# OUTSOURCING: DATA SECURITY AND PRIVACY ISSUES IN INDIA

**Nipul Patel, Purdue University North Central, npatel@pnc.edu**
**Susan E. Conners, Ph.D., Purdue University Calumet, conners@calumet.purdue.edu**

## ABSTRACT

T*he paper discusses security and privacy issues with companies outsourcing IT to India . The questions examined are if India has adequate security measures and does the Indian legal system offer similar privacy and security protections other countries. The measures taken by India and cyber laws in India, the United States, and the United Kingdom are reviewed. The findings discuss the steps India has taken to compete in the global outsourcing market.*

**Keywords:** Outsourcing, security, India, information technology

## *INTRODUCTION*

India is the second largest populated country, behind the United States with English as its primary language. It has one of the fastest growing demographics of personal computer and Internet usage. Due to tremendous technological growth, India is experiencing a major paradigm shift to using a multitude of technologies. Some of major changes occurring include computerization of governmental and other regulatory agencies, mobile camera phones in public places, and RFID transmitters in identification cards. The general population is still primarily unaware of consequences related to identification theft. India is quickly benefiting from the worldwide process of outsourcing. Tremendous amounts of personal information and data are flowing into Business Process Outsourcing (BPO) companies throughout India. Currently the Indian IT industry lends its services to about 100 countries around the world with the United States and the United Kingdom as its biggest customers.

### India's Challenges in Outsourcing

India recognizes the need for world's biggest organizations to be able to process information quickly and inexpensively and its response has made it the world leader in the outsourcing industry. India is the preferred destination because of its ability to provide a technically proficient labor force at a relatively cheap cost. Although BPO's continue to attract new customers, the industry in general is still looses clients annually because of lack of trust in its security and privacy issues.

Indian service providers, BPO's, and data centers do not demonstrate adequate compliance with data security and privacy measures. The serious disagreement between courts on interpretations of the law creates problems for IT companies. This generates distrust from foreign customers. There are concerns that the Indian legal system does not guarantee security and privacy like its counterpart the Data Protection Act in the United Kingdom. India's legal process is rather slow in due diligence and discovery. It needs to be more proactive. It is sometimes extremely slow in digital piracy cases because of varying legal interpretations. This lengthy process creates adverse conditions for companies involved in digital commerce where time is of utmost essence.

There has been only one major case of data piracy but it has adversely affected the country's image due to international publicity. NASSCOM (National Association of Software and Service Companies) is India's self-regulatory body of IT related matters. It has identified malware, spam and behavioral misconduct by key employees as some of the key concerns for the industry. Due to the public knowledge of these cases, foreign companies prefer to establish strict standards for data security and codes of employee conduct prior to signing any outsourcing contracts with India.

### Meeting the Challenges

United States and United Kingdom companies that engage in international outsourcing are implementing initiatives to comply with various laws. These initiatives include a rigorous vendor selection process and emphasis on data security measures, identification and sharing of best security practices, appointment of security and legal teams to train the vendor's employees, continuous internal and external auditing, ongoing integrity and security training at the vendor location, strict confidentiality and security agreements prior to awarding any work, dedicated network infrastructures, and only sharing production data when appropriate. Vendors have access to dummy data during the testing phase and testing on

production data takes place on the client network and only at the client location.

Even though, none of the current regulations within US require encryption of any stored data, companies are discovering that encrypting sensitive data involves relatively small financial burden and saves the organization expenses related to data breach fines and overall embarrassments. According to a CIO magazine report, most proactive companies now encrypt all portable data (Laptops, PDA or data that shipped while outsourcing), while leaving all in-house data intact. [6]

**Data Security Problem**

Whether data stays in-house or is off shore, data security is always a major concern. The real issue is ethical behavior by employees. Background checks along with proper and thorough employee training are the most essential components for security. Indian BPO's are certified with BS7799, the most widely recognized information security management certification. BPO's throughout India are employing a complete paperless workplace to improve security and measures are being taken to protect and isolate client data from being stolen or improperly accessed.

A recent study by Price Waterhouse Cooper and CIO magazine found that despite the perceived lag in data security protocols, Indian companies are finding ways to improve their security measures. These companies are outspending other nations by almost thirty percent on data security. Western companies continue to struggle with the constant updating of security and privacy laws. The study reports 1 out every 5 companies are not compliant with various state security breach notification laws. That number rises to almost thirty five percent that are non-compliant with the Sarbanas-Oxley law. Forty percent of the respondents report non-compliance with HIPAA. The same study indicates that this problem is worldwide. Fifty percent of the Australian organizations are not fully compliant with Australian Privacy Legislation. Forty two percent of French organizations did not meet compliance with CNIL (Independent French administrative authority on data privacy). Thirty one percent of the United Kingdom based organizations did not meet compliance with Data Protection Act. The number is about forty-five percent with other European Nations and about thirty percent with Canadian companies.[13]

The same study also reveals some surprising facts about specific industries. The financial services industry encrypts data during transmission only sixty eight percent of the time. Only forty three percent of the companies' encrypted stored data and forty two percent of the companies kept accurate inventory of user related data. Security policies reveal that more than half of the companies within financial services industry do not address adequate data protection, disclosure and destruction.

According to a similar study published in CIO magazine, top IT executives are occupied with operational demands and unable to devote time to implement all the new legislation. The study reports IT organizations spend between 5,000 and 20,000 man hours annually trying to comply with the Sarbanes- Oxley Act requirements. The laws are often hard to interpret and do not have specific requirements. The California security breach notification law does not require notification in the event that data is encrypted yet there is no requirement to encrypt data. [6]

Data breaches are common in governmental agencies as well as in businesses.(Holmes, 2006) In April 2007, the U.S. Department of Agriculture (USDA) reported that thousands of social security numbers of loan recipients were publicly available from a database maintained on the USDA website. In August 2006, the Veterans Administration admitted to losing a considerable amount of patient insurance claim data. Major universities report unknowingly exposing student or faculty data including addresses, social security numbers and tax information.[8]

## RESEARCH QUESTIONS

This paper examines whether the Indian companies (BPO's) take adequate measures to protect personal information and whether the legal system provides adequate protection for its international customers.

The research questions examined are as follows:

$_1$: Does India have adequate security measures to safely handle outsourcing from other countries?

$_2$: Does the Indian legal system offer privacy protection similar to other countries?

The paper examines the current privacy issues of IT outsourcing to India and discusses the various cyber laws of the countries that are its main customers.

## FINDINGS

An explanation of Indian security measures and a discussion of legal security issues in India and its major customers are reviewed.

### Measures Instituted by Indian BPO's

A study conducted by United Kingdom's Financial Services Authority reveals that customer data handled by call centers in India is as secure, if not more secure, than their counterparts in the western hemisphere. Despite security concerns and negative publicity, some of the biggest software and hardware production enterprises place high stake operations in India. The companies are assured by their Indian service providers that data security and privacy standards are in place. Reputable BPO's agree to be held accountable to global laws and litigations. The increasing domestic and global competition forces BPO's to adopt and implement international standards for information security and privacy. These standards require a thorough background check for all potential employees. Their Internet access is limited unless required for a job function. This affords protection from malware and viruses. Tools that can be used to copy data, such as USB drives, mobile phones, cameras or even pens and pencils, are prohibited in the job environment.[4]

The Indian BPO's safeguards are sometimes more robust than the clients' own servers and locations. Western clients are looking for safeguards related to network security, personnel security, physical security and protection of privacy and information. These companies require technologies such as, state of the art security systems, data guards such as firewalls and adequate and up to date virus protection. Personnel and physical security standards must be defined prior to any work be sent offshore. Past experiences and security measures along with certifications such as BS7799 are thoroughly reviewed prior to awarding any work. Some companies have chosen to deploy their own security consultants and companies to provide protection.

Industry giants in India, Wipro and Infosys, were employing strong security measures even prior to the 2000 legislation. According to Computerworld Magazine, Wipro call centers are protected by physical security, network security, and personnel security. Physical security methods include security fence with sliding steel gates where all visitors are issued photo-ID badges, card keys and biometric authentication devices are used to control access to highly sensitive areas, closed circuit monitoring for surveillance, employees are prohibited from carrying mobile phones or any other type of mobile storage devices, and all ports and devices that can be used to transport data outside of the center are disabled. Network security measures used are complete documentation including implementation of the network, thorough event logging, complete set of monitoring tools, state of the art intrusion detection tools, and completely updated encryption technologies and secure connections. There are two methods used for personnel security thorough background and reference checks on potential employees and confidentiality agreements by all relevant employees.(Vijayan,2004)

Infosys, another leading BPO in India, now has a backup storage sites outside of the country. As a precaution, client data is shipped at a regular interval to these "offshore" facilities in addition to providing exclusive backup facility for each of its clients.[12]

According to IEEE, major players within the BPO industry in India already have stringent security measures in place. Masking of sensitive information (Social Security Numbers, Names, Addresses, etc.) is achieved at the preference of outsourcing company. All hardware devices that could be used to store, copy or forward data are removed from computers. Biometric security devices, including palm and retina scanners, are used to identify employees. Strict background checks, magnetic access cards, and checking all handbags upon entry and exits are standard features at most companies.[9]

Compliance regulations from Securities and Exchange Commission and other regulatory agencies require internal controls for application development and maintenance that must be extended offshore if any portion of the work is to be outsourced. Compliance documents from western clients must now include data security and privacy assurances from outsourced companies. BPO's must be constantly aware of new regulations if they want to stay ahead in the race. NAASCOM is setting up a legal arm that would constantly monitor law revisions around the world.

Although, Indian legal system (IT Act 2000) provides measures for basic protections, India does have other laws in place to assure companies looking to offshore processing work. Western companies require their Indian counterparts to have legal understanding of

laws such as, Data Protection Act (UK), HIPAA and the Gramm-Leach Bliley Act (GLBA) (US).

**Cyber Laws**

Cyber laws around the world are attempting to define rules and guidelines for legal electronic business activities. Interpreting these laws is often an art rather than a science. Companies compare the policy compliance with bottom line consequences. In a recent report in CIO magazine, most companies comply with legislative requirements because they are mandatory. However going above and beyond these laws is a business decision and depends on its effect on corporate profit.[6]

*IT Act 2000 (India)*

India regards its IT industry as one of its top revenue generating industries and has a separate Ministry of IT. The purpose of this ministry is to streamline the approval process and reduce government regulatory processes. In May 2000, India passed the long awaited IT Act 2000 to address the growing demand for e-commerce and recognize e-commerce as parallel with traditional commerce. This act provides legal recognition for electronic transactions, provides legal definitions for most of the IT related terminologies and outlaws any crime of an electronic nature. In addition, it recognizes digital signatures as unique and proper identification for a sender. Digital signatures are given equal status to traditional signatures and are accepted in Indian Courts. The Indian IT Act of 2000 provides legal protection to business conducted via electronic means. It revises ancient laws and provides remedies for electronic-crimes. Highlights of the Act include e-mail communication has legal status as a valid form of communication within India, digital signatures and digital records (Government and private) have legal status and are considered legal records in litigation, and e-governance is defined. Governmental departments are empowered to create, file, and store governmental documents in digital format. Monetary damages are implemented for cyber crimes, and internet service provider guidelines are defined. The IT Act 2000 is a major step toward convincing offshore customers that they are protected by the legal system in India.[7]

The IT Act 2000 is a first step towards creating a legal framework for the IT industry. NASSCOM is working towards further changes in the law. Key areas for revision are defining and regulating electronic monetary exchanges or electronic payments. The growth of banking and e-commerce industries are dependent on this type of regulation. Intellectual property rights are vaguely defined and require stronger protection and domain name rights are unprotected. An investigation of cyber crimes is the jurisdiction of local police agencies and local police officers are not always informed about the legal aspects of e-commerce. This creates a problem and the investigation takes longer than necessary.

The Indian Government has demonstrated its readiness for the next phase of commerce by the E-Governance initiatives. In late 2006, the Indian Parliament approved new data security and privacy proposals to strengthen and reaffirm confidence in Indian companies. These proposals enhance the IT Act 2000 with stronger provisions against data theft and security breaches. Legal accountability for data breaches, identity theft and misuse of private information are addressed in these revisions. There are several proposed changes and additions to the existing act. The updates include making leakage of personal data a criminal offense. The unauthorized access of a computer system and accessing personal information without proper consent or unauthorized copying of data would be punishable with a mandatory jail term. The burden of protecting the data is on the organization itself and failure to act on discovery of a breach would result in civil and criminal penalties. The development of internal and external best practices and guidelines for each licensed company's commercial security and communications policy is required.

The Indian outsourcing industry realized in 2006, that China, the Philippines and other countries are rapidly entering and competing for the outsourcing market. Although, India has taken several steps towards positive assurance, data privacy and security continues to remain as the top concern for western companies looking to outsource work to India. NAASCOM has setup a watchdog organization to monitor data security and privacy practices in the IT sector, call centers and BPO industries. These initiatives are a reaction due to allegations of data hijacking and data piracy by Indian outsourcing employees.[11]

Companies looking to outsource any work internationally must first ensure that precautions are in place. Rigorous background checks are required and conducted prior to hiring any employee. Employers require confidentiality agreements prohibiting disclosure of any privileged information. Data security standards such as BS7799 or SAS70

are required to be in place prior to awarding any work. There are announced and unannounced data security audits and data protection mechanisms are include encryption standards, firewalls, intrusion-detection systems, content filtering tools, event logging and monitoring technologies. The physical security standards, access-control audits, and disaster prevention mock drills are reviewed. In addition, off-site storage and disaster recovery plans must be reviewed prior to awarding any offshore work.

*Data Security and Privacy*

Security is still considered a technical issue instead of a boardroom discussion. Data security and privacy should be controlled through corporate procedures or a business framework. Companies need to be proactive and identify "holes" in their systems in advance to avoid waiting to take corrective actions when the breach occurs. They need to be completely transparent about the security measures and use the information as a marketing standpoint to perspective clients. Employing certified security professionals to safeguard the data would prevent possible breaches of security.[10]

According to the Network Magazine, traditional unbounded networks are concerned about the confidentiality, integrity and availability of information. The increased usage of Intranets, access controls, authentications and non-repudiations are major issues for organizations.[10]

A national skills registry allows employers to conduct background checks on prospective candidates. A recent report states approximately seventy percent of the Indian IT workforce is part of this registry. NASSCOM is setting up a self-regulatory organization that conducts audits at member locations. It will monitor member companies to ensure data security and standards compliance. Outsourcing firms are hesitant to discuss their outsourcing decisions because of overall negative feelings and general public relation concerns. The skills registry and other concrete security decisions by Indian BPO's have helped ease these concerns.[1]

According to NAASCOM, the current environment suggests that positive changes have been made by most Indian BPO's. All member companies are compliant with BS7799, IT Act 2000, Copyright Act, Contract Act, and Penal Code of India and provide adequate protection for data security. The IT Act 2000 is being reviewed and revised by current legislators and Health Insurance Portability and Accountability Act (HIPAA), and the Gramm-Leach-Bliley Act (GLBA) compliance is being addressed for United States clients. Data Protection Act compliance is being addressed at the request of United Kingdom clients.

Data Protection Act of 1998 and Electronic Communication 2003 (EC Directive) of United Kingdom require UK based companies not to share personal information without proper legal arrangements. Similarly US based companies are required to comply with HIPAA (Healthcare Industry) and GLBA (Financial Industry). Compliance with these laws is particularly important when with offshore work due to punitive penalties attached to non-compliance.[3]

*United States Regulations*

The Health Insurance Portability and Accountability Act (HIPPA) among other provisions, provides a uniform protection for all health related information that is stored and transmitted electronically and contains security and privacy clauses. These clauses require all entities to ensure confidentiality, integrity and availability of all electronic records. Healthcare providers are required not to disclose any health related information without the consent of all affected parties.

The Gramm-Leach-Bliley Act (GLBA) provides privacy protection for the financial services industry. It ensures protection for personal and financial information of customers and safeguards against anticipated threats and hazards to customer information. It includes measures for protecting unauthorized access of sensitive information.

The Right to Financial Privacy Act (RFPA) provides the confidentiality of individual financial records. It requires notification to the customer prior to disclosing any records to governmental entities. It allows customers explicit rights to challenge such disclosure. In addition, it requires all concerned governmental entities to produce an appropriate audit trail of such disclosures and any transfer between governmental agencies.

The Sarbanes-Oxley Act of 2002 is administered by the Securities and Exchange Commission which sets deadlines for compliance and publishes rules on its requirements. This act is not a set of business practices and does not specify how a business should store records. It defines which records are to be

stored and the retention period. This legislation requires that all business records, including electronic records and messages, must be saved for "not less than five years." The consequences for non-compliance are fines, imprisonment or both. Companies are faced with the challenges of creating and maintaining a corporate records archive in a cost-effective fashion that satisfies the legislation requirements.

*United Kingdom Regulations*

While the United States has sector specific laws to combat data security and privacy issues, The Data Protection Act is considered an umbrella protection law regarding all public and private information within the United Kingdom. It covers all issues related to the collection, storage, processing and distribution of personal data. The act provides measures for individuals to access their personal information. Upon discovery of false information, the act allows individuals to claim compensation from obligatory organizations.

The Regulation of Investigatory Powers Act 2000 (RIPA) explicitly outlaws any interceptions of electronic communications without express or implied consent of both sender and receiver. The Privacy and Electronic Communications Regulations 2003 (EC Directive) ensures the protection of rights and freedoms associated with processing personal data and right to privacy in the telecommunications industry.

*Results*

The first question examined is "Does India have adequate security measures to safely handle outsourcing from other countries?" and the findings report major advances in India to achieve this goal. The advances in the Indian cyber laws and measures put in place by Indian companies suggest that India is keeping pace with other international security measures

The second question is "Does the Indian legal system offer privacy protection similar to other countries?" The review of the Indian cyber laws indicates that India is addressing the major legal security and privacy issues being addressed in other countries. The requirement to address the laws of outsourcing countries is impacting the Indian cyber laws.

Overall, India is successful in attracting outsourcing countries and meeting the security and privacy concerns.

## CONCLUSIONS

Indian companies will have to provide proper data security and privacy protection infrastructures to attract international clients. Information security is not only a legal requirement but a factor to compete globally. A secure information technology infrastructure aided by defined copyright and other strong cyber laws is a necessity for future growth. The outsourcing industry is more competitive and the overall awareness of security issues surrounding the industry is increasing. Companies need to be aware that not only the process but sensitive customer data is being outsourced and needs to be protected. Failure to recognize these issues can negatively impact the companies' reputation.[2]

In addition to United States and United Kingdom laws, Canada, Japan, and the European Union are increasingly becoming stricter on data privacy and protection and defining what measurements must be taken to protect data. This is an international concern and countries wishing to attract international outsourcing must address security and privacy issues.

## REFERENCES

1. Carr, S., India to Tighten Offshoring Data Security, ZDNet News, May, 2006
2. Daniel, D., Security Secrets of Outsourcing, CIO Magazine, April, 2007.
3. Ernest & Young, Achieving Success in a Globalized World: Is Your Way Secure, 2006 Global Information Security Survey
4. Financial Services Authority Offshore Operations: Industry Feedback Report, April 2005, London, England
5. Holmes, H., The Global State of Information Security 2006, CIO Magazine, September 15, 2006, p. 3-11.
6. Holmes, A., Your Guide to Good Enough Compliance, CIO Magazine, April, 2007.
7. NASSCOM press release, NASSCOM Announces Milestones for Its 'Trusted Sourcing' Initiative, April, 2007.
8. Rosencrance, L., U.S. Agency Acknowledges Data Breach, CIO Magazine, April, 2007.
9. Singh, V., Under Pressure India Mulls Step to Protect Privacy, IEEE Spectrum, February, 2005.
10. Pereira, B., Information Security: A New Approach, Network Magazine, April 2003.

11. Trombly, M., India Tightens Security, Insurance Networking New, August, 2006.
12. Vijayan, J., Security Expectations, Response Rise in India, Computerworld, August, 2004.
13. Oliver, K., The State of Information Security 2006, A Worldwide Study by CIO, CSO & PriceWatehouseCoopers, September, 2006.