 24x7 call center – 9 more by the end of 2006 ▪ NASSCOM to launch National Skills Registry of IT & BPO employees and vendors

Mumbai Cyber Lab – MCL

NASSCOM, under its Trusted Sourcing Initiative has been working very closely with Police Organizations in India, helping to train them in Cyber Safety and Cyber Crime Investigations. To facilitate this, NASSCOM and Police organizations have set up Cyber training labs in Mumbai and Thane. Similar Cyber Labs are being planned in more cities all over India, including Bangalore, Delhi, Hyderabad, Pune and Kolkata. To familiarize the Mumbai Police officers with the ITES-BPO industry, a "Suraksha Setu: Know your BPO" Program was launched recently. Under this program Senior Police Officials visited a BPO Operations Unit in their jurisdiction and interacted with the senior management of the organization, with a two-fold objective to know more about the operations of a BPO and how they work as well as to understand the various concerns and issues faced by the industry.

This venture is being actively backed by IT industry as well as various information security professionals who have volunteered to share their expertise to make the lab the foremost center for information security in the country.

National Skills Registry

The booming demand for Indian IT/ITES-BPO services globally has resulted in an increase in the requirement for adequately trained and skilled resources in the industry. The key resource for the success of the Indian IT / ITES-BPO Industry is human capital and steps should be taken to ensure a free flow of talent across the industry.

NASSCOM has been working with different players in the industry to set up a National Skills Registry of employees in the BPO sector. The National Skills Registry is a step to ensure that there is a verified database of the skill sets and talents of the human resources within the Industry, which would enable them to shift within the industry with a minimum of paperwork and reference / verification checks.

This would work as an online registry of workers in the industry and include the employee's professional history, educational and personal background. The data will be validated through an independent third party, but will be owned by the employee.

The registry would enable employees to find jobs quickly and efficiently. For employers it gives them an opportunity to recruit the best.

India-US Information Security Summit

In line with various initiatives by NASSCOM to build a risk-free environment, conducive for business transactions and thereby promote a culture of Information Security, the Information Technology Association of America (ITAA) and NASSCOM hosted the first ever India-US Information Security summit in New Delhi from October 12-13, 2004, and the second one is scheduled from January 18-19 2006 - **"India and the United States: Protecting the Critical Information Infrastructure Alliance".** The conference aims to compare both BPO and client enterprise needs in each main element of information security – people, process and technology -- and highlight best practices and opportunities for further cooperation at the enterprise and national levels for improving the global challenge of information security.