

Data Security Council of India

A Self Regulatory initiative in Data Security and Privacy Protection

Nandkumar Saravade and Ponnurangam Kumaraguru (PK)

India currently occupies the leading position in the IT outsourcing and Business Process Outsourcing (BPO) industry. India's total revenue due to IT and BPO outsourcing was US\$33 billion, which is estimated to grow to US\$60 billion by the year 2010. Increasing amount of personal information is thus flowing to India from many countries.

The Indian ITeS (Information Technology Enables Services) and BPO industry, which started with the advantage of low-cost human resources, has now moved on to add quality, reliability and diversity as its differentiators. Companies maturing and successfully coping with the issue of scaling up and expanding, will now need to tackle the problem of offering consistent data security to the customers at an affordable cost. The security landscape is constantly evolving, as the threats, consumer perceptions and legislative and regulatory strategies keep changing. These are the challenges that demand effective responses.

The Indian ITES/BPO companies are striving hard to ensure the security of data and privacy protection. They are following the stringent security controls specified by their customers through contracts. However, many times, the problem cannot be contained by an individual company, irrespective of the cost incurred, and requires industry-level solutions. Successful security solutions require a convergence of the three components: technology, people and processes. Furthermore, a single security breach can tarnish the entire industry's image and the country's reputation as a safe destination for data. Smaller companies lack dedicated resources for handling security and need cost-effective approaches for demonstrative security levels. India's National Association of Software and Service Companies (NASSCOM), the premier trade body and the chamber of commerce of the IT software and services industry in India, is dedicated to acting as a catalyst for the growth of the software-driven IT industry in India. Other goals include facilitation of trade and business in software and services; encouragement and advancement of research; propagation of education and employment; enabling the growth of the Indian economy; and providing compelling business benefits to global economies by global sourcing.

NASSCOM has been proactive in pushing these causes to ensure that the Indian information security environment benchmarks with the best across the globe. As a part of its Trusted Sourcing initiative, NASSCOM is in the process of setting up the Data Security Council of India (DSCI) as a Self Regulatory Organization (SRO) to establish, popularize, monitor and enforce privacy and data protection standards for India's IT & ITeS industry.

Self-Regulatory Organizations

The self-regulatory approach has been applied in different sectors around the globe including the:

- (1) National Advertising Review Council (NARC). The NARC was formed in 1971 to guide and set standards of truth and accuracy in U.S. national advertising ;
- (2) Financial Industry Regulatory Authority (FINRA). FINRA was formed in the U.S. in 2007 to protect investors and market integrity. FINRA educates securities firms and the investing public; enforces federal securities laws; and administers dispute resolution among investors and registered organizations;

- (3) The Banking Codes and Standards Board of India (BCSBI) was formed in 2005 as an banking industry watchdog to ensure that the consumer of banking services get what they are promised by the banks. In addition, there are other SROs in sectors such as accountancy, medical, telecom, and law around the world. As of the writing of this article, there are no SROs elsewhere created for the IT and BPO industry.

As a part of its Trusted Sourcing initiative, NASSCOM has engaged with the various stakeholders to understand the landscape to create an organization to help the Indian IT industry to achieve better security and data protection practices. The research concluded that self-regulation might be the best way for the Indian IT industry to address the security and data protection concerns of the customers from the U.S. and other countries. A few of the advantages for self-regulatory organizations are:

- An industry body is best positioned to develop appropriate data privacy and security standards based on its greater knowledge and sophistication;
- Prompt, efficient responses to industry requirements and market developments;
- Higher compliance as the result of volunteer participation in the SRO; and
- The cost of the regulation is borne by the industry rather than customers.

However, there are also limitations for SROs:

- As the self-regulation is typically on a voluntary basis, the success is dependent on the number of its members. The greater the number of participants, the more effective it will be;
- It is difficult for SROs to raise revenue to sustain and be operational; and
- Since the membership is voluntary, organizations can refrain from becoming a member.

Looking at the advantages that an SRO can bring to the Indian IT and BPO industry, NASSCOM is currently in the process of establishing the DSCI. There is no other organization similar to DSCI around the world.

Mission for DSCI

The following objectives have been developed for DSCI based on NASSCOM's research, interactions with the experts, and the advice received from the Centre for Information Policy Leadership (CIPL):

- To **create awareness** among industry professionals and other stakeholders about security and privacy issues;
- To **build capacity** and provide training among members to develop, and continually improve appropriate data protection and security programs;
- To **adopt, monitor and enforce** an appropriate security and data protection **standard** for the Indian IT/ITES industry that would be adequate, cost effective, adaptable and comparable with the global standards;
- To **create** a common **platform** for promoting sharing of knowledge about information security and to foster a community of security professionals and firms; and
- To **provide** appropriate oversight and **certification** services for member organizations.

DSCI will work in three phases.

Phase I

- To **analyze** the existing security and data protection practices among the organizations in India and to identify areas of improvement.
- To **create** a repository of model contracts which organizations can re-use.
- To **create awareness** among the industry for the importance of the security and data protection practices and raise the bar. To create Security Forums throughout the country to generate awareness among the involved entities and individuals about the importance and measures for data protection.
- To **establish** a credible governance structure for the DSCI.

Phase II

- To **create** various programs through which organizations in India will be trained on different security and data protection aspects.
- To **encourage** and **facilitate** conferences, workshops, symposiums, and discussions on data security and data protections among client organizations and outsourcing service providers.
- To **consolidate, devise and enforce** ethical standards and best practices in line with international standards for creating a secured environment for data in India that would be cost effective and easily adoptable.
- To **certify** companies that adopt the DSCI standard.

Phase III

- To **establish** targets and propose timetables for achievement of the DSCI's goals.
- To **communicate** industry initiatives and successes.

Current status

As of October 2007, DSCI is in Phase I of its planned activities. DSCI has formed a board of directors comprising a mix of industry CEOs, NASSCOM officials, a former senior civil servant and an academician. DSCI also has formed a steering committee comprised of security experts, academicians, industry members and government officials. DSCI had the inaugural meeting of the steering committee members during mid-September 2007 in Bangalore, India. There were many interesting discussions and debates that took place during this meeting.

The members agreed on forming three different working groups to address specific issues. (1) **Research:** This group will focus on understanding the current status and interest of Indian organizations in the context of security, privacy and data protection. The group will conduct a survey to collect this data and write a report on the results; (2) **Model contracts:** This group's aim is to collect different types of contractual agreements from larger organizations or the consultancy companies, and disseminate them to smaller organizations. This will help the smaller organizations to develop their processes according to their clients' expectations. (3) **Business model:** This group's main focus will be on devising methods for DSCI to generate revenue.

The DSCI has embarked on a novel and ambitious plan and will chart its path with the help of all stakeholders.

Nandkumar Saravade is the Director of Cyber Security and Compliance at NASSCOM. Nandkumar is an Indian Police Service (IPS) officer. He specializes in cybercrime issues. He is handling NASSCOM's outreach program on cyber security, focusing on law enforcement capacity building on cybercrime response and enhancing

information security awareness for different IT user groups. He holds a post-graduate degree in Environmental Engineering from the IIT, Mumbai. He can be reached at saravade@nasscom.org.

Ponnurangam Kumaraguru (PK) is a Ph.D. candidate in the COS (Computation Organization and Society) program with the School of Computer Science at Carnegie Mellon University. His research interests include building system to educate users to make better trust decisions, trust modeling and international cyber security and privacy issues (specifically in India). PK is currently helping NASSCOM in planning and executing DSCI. He can be reached at ponguru@cs.cmu.edu.