OUTSOURCINGCENTER
#1 Digital Hub for All Things Sourcing

- **Home**
  - **News Alert**
- **Login**
- **Forgot Password?**
- **Editorial Calendar & Special Offers**
- **Contact Us**

Navigate to … ▼

- **Business Challenge**
  - **Attract & Retain Talent**
  - **Business Transformation**
  - **Cost Reduction & Avoidance**
  - **Customer Satisfaction**
  - **Enter new market**
- **Function**
  - **CRM & Call Center**
  - **Finance & Accounting**
  - **Human Resources**
  - **Insurance Transactions**
  - **IT Infrastructure & Applications**
  - **Procurement**
- **Cloud/Mobility**
  - **Big Data/Analytics**
  - **BYOD**
  - **Cloud**
  - **Mobility**
- **Industry**
  - **CPG/Retail**
  - **Energy & Utilities**
  - **Financial Services & Insurance**
  - **Government**
  - **Healthcare & Life Sciences**
  - **Manufacturing & Hi-tech**
- **Webinars**
- **Awards**
  - **OC 100**
- **Subscribe**

Navigate to … ▼

You are here: Home » India Responds to Growing Concerns Over Data Security | Article

By Gaurav Bhagowati, Business Writer, Everest India December 1, 2004 Read More →

India Responds to Growing Concerns Over Data Security |

Article

A recent opinion poll of 115 IT companies in both India and the US found that 82 percent of customers of Indian IT companies and 76 percent of customers of US IT companies are more concerned about information security than ever before. [*Editor's note*: India's IT industry consists of three major segments: IT hardware, IT software, and IT enabled services which include outsourcing.] Conducted by the National Association of Software and Service Companies (NASSCOM) and the Information Technology Association of America (ITAA), the findings among companies polled indicate that information security is perceived as a key differentiator — greater than 75 percent of respondents agreed that offering sophisticated information security provisions and practices provide a competitive advantage because security has become a critical selling point. The poll results expose a growing concern about data security in the software industry — a part of the backbone of India's position as an offshore provider. Researchers in general agree that as a trend, these security challenges will have implications on outsourcing. As the momentum to offshore to India builds, India's domestic IT services and BPO providers must respond to a daunting wake-up call: balance the escalating costs of maintaining global security standards while staying competitive in a cost-driven market.

The Concerns

India's data security readiness has come under immense scrutiny after the recent hearing of a case involving the theft of source code by an Indian employee. An ex-employee of Geometric Software Solutions Ltd (GSSL), a Mumbai service provider, tried to sell a source code from Solid Works, its US buyer, to another US-based company, according to the case. Pavan Duggal, one of India's eminent cyber law experts and Supreme Court advocate, says there have been numerous cases like this in the recent past. "I'm afraid that this is just the tip of the iceberg. In India, there are far more incidents that are happening than have been reported. India must ensure better safeguards" he says.

According to Ernst & Young's 2004 Global Information Security Survey, companies have identified major viruses, spam and employee misconduct as the key concerns in India. The survey rates major viruses and internet worms as the top concern in India. Employee misconduct is ranked as the number two worry worldwide but is only third in India. Spam mail is considered the big headache. Hence, 91 percent of Indian respondents have anti-virus systems and 56 percent have specific anti-spam protection for their networks. However, less than half (40 percent) of Indian respondents provided their employees with ongoing training in security and controls. Clearly, enforcing standards remains a far cry away. The fundamental and near-term challenge facing Indian companies is to provide the necessary security and data protection while extending access to confidential employees and clients.

The Regulatory Challenge

India's IT Act 2000, which came into effect almost three years ago, remains silent on the issues of privacy, protection and regulated use of data. The Act in its existing form only covers unauthorized access and data theft from computers and networks with a maximum penalty of about $220,000 USD and does not have specific provisions relating to privacy of data. Indian law doesn't cover data interception and computer forgery at all. Thus, data protection issues primarily remain in an unregulated Indian environment.

The Enforcement and Awareness Challenge

According to Anurag Jain of Perot Systems Business Process Solutions and CEO of Vision Healthsource–a part of Perot Systems' healthcare group, major gaps remain in two areas: enforcement and awareness. As a result of high demand by companies looking to reduce costs, some outsourcing service providers in India are hiring new staff by the thousands in a single month. It becomes critically important to ensure that all employees adhere to the same standards. But that becomes difficult when dealing with mass numbers of new hires. The current reality is that an employee hired, for example, in a call center is bound by service contract. Confidentiality and privacy are part of the contract; hence for any breach the employee is liable under the IT Act, Indian Contract Act and Indian Penal Code. "Enforcement is something that we are traditionally not good at and need to take a leap ahead. The government should focus on creating regional bodies that understand the provisions of these acts by employing experts who are empowered to run these provisions," Jain adds. "Thus training, education, and ongoing awareness campaigns for new hires may alleviate part of the problem." To further protect

confidential information and privacy, pundits agree that the best safeguard may be to enact a law on data protection. The United Kingdom, for example, has the Data Protection Act, 1998, in place. There is no such law, or its equivalent, in India. Even if the law existed, enforcing standards, in short order, on mass volumes of new employees is daunting. Pavan Duggal says, "The IT Act 2000 has provisions to protect data that comes from overseas, but to say that it's enough would be a fallacy. It is not comprehensive, to say the least. We [India] must provide effective and comprehensive safeguards against data theft."

Certification and Standards: An Interim Solution?

NASSCOM estimates said that the country's software and services exports industry recorded revenues of $8.9 billion in 2003-04, while the BPO segment witnessed a growth of 46 percent to touch $3.6 billion in 2003-04. Unless India provides enabling factors to protect the country's projected growth, outsourcing will take a hit, according to Duggal. Though most Indian firms are now implementing strong security practices and resorting to standards like the British Standards Institute's BS 7799 or Six Sigma certifications, Duggal makes another point. "I agree that certifications are good to garner more business and it makes US or UK-based clients happy. But it is important to note that despite compliance of these foreign laws, there is no provision in Indian law that provides remedies if there is a data breach in India." In fact, says Duggal, "There are hardly any laws enacted by parliament with outsourcing in mind."

Rob Ramer, founder of outsourcing risk mitigation firm Terra Firma Security Inc., says, "Depending on the nature of a company's core business, their IP is what can make them or break them and therefore it is totally irresponsible to expose critical intellectual property to risk merely to cut costs." Vision Healthsource's Jain points out another important issue: there is clearly a need for more qualified information security experts than available. "Even leading information risk management bodies lack qualified experts in their fold and hence, fail to do a good job," he says. "The fact that there are different industry acts that need to be complied with, like the Sarbanes Oxley Act (SOX), the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA), makes the problem even more complicated. "

Reality Check

To press forth India's case as the most favored sourcing destination, NASSCOM says that Indian companies are relatively better positioned and more focused than US-based or other service providers when it comes to enforcing security standards or taking on globally accepted certifications. A 2004 report entitled Study on Indian Information Security Environment conducted by NASSCOM and business research firm Evalueserve suggested that Indian companies have efficient mechanisms and practices in place and that most Indian companies are well aware of the latest technologies and are willing to adopt the requisite practices. Still, in October, at the NASSCOM-ITAA sponsored India-US Information Security Summit 2004 in New Delhi, Jerry Rao, chairman and CEO of MphasiS BFL and chairman of NASSCOM, warned against complacency. "With Indian firms increasingly dealing with more high-end work and sensitive data from overseas, it's becoming essential to adopt and enforce best practices in security and integrate the concept," he said. Terra Firma Security's Ramer agrees. "It is true that many Indian companies have invested heavily and made great strides in information security. But this gives us all a false sense of security. I would argue with any company that said their mechanisms and practices ensure information security. The fact that you have never been attacked is not proof that you have a good information security program. The only proof that your security program is good is in how it responds to an attack." Most leading Indian outsourcing companies, including Infosys Technologies, Wipro Technologies, and Tata Consultancy Services (TCS), go to extreme lengths to protect their customers' data. It is absolutely critical that suppliers make sure that only the right people working on a project have access to the data. If a client says that a particular project is sensitive, Infosys, for instance, uses biometric security, including retina scans and palm reading, to identify employees against their records. In addition to performing employee background checks and using magnetic access-cards, many outsourcing providers also monitor employee access electronically and search bags when people enter and exit the facilities.

Hope on the Way

NASSCOM says it is working with the Indian government to incorporate new clauses that will likely enable the IT Act 2000 to conform to the adequacy norms of the European Union's Data Protection Directive and the Safe Harbor privacy principles of the US. As the offshoring marketplace in India expands, there is hope on the horizon in addition to the governmental action currently underway. Third party auditors who regularly review the security policies, procedures, and processes are already in place to meet the increasing need for security compliance. "Third party auditors are needed, but this does not necessarily mean using high-dollar international accounting firms. It is important to ensure that the auditors are truly independent of the service provider," emphasizes Rob Ramer. Buyers of outsourcing services in India may consider data

security and protection measures as part of the performance targets achieved by suppliers and may also consider supplementing the outsourced service with a third-party security auditor.

The Wake Up Call Appears to Be Working

Despite the fact that India's low-cost and highly-skilled labor pool is seen as an attractive solution when outsourcing IT applications and processes, the weak implementation of security standards present Indian outsourcers with a major dilemma. However, current studies and statistics present positive evidence that India is waking up to reality, albeit sluggishly. Keep in mind, India's economy shook off the shackles of government bureaucracy and its famed red tape only in the early 1990's. The history of legal developments and ethics in India is relatively new compared to the US or the rest of the developed world. So, it appears that the wake-up call is working and India is donning fighting clothes to compete in the world-wide data-security and protection arena.

Posted in: [Articles](), [Big Data/Analytics](), [Contract](), [CRM & Call Center](), [Financial Services & Insurance](), [Function](), [Government](), [Healthcare & Life Sciences](), [Industry](), [IT Applications](), [IT Infrastructure & Applications](), [Manufacturing & Hi-tech](), [Security](), [Vendor Management]()

Subscribe

If you enjoyed this article, subscribe to receive more just like it.

[Click here to subscribe to Outsourcing Center.]()

Post a Comment

Your email address will not be published.

[   ] Name (required)

[   ] Email (required; will not be published)

[   ] Website

I'm not a robot
reCAPTCHA
Privacy - Terms

You may use these HTML tags and attributes: `<a href="" title=""> <abbr title=""> <acronym title=""> <b> <blockquote cite=""> <cite> <code> <del datetime=""> <em> <i> <q cite=""> <strike> <strong>`

Submit Comment

Enter Search Terms | search

Top Downloads

1 Value-Driven Sourcing in the Digital Era: The New Playbook

R. Arun Kumar, Capgemini. Sameer Bhagwat, Capgemini. Duncan Aitchison, Capgemini

2 Top Ten Reasons Why Outsourcing Fails

Outsourcing Center, Karthik Nagendra, Business Writer

3 Customizing Service Level Agreements

Outsourcing Center, Karthik Nagendra, Business Writer

4 Transition to Cloud: Challenges and Best Practices

Moninder Bhogal, IMS Solutions Architect, NIIT Technologies, Inc.

5 Unlocking Media Industry Innovation with the Cloud

Jeremy Greening, Dell Cloud Services. Jerry Maier, Dell. Barbara Lewis, Outsourcing Center

Most Read

1 Insurance Forecast: The 13 Big Challenges of 2013 or How to Leave the '80s Behind

Beth Ellyn Rosenthal, Senior Writer

2 Five Tips for Surviving Outsourcing Orals

Ben Trowbridge, Chairman, Outsourcing Center

3 Ten Key Questions for Developing an Effective Service-Level Agreement

Brad L. Peterson, Partner, Mayer Brown LLP

4 Running IT at Two Speeds

Alex Martins, TaaS Global Capability Leader, HP

5 Is Your Maintenance & Support Approach Making Your IT Sick?

Debbie Fisher, Business Writer, Outsourcing Center

Monthly Content

Select Month ▼

Sponsors

-
-
-

- [About Us](#)
- [Tags](#)
- [Contact Us 214-537-3307](#)
- [Outsourcing Center | 100 Crescent Court | Suite 700 | Dallas, TX 75201](#)
- [Privacy Policy](#)

© 2016 Outsourcing Center. [WordPress Theme by Solostream.](#)

☺