

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 ITES 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. Indian ITeS-BPO companies today adhere to international best practices – they are regularly audited by independent certified auditors, comply with international standards at the highest levels, update procedures and practices regularly and meet, if not exceed the worldwide information security standards to ensure that data and personal information of international customers is adequately protected.

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 is also helping Indian companies build credibility among customers. While most Indian BPO firms are recognized for high quality processes and services, information security practices need to be constantly reviewed and updated according to the rapidly changing environment. Customer data demands special focus.

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 taken a holistic view of Information Security through its 'Trusted Sourcing'¹ initiative to strengthen the regulatory framework and further improve India's attractiveness as an outsourcing destination. This multi-pronged initiative is targeted at employees, organizations, enforcement agencies and policy amendment, through a '4E Framework' - **Engagement, Education, Enactment and Enforcement**.

NASSCOM has been working closely with the ITeS - BPO industry in India, to create a robust and secure Information Security culture, and in association with other stakeholders like the Indian Government on the issue of creating a relevant regulatory environment. All these initiatives aim to further strengthen information security environment, together with initiatives being rolled out by NASSCOM and the ITeS - BPO industry.

NASSCOM, with the Indian government has also laid the foundation for the required legal framework through the proposed Amendments to the Indian IT Act of 2000² which includes laws and policies concerning data security and cyber crimes and the Indian Copyright Act of 1972 which deals with copyright issues in computer programs.

Trusted Sourcing Initiative

This initiative seeks to reinforce 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 until now:

4Es	Activities Planned	Status
Engage	<ul style="list-style-type: none"> ▪ Creation of Global and National Advisory Boards on Security ▪ Meet all stakeholders in India and key markets 	<ul style="list-style-type: none"> ▪ National Advisory Board operational from December 2004 ▪ Engaged with the following stakeholders <ul style="list-style-type: none"> • Department of Homeland Security • Treasury – Infrastructure Compliance • Federal Reserve Board – New York • Industry bodies – ITAA, FSTC, BITS • Think tanks – Heritage, CSIS, IPI • Academia – CMU
Educate	<ul style="list-style-type: none"> ▪ Reports to members on model contracts, SLAs, security practices and standards, industry legislation like HIPAA, GLB, DPA 	<ul style="list-style-type: none"> ▪ Focus on NASSCOM members – created awareness about secure sourcing <ul style="list-style-type: none"> • Commissioned research reports on security • Educated members on Model contracts, SLAs, best practices through reports and meetings

¹ NASSCOM launched the Trusted Sourcing initiative in 2005. This initiative seeks to reinforce 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.

² 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

	<ul style="list-style-type: none"> ▪ Seminars to educate members, lawmakers and judiciary ▪ Create intellectual capital for members and other stakeholders 	<ul style="list-style-type: none"> ▪ Educational collateral for judiciary and police in India <ul style="list-style-type: none"> • Set up training labs – currently 4 cyber labs operational - Mumbai, Pune, Thane, Bangalore <ul style="list-style-type: none"> ▪ Imparts one-week training module to officers ▪ Organised awareness seminars for senior police leadership in Pune, Nasik, Jammu, Gandhinagar, Barrackpore, Aurangabad, Nagpur, Goa, Bhopal, Indore, Jaipur and Gujarat • Addressed workshops and seminars for trial judges • Organised workshops for public prosecutors • Cyber Safety Awareness Week being organized in Mumbai every year since 2003, also conducted in Hyderabad in July '06
Enact	<ul style="list-style-type: none"> ▪ 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 	<ul style="list-style-type: none"> ▪ 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 ▪ The proposed Self Regulatory Organisation (SRO) for the industry is underway ▪ Working with members to enact secure practices <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> –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 <ul style="list-style-type: none"> • Liaised with law enforcement to follow up cases involving data security to ensure adequate and prompt response
Enforce	<ul style="list-style-type: none"> ▪ Established Cyber Labs in 4 cities – to be extended to other cities ▪ Security audit of members, security certification for employees ▪ Focus on personnel security 	<ul style="list-style-type: none"> ▪ 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 launched the National Skills Registry of IT and BPO employees in January 2006

NASSCOM'S FLAGSHIP INITIATIVES**▪ Proposed Self-Regulatory Organisation (SRO)**

The Self-Regulatory Organisation has been conceptualized following an in-depth gap analysis of the Indian law and various international standards (like US and EU laws), identifying the loopholes and then attempting to amend the Indian law to make it equivalent to the global standards which exist. SRO is an independent, self-regulatory body that proposes a basic set of security and privacy standards, to which companies can choose to adhere. This SRO would establish, monitor, and enforce privacy and data protection standards for India's ITES-BPO Industry.

▪ National Skills Registry (NSR)

NSR is a centralized database of all employees of the IT services and BPO companies in India. This database contains third party verified personal, qualification and career information of IT professionals. The objective of NSR is to improve recruitment practices in IT and BPO industry, which will in turn help in maintaining India's global competitive advantage. It is an employee-friendly measure to minimize any misuse of employee identity, where employers will be able to view the verified resume of the IT professional, if authorised by the professional.

Amendments to the Indian IT ACT

The Union Cabinet (on October 16 2006) has approved the amendment to the IT Act 2000. NASSCOM worked with the government to evolve recommendations for amendments to further strengthen the Indian IT Act 2000. The recommendations are focused around protecting overseas customer data and tightening the punishment for defaulters. We understand that these amendments have incorporated most of the recommendations, and are hopeful that this will lead to better handling of cyber crime by enforcement authorities. We expect this to be discussed in the winter session of the parliament.

Additionally, most Indian IT BPO companies conform to global standards such as BS 7799 and also specific standards depending on the country/sector they cater to. For example in the US, Healthcare requires compliance with HIPAA, Financial services require compliance with GLBA.

For further information please contact:**Parul Gupta**

NASSCOM Press office - Text 100

Tel: 91 11 55600144-154

Mobile: 9891071999

Email : parulg@text100.co.in**Deepakshi Jha****NASSCOM**

Phone : + 91 11 23010199

Mobile: 9899096202

E-mail : deepakshi@nasscom.org