THE FINANCIAL SERVICES ROUNDTABLE

Impacting Policy. Impacting People.

HOW SAFE AND SECURE IS IT?

AN ASSESSMENT OF PERSONAL DATA PRIVACY AND SECURITY IN BUSINESS PROCESS OUTSOURCING FIRMS IN INDIA

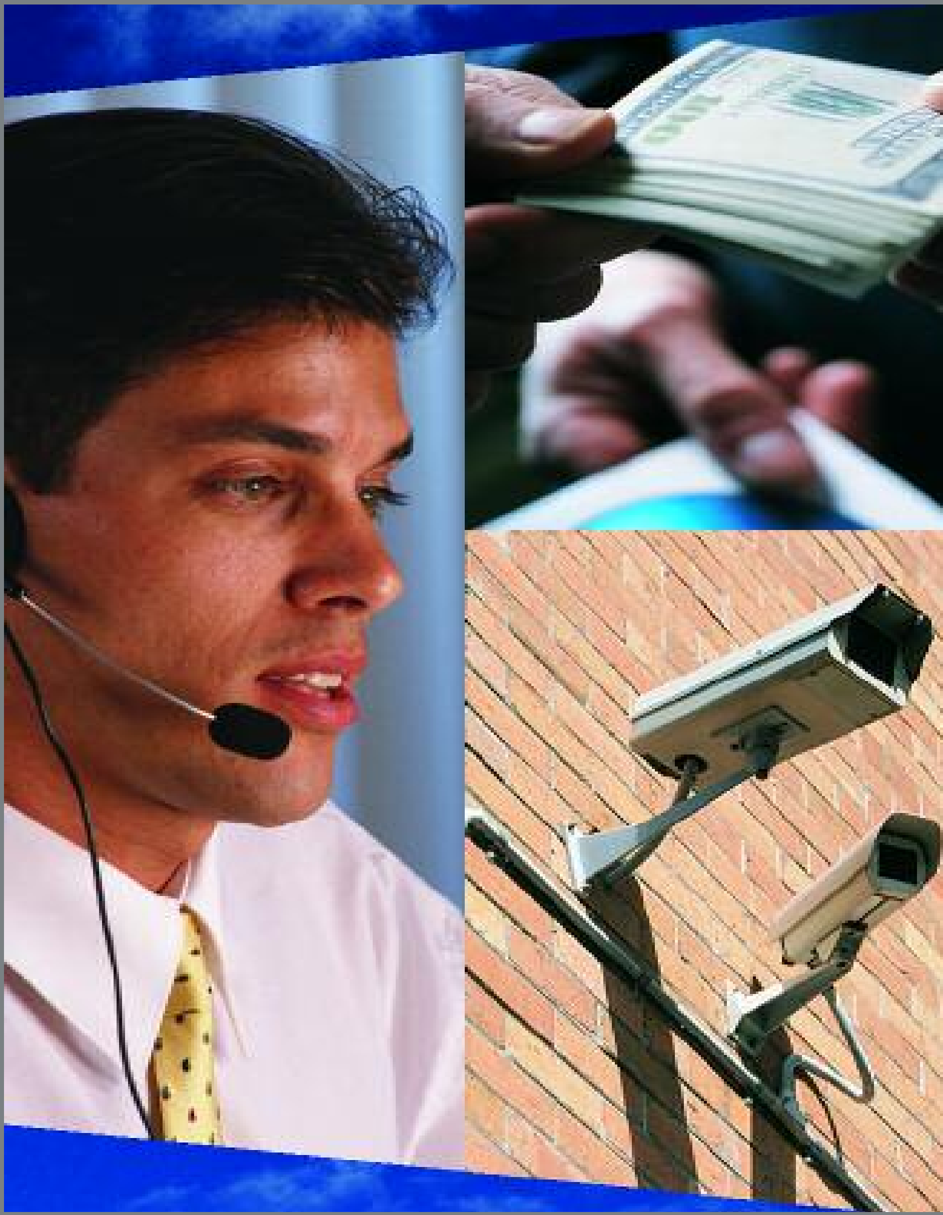


Table of Contents

Message from Cluff Fund Chairman Kenneth J. Glass, Chairman and CEO, First Horizon National Corporation

On behalf of the Anthony T. Cluff Research Fund of The Financial Services Roundtable, I am pleased to present this study on outsourcing firms in India.

This study will be particularly helpful for those who are interested in answering the question posed in this study – namely, how safe is personal data when so many financial services companies outsource work to firms in India?

On behalf of the Trustees, I would like to thank Dr. Michael Turner and the Information Policy Institute for his time and expertise. I would also like to commend the members of the BITS IT Service Provider Working Group for providing information and insights to develop this survey. Also, Faith Boettger, Senior Consultant, BITS, and John Beccia, Chief Regulatory Counsel and Research Director for The Financial Services Roundtable, for their efforts with this study.

Should you have any questions about this study, please do not hesitate to contact John Beccia at the Roundtable at 202.289.4322.

Sincerely,

J. Kenneth Glass

J. Kenneth Glass
Chairman, Anthony T. Cluff Fund
Chairman, and CEO, First Horizon National Corporation

The Anthony T. Cluff Research Fund designs, approves, and funds research on issues affecting the financial services industry and related public policy. The results of these studies advance the policies of the Roundtable, and inform and educate opinion leaders and policy makers

A. The Issues

Early in the 2004 legislative year, state and federal lawmakers increasingly began to view the offshoring debate through the lens of data security and privacy. Stories circulated of disgruntled data processors in far away places holding sensitive health or financial data about Americans for ransom, or selling it to rings of organized criminals. While some of these stories were true[1], much of what circulated through policy circles was exaggerated and distorted.[2]

These stories have yielded the perception that sensitive data about Americans is extremely vulnerable once it leaves U.S. shores. This perception has led to proposed legislation that, in the name of consumer protection, would restrict transborder flows of financial and medical information.

The trend toward worldwide sourcing by firms is a significant phenomenon, but how significant it happens to be is unclear. McKinsey estimated that the value of business processes offshored from the United States was $25.7 billion for 2001.[3] Input, an IT market research firm, estimated the value to be $26.4 billion in 2003.[4] Both assume the trend to be growing by more than 30% a year. At 30% growth per year and $25.7 billion in 2001, we would expect the total value of business process outsourcing (BPO)[5] to have been $43.4 billion in 2003. BPO revenues in India were estimated by the National Association of Software and Service Companies (NASSCOM) to be $3.9 billion in the 2003-2004 period, less than 10% of the value of the sector globally.[6] Nonetheless, the trend is growing.

Consumers also have taken notice.

This study answers some questions that are of concern to consumers and the public in general: Is my personal data safe overseas? Is the financial institution I use safeguarding my data from hackers, identity thieves, and other criminals? When my institution outsources business practices overseas, what do they do to ensure the safety of my personal information? Would I have to sue someone overseas to protect my rights if my data is misused? The heart of the matter is this:

[1] Lazarus, David. "A tough lesson on medical privacy: Pakistani transcriber threatens UCSF over back pay," *San Francisco Chronicle,* October 22, 2003.

[2] Informal interviews with legislators, legislative staffers, regulators, and members of the press corp.

[3] McKinsey Global Institute, "Offshoring: Is it a Win-Win Game?" San Francisco, 2003. p. 8.

[4] www.input.com/public/article38.cfm

[5] While "business process outsourcing" is the term commonly used, the key element of the phenomenon is less the outsourcing of process in the sense of subcontracting than the offshoring, the relocation outside the U.S., of processes.

[6] NASSCOM "Indian ITES-BPO [Information Technology Enabled Services-Business Process Outsourcing] Trends." www.nasscom.org/artdisplay.asp?cat_id=800

Is the information as safe abroad as it would be if processed in the United States? How do the technological, administrative, contractual, and legal safeguards and practices in operation overseas compare with those at home in the U.S.? Answering these questions is important because the security of consumer information and the privacy of U.S. citizens in these circumstances cannot be automatically assumed.

In this study we address the questions raised above. Moreover, we answer some broader policy questions about whether to act legislatively, and if so, how.

Our focus is Indian BPO operations. We chose this emphasis because India has emerged as the leading destination of offshored personal data processing activity. We found that security practices of Indian BPO firms compare favorably with data security practices of U.S. financial services institutions.

B. Key Findings

Based upon results from surveys[7] of U.S. and Indian firms, as well as interviews of industry executives and legal experts, site inspections, facility tours, and extensive field research in the U.S. and India, we conclude that *for Tier 1 and Tier 2 Indian BPO firms, sensitive medical and financial data about American citizens is generally as safe and secure being processed in India as if it were being processed in the U.S.*[8]

Finding #1: Driven by concerns for reputation and by the requirements of clients, data security practices of Indian BPO firms favorably compare to data security practices of U.S. financial services institutions.

Indian BPO firms and their U.S. clients have been prioritizing data security and data privacy, and have implemented strong measures to ensure the adequacy of data protection measures. Year over year progress for this four-year old industry is impressive, and continues to improve. To a considerable extent, improvements result from the efforts of clients through monitoring and cooperation. In some instances, vendors themselves have made improvements that go beyond the requirements of their clients.

Breaches appear to be rare. Our survey respondents reported only 12 data breaches during the past three years. Vendors may of course be underreporting, and breaches may be more commonplace than this would suggest. On the other hand, clients, who would be made aware through effects such as fraud claims by consumers, reported very few instances of dismissing vendors or closing specific

[7] Details of our research methodology are summarized in Section XIII below, beginning on page 40.

[8] Although there exists no textbook definition of Tier 1, Tier 2, or Tier 3 BPO firms, from our interviews with industry executives and outsourcing experts, Tier 1 BPO firms are generally understood as having at least 1,500 seats. A seat is the equivalent of a full-time employee. Thus, a firm with 1,500 seats, running three shifts, may have 4,500 full-time employees. A Tier 2 BPO has between 500 and 1,500 seats, while a Tier 3 BPO has less than 500 seats, usually considerably less. Interviews with Indian BPO executives, industry consultants, and NASSCOM staff. June 9-28, 2004. Results may not hold for Tier 3 firms.

offices. Despite this, clients are vigilant and often push their vendors to improve data security practices.

The potential for serious reputational harm that disclosure of breaches would cause is a major driver of security practices for all parties, including Indian and U.S. firms. As one senior executive from a large Indian BPO put it, “In the United States, tens of billions of dollars worth of fraud and identity theft are perpetrated every year. Yet in India, if even a single dollar is stolen as a result of fraud or ID theft, then it becomes a front page story in every major American daily newspaper.”[9]

Finding #2: Leading Indian BPO firms are basing their security programs on internationally accepted standards.

Seventy per cent of survey respondents reported that they were either BS7799 or ISO17799 certified. The two standards are stringent and essentially identical.[10] (See Appendix C for summaries of the “7799” standards.) Needless to say, meeting the requirements for certification does not solve the issue of data security, but it does certify that core security concerns have been addressed. Some U.S. financial institutions also have their own standards which they feel exceed the “7799” standards.

These standards consist of data security practices developed by the International Standards Organization and British Standards Institution. They cover ten major sections including: business continuity planning; systems access controls; personnel security; and security policy. Specific measures include disabling ports and disk drives, maintaining a clean desk and a clear screen, use of ID badges, and security guards. Adherence is verified by an independent third party. Compliance is not a guarantee against breaches, especially as technological changes and ever-improving ingenuity among criminals make a guarantee impossible.

Of those respondents that weren’t certified, nearly all were in the process of becoming certified, with nearly two-thirds of that group in the process of employing an accredited auditor to evaluate their information security management systems during 2004.[11]

The Indian BPO firms we surveyed employed current IT security technologies, including multiple firewalls, intrusion detection systems, and network terminals, usually based on CITRIX or Windows Terminal Server, a network terminal client server system. Network terminal systems generally consist of “dummy” terminals deployed on the vendor side of the process, with the actual applications and data still residing with the client. These practices are not universal. Some U.S. firms

[9] Structured interview with Indian BPO executives. June, 2004.

[10] BS7799 Part 1 was adopted as ISO17799:2000. Certification is provided by third-party auditors. BS7799 Part 2 is a certification program conducted by the British Standards Institution. Only three of the firms we met with had received certification under Part 2 of the standard.

[11] BS7799 compliant information security management systems are being implemented.

report that they have discovered some vendors to be less than up to date with security measures. In general we found that demands by clients drive how extensive and up to date security systems are.

Finding #3: U.S. privacy and security standards are maintained offshore through the use of enforceable international contracts.

The U.S. financial services firms that we surveyed require contracts that provide both for U.S. jurisdiction over disputes as well as compliance with relevant U.S. laws, including The Gramm-Leach-Bliley Act (GLBA), the Fair Credit Reporting Act (FCRA), the Right to Financial Privacy Act (RFPA), the Sarbanes-Oxley Act (SOX), the Federal Debt Collections Practices Act (FDCPA), and the Health Insurance Portability and Accountability Act (HIPAA). U.S. regulators often have access to these vendor firms in principle; contracts and regulatory obligations transferred through contracts give U.S. agencies such as the Office of the Comptroller of the Currency (OCC) the power to audit vendors.

In most standard contracts, data security requirements clearly are defined and monitored with service level agreements (SLAs). Client firms monitor performance and maintain business continuity and data recovery plans in the event of a natural or manmade disaster. *Indian BPOs surveyed reported they assume at least one-year's revenue as a minimum liability requirement.* In conjunction with routine monitoring by the client, contracts and SLAs serve to ensure that data protection measures are adequate.

Moreover, the contract regime that governs privacy and security is effective in the event that a U.S. consumer has a grievance over the misuse of their data. If an Indian data processor misuses non-public personal information concerning a U.S. citizen, that individual has the right to pursue legal action in U.S. courts against the U.S. firm that moved the data offshore.[12] Even though the breach may have been committed by an independent vendor or subcontractor in India, the U.S. firm is liable to its customer.[13]

Finally, should a ruling involving damages come down against a U.S. firm for data breach costs, those costs could then be passed to the Indian BPO vendor by the U.S. firm (assuming the contract is properly structured). Furthermore, some of the Indian BPO firms have assets in the United States, making collection of damages easier. For others, the potential loss of business, including potential business from other clients,serves as an incentive to institute adequate data security measures.

[12] Liability is specified by a host of regulations, depending on the type of information: the FCRA, GLBA, and HIPPA, for example.

[13] As the FFIEC explains, "Compliance risk involves the impact foreign-based arrangements could have on an organization's compliance with applicable U.S. and foreign laws and regulations. An organization's use of a foreign-based third party service provider should not inhibit the organization's compliance with applicable U.S. laws including consumer protection, privacy (Section 501(b) of GLBA), and information security laws as well as Bank Secrecy Act requirements concerning the reporting and documentation of financial transactions." www.ffiec.gov/ffiecinfobase/booklets/outsourcing/15.html. It is for this reason that the FFIEC recommends that financial service providers exercise particular caution when agreeing to clauses limiting the liability of the service provider in the event that the service provider fails to fulfill its obligations (i.e. implementing adequate safeguards to protect consumer data.) "Risk Management of Outsourced Technology Services." FFIEC. November 28, 2000. www.ffiec.gov/exam/InfoBase/documents/02-ffi-risk_mang_outsourced_tech_services-001128.pdf.

Finding #4: Indian legislation and law enforcement practices are not yet aligned with U.S. standards.

Indian data security and data privacy laws are catching up to practices in the U.S. and the European Union. The Indian BPO industry has been responding to considerable pressure from U.S. and European firms to align their cyber crime laws more closely with U.S. and E.U. law, and to bolster their law enforcement efforts. These efforts are at their early stages but moving quickly as law races to catch up with an emerging industry.

Regarding law enforcement, progress is being made. Crimes involving data breaches and ID theft are covered by the Indian IT Act of 2000. The IT Act assigns principal jurisdiction for enforcement to the Central Bureau of Investigation. In March 2000 the Bureau established the Cyber Crime Investigation Cell (CCIC) to handle offences under the IT Act and other high-tech crimes. Similar units have been set up at the state and city levels, both in the state of Karnataka and the city of Mumbai. For example, the Mumbai Cyber Lab (MCL) has trained 108 police personnel in the basic aspects of Cyber Crime. All 83 police stations under the jurisdiction of the Mumbai Police have at least one officer in each police station who has undergone cyber crime training.[14]

To a certain extent, the relative underdevelopment of Indian IT law is not an issue for American consumers, because U.S. law, of course, governs consumer data on U.S. citizens even when processed overseas. Improvements in these areas in Indian law would in most cases, have their greatest impact on Indian consumers. One clear way, however, that changes in Indian law might improve the safety of U.S. consumer data is by making it easier to punish cyber-criminals.

Finding #5: "Captive" data processing done by a wholly-owned subsidiary in India is the most secure model for BPO, but other models are also secure.

The most widely used taxonomy of BPO business models includes four types of firms that vary along a continuum, according to their ownership structure. The first business model for a BPO firm is called "captive," and is a wholly-owned subsidiary of a foreign based firm. A sub-variant of this model is the captive of a U.S. vendor. Firms such as IBM, EDS and Accenture are hired as vendors by financial firms; the former sends the information for processing to its overseas captive. In principle, this model operates largely as a captive, since the principal subcontracting relationship is one of a domestic client and a domestic vendor, with the offshored operation functioning as the captive of the domestic vendor.

The second business model is the **joint-venture**. In this model, both the client and the data processor own a share of the data processing venture.

[14] Data provided by NASSCOM.

Build-operate-transfer, or “BOTs” are the third business model in the industry taxonomy. In this case, a client company contracts with a third-party data processor to ramp up a BPO operation specifically for the client. The client reserves the right to purchase all or some of the BOT at some future date.

The final business model is the independent BPO. These firms are owned and operated by non-U.S. companies, and process data on a contractual basis for a number of clients. Firms such as Wipro-Spectramind, Tata, ICICI, and Infosys are examples of independent BPOs.

Through the “captive” model, financial institutions can maintain a higher degree of managerial control than would be afforded by any of the other three models. The degree of managerial control is the key difference. Other interviewees indicated that through comprehensive contracting and effective monitoring the difference in total security with respect to data processing can be made negligible.

As Indian security improves, there may be a trend in the other direction. Several U.S. financial service institutions with sizeable captive operations in India have begun either spinning off certain business processes previously done in-house, or outsourcing those processes to independent third-party BPOs. This behavior may reflect both the higher level of comfort many U.S. financial services institutions have achieved with outsourcing business processes and the substantial improvements in data security made by the Indian BPO industry.

C. Background

Worldwide sourcing of BPO refers to the relocation of elements of a firm’s information functions such as call centers, customer support, and accounting to anywhere in the world. (Worldwide sourcing can refer to locations both at home and abroad.) These services are performed by a third party (subcontractor), by the firm’s foreign subsidiary, or some combination of the two such as a joint venture. Global networks allow instantaneous transmission of encrypted data throughout the world.

A wide range of activities are being offshored. The trend began with code repair for Y2K and moved into additional outsourcing for low-skill, labor intensive back office work such as data entry, medical transcription, and processing application forms and transactions. The experience of coding for Y2K demonstrated that a skilled pool of labor was available abroad. Driven primarily by wage disparities, many companies had an incentive to relocate to sites such as India and Ireland.[15] Customer relations and help desk functions could be moved to locations where a large pool of competent English speakers could be found. Moreover, call-center jobs are held in higher esteem abroad: employers could expect lower attrition rates and far higher education levels. Increasingly skilled activities have been offshored since, including

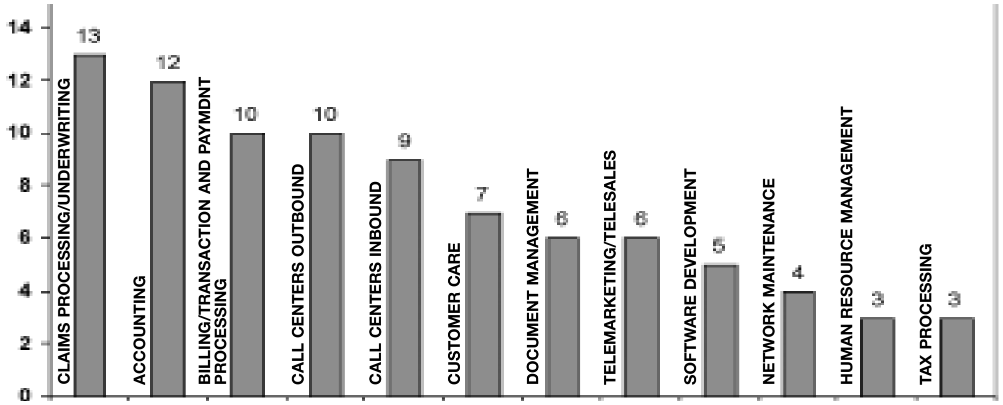
[15] Martin Kenny and Rafiq Dossani, Went for Costs, Stayed for Quality, pp. 17-18.

accounting, human resources, IT support and application maintenance, and software development.

In the financial services industry, the scope and scale of offshore outsourcing has been growing.[16] The range of activities includes: customer service; lead generation; inbound and outbound telemarketing; accounting; insurance claims processing; collections; loan processing; and equity research.[17] Some firms are even beginning to send abroad more sophisticated business functions such as research and credit risk analysis.

The Institute's own analysis is consistent with the findings of a Deloitte Research study on financial services offshoring. As shown in Figure 1, the range of financial services activities now subject to offshore outsourcing is broad. Among those Indian BPOs with U.S. financial services clients, the Institute found claims processing/underwriting to be the most frequently offshored activity, with more than 75% of respondents engaged in this activity. Accounting was the second most frequently outsourced activity with roughly 70% of Indian BPOs undertaking this process. Billing and transaction payment processing rounds off the top three with nearly 60% of surveyed BPOs indicating involvement. Activities involving voice—inbound and outbound call centers, telemarketing/telesales, and customer care—were conducted by 60% of respondents. The more complex processes, such as human resources management and tax processing were far less present among those Indian BPOs surveyed by the Institute, with only 18% percent of the respondents and interviewees indicating they were engaged in such activities.[18]

Figure 1: BPO Activities of Indian Firms Visited On-Site, by type (multiple responses possible)[19]



[16] Rai, Saritha. "Financial Firms Hasten Their Move to Outsourcing," *The New York Times*. 18 August 2004. Section W1-World Business.

[17] *Op. Cit.*

[18] Structured interviews of Indian BPO executives conducted by the Information Policy Institute in Bangalore, New Delhi, and Mumbai India (August 9-28, 2004). These results were supplemented with responses to a survey of similar firms fielded by the Information Policy Institute (June-August, 2004).

[19] This tally is of the 17 tier 1 and tier 2 BPO firms we inspected on-site in India plus three additional firms that provided us with answers to a detailed questionnaire.

A. U.S. Regulatory Requirements

The principal federal law governing financial data flows is the Gramm-Leach-Bliley Act (GLBA). Under GLBA, U.S. consumers may not opt-out of cross-border information transfers of nonpublic personal information to nonaffiliated service providers when the transfer is:

> "…in connection with -- (A) servicing or processing a financial product or service requested or authorized by the consumer; [or] (B) maintaining or servicing the consumer's account with the financial institution…"
> (15 U.S.C. 6801)

Under what is commonly known as the "Safeguard Rule" of GLBA, financial institutions are expected to take safeguards appropriate to the complexity and size of their practice to ensure that consumer data is afforded adequate protection. These steps include the selection and retention of third-party service providers "capable of maintaining appropriate safeguards for the customer information at issue" and specification of these safeguards in all contracts.[20]

Though the Indian BPO industry is very young, offshore outsourcing issues already have been the subject of extensive guidance issued by U.S. regulators. This indicates that U.S. regulators take the risks associated with offshoring seriously. When implementing regulations for the Safeguard Rule of Gramm-Leach-Bliley were issued jointly by the OCC, FDIC, OTS, Federal Reserve Board and FDIC in 2001, they addressed the risks associated with offshore outsourcing by requiring service providers of financial institutions to meet all requirements of the guidelines. Moreover, by attaching the guidelines as an appendix to safety and soundness regulations, bank regulators made it clear that failure to safeguard consumer data is a threat to the safety and soundness of a financial institution.[21]

Bank regulators note that most banks demonstrate appropriate due diligence with respect to the safeguarding of consumer data: "most if not all [financial] institutions already have information security programs in place that are consistent with the Guidelines."[22]

Additional evidence of the importance of offshoring to financial regulators is found in a series of circulars issued by regulators offering guidance to financial institutions

[20] Federal Trade Commission, "Standards for Safeguarding Consumer Information." *Federal Register*. Vol. 67, No. 100. (Thursday, May 23, 2002) pp. 36484-36494. Section § 314.4 (d)(1).

[21] Federal Reserve System Federal Deposit Insurance Corporation 12 CFR Part 30, et al. "Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000. Standards for Safety and Soundness; Final Rule." www.ffiec.gov/exam/InfoBase/documents/02-joi-safeguard_customer_info_final_rule-010201.pdf

[22] Ibid.

engaged in offshore outsourcing. For example, a recent analysis by the Federal Deposit Insurance Corporation (FDIC) identified six principal areas of risk for U.S. financial firms when drafting contracts with offshore vendors[23]:

- Country Risk — those risks associated with political infrastructure, socio-economic conditions, and how changes in each might affect a vendor firm's ability to fulfill its contractual obligations;
- Reputation Risk — risks to earnings or capital arising from negative public opinion, for example, in the event of a security breach;
- Operations/Transactional Risk — risks associated with service or product delivery;
- Compliance Risk — risk associated with liability for legal non-compliance;
- Strategic Risk — risk associated with adverse business decisions, inadequate management; and,
- Credit Risk — essentially, risks associated with the financial condition of the third party provider.

The FFIEC added to the aforementioned areas liquidity risks, transactional risks, and geographic risks.[24] Liquidity risk involves the problems of investment processes and repayment assumptions, and may stem from repatriation and foreign exchange issues. Transactional risk concerns the costs associated with the operation of the venture and implicate the writing, monitoring and enforcement of contracts, and associated problems of dispute resolution. Geographic risk comprises the possibility of manmade and natural disasters.

As the FDIC notes, these risk factors are influenced by a number of issues: the institution, the service provider, the type of function outsourced, and the business model of the contracting relationship (i.e. third-party vs. joint-venture.) To a large extent, the issues faced by a U.S. firm purchasing BPO services do not change when contracting abroad. However, the traditional features of contracting with BPO providers do require additional scrutiny when contracting abroad due the specific risks introduced by an offshore environment.

The categories of risk that a firm must consider are not significantly different from contracting with domestic vendors: due diligence in the selection of a service provider; validation of controls and recovery capabilities; the definition of contractual, service-level, and insurance agreements; and, the definition of management requirements, oversight, and the ongoing process of verifying that contractual obligations are being met.[25] But the differences do require that an additional level of security and monitoring be put in place.

[23] "Offshore Outsourcing of Data Services by Insured Institutions and Associated Consumer Privacy Risks," Federal Deposit Insurance Corporation. June 2004.

[24] Federal Financial Institutional Examination Council, "Outsourcing Technology Service." IT Examination Handbook. (June 2004) www.ffiec.gov/ffiecinfobase/booklets/outsourcing/Outsourcing_Booklet.pdf, p. 30.

[25] BITS Framework for Managing Technology Risk for IT Service Provider Relationships (Washington, DC). November 2003.

In India, contracts are used by U.S. financial firms to compel vendors to comply with relevant U.S. law when handling data on U.S. consumers. The ability of U.S. firms to pass on liability via properly structured contracts, in addition to the reputational effect when a breach has occurred, compel vendors to take additional measures to ensure the adequacy of data security measures and compliance with U.S. law. (Needless to say, regular monitoring of contractual relations is needed, and some U.S. clients have indicated that they had to modify their monitoring practices before an adequate system was instituted. A well-structured contract and monitoring system serves to minimize many of these risks, and through it businesses purchasing BPO services abroad mitigate risks to their consumers.

We found that the contracts in place give U.S. consumers adequate protection in the event that data is compromised abroad.[26]

Our determination was based on the answer to the following sets of questions:

- What contractual arrangements, technical measures, administrative procedures, personnel selection practices, and physical and system access controls are in place to protect consumer data? How are these evaluated? Are these practices adequate to the sensitivity of the data being processed?[27]
- Are breaches of data security prosecutable breaches under Indian law? Is law enforcement capable of dealing with cyber crime? What measures have been taken to improve the Indian state's capacity to address cyber-crime?
- What have been the security experiences of India BPO firms?

B. The Indian IT Act of 2000 and Prosecution of Cyber Crime

One important measure of how well the contract regime functions is the extent to which consumers have been harmed as a result of worldwide sourcing, and whether breaches that result in consumer harm are more prevalent overseas. Measuring breaches is a complicated issue. Measurements must rely largely on self-reports. A breach in and of itself does not necessarily imply consumer harm. Most "breaches" involve incidents such as computer viruses, and do not necessarily involve threats to consumer data. Many of the breaches where consumer data is potentially at risk are rectified before harm to consumers actually transpire. The issue is of course whether the information is comparably safe: is it as safe as it would be if processed by U.S. firms? Part of this question requires that we consider the legal and law enforcement contexts.

The problems related to self reporting are straightforward. Vendors have an incentive

[26] By "adequate", we mean that the likelihood of breaches and the damage done by breaches are not measurably different than those in the United States at least in tier one and tier two BPO firms

[27] This last question is addressed by the Safeguard Clause of GLBA.

to underreport and hide breaches. Clients also are reluctant to report breaches reported to them by their clients. This is not to conclude one way or another on the issue of self-reported breach data. There are indications that breaches are increasing not only in India, but worldwide. Greater awareness of computer systems, rapid increases in the amount of business conducted on-line, and increasingly sophisticated and successful cyber-crimes are all trends that caution against reports of very low breaches at face value. For our survey, respondents reported only 12 data breaches during the past three years. Only three of these reported breaches involved harm to U.S. consumers.[28]

Though the numbers imply that breaches are rare, the costs and likely costs of breaches have led the Indian state to take a number of measures to address the issue. They have issued materials offering guidance on data security, enacted a growing legal code to address cyber-crime, and are devoting greater resources to cyber-crime departments of local and national law enforcement. These are of course developments that are similar to legislative trends throughout the world.

A key factor is whether Indian law provides prosecutors and law enforcement adequate tools to prosecute cyber-criminals. The Indian Information Technology Act of 2002 makes cyber-crimes, including unauthorized use and access of electronic information, federal crimes in the Indian Union. (The Act amends the 2000 Information Technology Act.) The IT Act permits awards of up to 10 million Indian Rupees, or approximately $250,000, for damages resulting from a data breach.

Enforcement is primarily the charge of India's Central Bureau of Investigation (CBI). In response to the concerns of the burgeoning IT sector, the CBI established the Cyber Crime Investigation Cell (CCIC) in March 2002 to investigate crimes covered by the IT Act.

Similar cells have been set up at the state and city level, both in the state of Karnataka and the city of Mumbai. Their training includes:

- A review of The IT Act and what charges can be brought under the Act;
- Computing skills such as networking; and,
- Cyber-forensics, including how to read a server log and trace IP addresses.

In June 2002, the National Police Academy in Hyderabad was authorized by the central government to prepare a handbook on digital evidence handling procedures. One proposed measure is the creation of an Electronic Research and Development Centre of India that would develop new cyber-forensic tools.[29]

[28] Structured interview of Indian BPO executives conducted by the Information Policy Institute during June 9-28, 2004 in Bangalore, New Delhi, and Mumbai, India. Interviews included site inspections and facility tours when possible. Interview results supplemented by results from survey questionnaire of leading Indian BPO firms fielded by the Information Policy Institute with the assistance of NASSCOM during June-August, 2004.

[29] Privacy International, "PHR2004 – the Republic of India."

The Mumbai Crime Lab was established with the assistance of NASSCOM. The lab coordinates and promotes collaboration among the Mumbai police, IT firms, industry groups, academics, and citizens. It participates in cyber crime investigation training for the Mumbai Police Cyber Crime Investigation Cell and serves as a cyber forensic development center for criminal breaches of information security. It also assists in providing resources and expertise for police in other parts of the country.

Anecdotal evidence suggests that these measures have been useful. Last year, for example, a BPO operator was successfully prosecuted for “online cheating” under the IT Act. As a result of his actions, the criminal was terminated from his job, banned from further employment in the BPO industry, and forced to serve one-year’s probation.

Law enforcement efforts targeting Indian cyber-crime are in their early stages. International private-public partnerships such as the SANS Institute and the CERT Coordination Center[30], which are devoted towards information security awareness, have done much to close the gaps between India and the U.S. What can be noted is the fact that the speed of these changes has been considerable. U.S. cooperation with Indian legislators and law enforcement stands to improve the quality of Indian cyber-crime and privacy law and law enforcement.

C. Structuring BPO Contracts

How the use of contracts protects U.S. consumer information in the context of worldwide sourcing can best be understood by way of example. Consider an American firm who sees fit to outsource its outbound telemarketing to a third-party call center located in India. The U.S. firm still is bound by consumer protection laws such as the “Do-Not-Call” list and is liable for violations, even when the violations are committed by an offshore third-party vendor. To limit liability exposure, detailed contracts and SLAs are necessary to ensure that a third-party vendor does not violate the law.

The companies interviewed for this study generally adhered to the standards discussed below. Specifically, among the firms we interviewed it was common for contracts to specify that the vendor be required to give access to any and all performance measurements, audits, or inspections as chosen by the client firm. In one case, this requirement is extended to provide mandatory access for the Office of the Comptroller & Currency of the United States.[31]

As with onshore service provider relationships, the strongest contracts are those that clearly define roles and responsibilities, terms and conditions, and performance

[30] The CERT® Coordination Center (CERT/CC) is a center of Internet security expertise, located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.
[31] Interview.

requirements. A framework generated by BITS, a financial industry consortium, recommends that contracts include the following provisions:[32]

- Take into account business requirements and key factors identified during the Receiver Company's risk-assessment and due-diligence processes. In particular, there are provisions protecting the privacy and confidentiality of consumers' records.
- Include a provision indicating that the Service Provider agrees that the services it performs for the Receiver Company are subject to U.S. regulatory requirements and examination.
- Develop and specify provisions of an exit strategy and for the extrication of consumer data and information on the business process in the event of the termination of the business relationship.
- Provide procedures to ensure that English-language copies are maintained of all contracts, results of due-diligence efforts, regular risk-management oversight, performance and audit reports, and relationship with the Service Provider.
- Include choice-of-law and jurisdictional covenants that provide for resolution of all disputes between the parties under the laws of a specific jurisdiction.[33] Local or outside counsel with offices in the country reviews this as part of the due diligence or RFP process.
- Prohibit the service provider from disclosing or using financial institution data other than to carry out the contracted services; this information should remain the property of the financial institution. This should extend to downstream subcontractors. (If sub-subcontracting is permitted, procedures should be specified.) Any disclosures of nonpublic customer information should be conducted in accordance with applicable privacy regulations. Security measures should also be in place to safeguard customer information.
- Evaluate and discuss what hardware/third-party software and/or third-party tools will be needed by the Service Provider. The contract should specify who will pay for the procurement and licensing of these tools and how export issues will be addressed. Additional third-party services required by the parties also should be set forth along with an understanding of any subcontracting relationships held by the Service Provider.[34]

[32] Excerpted from BITS Framework for Managing Technology Risk for IT Service Provider Relationships (Washington, DC). November 2003.

[33] Note, however, that certain local laws are mandatory and will apply to the contract regardless of the choice of law clause in the contract, such as data-protection laws and limitation of liability laws.

[34] It is interesting to note that, with the exception of recommendations bearing on "choice-of-law" and "jurisdiction issues", even this list of recommendations designed to specifically address *offshore* contracting issues is primarily comprised by concerns that are not unique to *offshore* outsourcing. For example, provisions designed to ensure compliance with U.S. law and regulatory authorities would undoubtedly appear in a contract with a domestic provider of BPO services.

- Specify the criteria for the selection, training and monitoring of personnel, including qualifications, background checks, training, and sanctions for breaches of standard operating practice.
- Outline and institute disaster recovery and business continuity plans that specify procedures in the event of failures to the network and system resulting from human action, infrastructural problems, and natural disasters.

A key component of properly structured contracts with offshore vendors is service level agreements (SLAs). SLAs are contractual arrangements that give U.S. firms a mechanism to specify detailed performance requirements and metrics for their vendors. Individual SLAs within a contract often cover required performance levels, monitoring arrangements, frequency of audits, privacy and security practices, and, in some cases, remedies or procedures for handling any failure to meet contractual requirements.

SLAs not only provide a controlling mechanism for U.S. firms, but they also provide invaluable guidance to Indian vendors of BPO services. The President of one major Indian company noted that SLAs are indispensable for both parties, "SLAs are our lifeblood . . . if you fail on your SLAs, it's curtains."[35]

D. Mitigating Risks involved in Subcontracting

A recent FDIC study argues that the business model with the greatest inherent level of risk involves outsourcing to offshore third-party vendors (e.g. an Indian BPO) who, in turn, further outsource elements of the process to other third-party vendors.[36] They contend that U.S. firms may expose their customers to data security and data privacy risks because of the difficulty of exercising control of these downstream vendors.

Results from the Institute's interviews and surveys indicate that U.S. financial institutions and Indian BPOs implement stringent measures to protect against the risk involved with these sorts of subcontracting arrangements. The Indian BPO firms we interviewed and surveyed responded that they did *not* subcontract business processes involving sensitive customer and client data to other firms. The U.S. firms we interviewed either prohibit the further subcontracting of BPO that involves consumer information to another firm by the vendor or allow it only after they, the U.S. client, scrutinize the arrangements. One U.S. client required a contract between it and the sub-subcontractor. All interviewees, clients and vendors alike, insist that 3rd party subcontracting does not take place without the express consent of the financial institution and their vendor.

Because of the varying risks associated with different business models, U.S. firms restrict certain business processes to specific types of contracting arrangements. For

[35] India Survey

[36] "Offshore Outsourcing of Data Services by Insured Institutions and Associated Consumer Privacy Risks," Federal Deposit Insurance Corporation. June 2004.

example, several executives from interviewed firms indicated that core operations involving either sensitive data or proprietary information would be handled by a captive operation so they could maintain hands-on managerial control.

E. Determining Jurisdiction and Arbitration for Dispute Resolution

Dispute resolution is a key issue in contracts, and no firm wants to find itself in a protracted liability dispute. Two key features of international contracts that are crucial to offshore BPO relationships are the clauses addressing “choice-of-law” (jurisdiction issues) and “arbitration“.

BPO contracts are generally subject to U.S. jurisdiction. Indian BPOs indicated that almost all contracts with U.S. clients specify that U.S. law applies and names the U.S. as the jurisdiction and venue for dispute adjudication.[37] Moreover, many U.S. firms only conduct business with offshore vendors with “significant U.S. assets”. Further, many of the vendor firms we interviewed do in fact have “significant U.S. assets.”[38]

Arbitration clauses are another way that U.S. firms use contracts to protect themselves in the event of a breach. Arbitration clauses are agreements to have disputes settled outside of court according to predetermined rules. The United Nations Convention on the Recognition and Enforcement of Foreign Arbitral Awards (the New York Convention) covers arbitration agreements. More than 70 countries, including India, recognize and enforce foreign awards as parties to the New York Convention. This process is generally far less expensive than traditional legal proceedings, and is very common when contracting across borders to developing countries. Most of the firms interviewed include arbitration clauses in their contracts in the event of contractual disputes. However, we did not find an example of a dispute that had reached arbitration proceedings, suggesting that contractual arrangements between financial institutions and BPO vendors are working.

The absence of a treaty between the United States and India under which judgments rendered in U.S. courts would necessarily be upheld in Indian courts and vice-versa remains a potential problem for cross-national contracting. The lack of reciprocity in judgments potentially suggests that judgments obtained in U.S. courts over contractual disputes would have to be re-submitted to Indian courts and reconsidered with reference to Indian law. This could be problematic since Indian law has different limits than the United States on damages obtained in civil cases. Of course, the concern is moot if the Indian vendor has sufficient U.S. assets to cover the claim, hence the premium placed by U.S. firms on finding Indian vendors with “significant

[37] In one instance, the contract was signed with the client’s European subsidiary, and the contract specified a Western European jurisdiction.

[38] Institute Survey. One of the firms actually replied that they “did not” have significant U.S. assets but as their parent company is a U.S. firm, they appear to, from a legal perspective, have “significant U.S. assets.” The notion of “significant U.S. assets” is not formal but generally refers to the notion of assets sufficient to cover damages in the event of a contractual dispute.

U.S. assets.” We did not find any instance of such a dispute, and the problem remains hypothetical to the best of our knowledge.

To our knowledge, Indian courts have yet to hear a case involving indirect damages: that is, a case where a consumer successfully sought damages from a financial services firm for harms resulting from the behavior of a BPO vendor, where the financial services firm in turn sought damages from the vendor firm.

CERTIFICATION TO INTERNATIONAL STANDARDS

Indian firms commonly seek certification under international standards for computer security; notably, the ISO 17799 and the BS7799. They also employ other internationally recognized standards for software quality and management practices. Certification processes are lengthy, involve detailed criteria, and require third parties to verify that a vendor meets the standards. These independent audits provide a means by which companies can attest to conformity with international standards.

The standards apply to specific domains. For example, the Carnegie Mellon's Software Standards Institute's Capability Maturity Model (SEI CMM) standards were established by the Department of Defense for subcontractors to ensure software performance. The Customer Operations Performance Center's COPC-2000® Standard covers contact center operations. Six-Sigma certifications assure a firm's process produces fewer than 3.4 errors per one million operations. The American Institute of Certified Public Accountants' Statement on Auditing Standards 70 audits an organization's control activities, including controls over information processes.

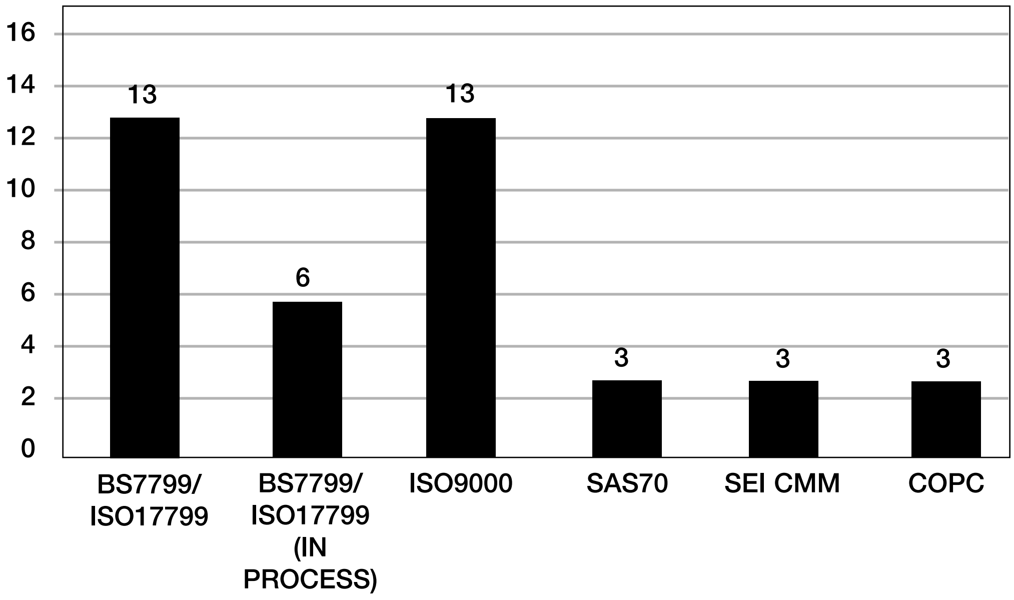
The "7799" standards issued by the International Organization for Standardization and the British Standards Institution provide codes of conduct for information security. It should be noted that some firms may choose not to seek certification. Large American companies have their own list of information security criteria which comprises the large bulk of "7799" but also add their own concerns.

With this caveat, "7799" standards provide for a firm's administrative control environment and activities, methods of assessing risk, information and communication processes, and monitoring capabilities and practices. And it requires that these practices be tested through drills and disaster recovery exercises. The 7799 series (the ISO17799 and BS7799) provide "a comprehensive set of controls comprising best practices in information security". The ISO17799 and part I of the BS7799 are essentially identical. A more recent iteration of the BS7799 standard, issued in 2002, specifies the process under which a firm can certify its information security management system. In general, third-parties can certify that a firm conforms to the provisions of "7799" standards.

In our interviews and surveys, we examined the extent to which vendors are certified. Our primary focus was on the level of certification for data security. We found that most large multinational clients have their own internally developed security standards which mirror to a large extent those of BS7799.

As indicated by the following chart, almost all of the firms that we visited were BS7799/ISO17799 compliant or were in the process of becoming so. Three firms were SAS 70 audited (though client firms are far less likely to look for SAS70 audits than they are for BS7799/ISO 17799 certification); three were SEI CMM certified; and three were COPC certified. In addition, several firms have employed Six-Sigma techniques to raise the quality of security implementation.

Figure 2: Certifications by Type (number of firms)[39]



[39] This tally is of the 17 BPO firms we inspected on-site in India plus three additional firms that provided us with answers to a detailed questionnaire.

SPECTRUM OF THREAT TO PERSONAL INFORMATION

A. Data Might Be Improperly Accessed – Data Security

The security of data refers to how well data is protected from being lost or improperly accessed. Security measures generally include (1) access controls that monitor who accesses information, or (2) how information is recovered and restored in an emergency. Measures to protect security generally are divided into two different categories:

1. *Physical Security* is concerned with protection of physical assets of the data processing center. Types of physical security practices include coded ID tags for access of personnel, and bomb proofing of building complexes where information is either processed or stored.

2. *Administrative (or Logical) Controls* are designed to limit, monitor, and control the universe of persons and automated processes that have access to various types of information. For example, a password system that lets outsourcing workers login only to the applications and data sets of a single outsourcing client would be considered preferable to any online login system that allows a unique login ID for access to any number of different customer applications.

B. Data Might be Seen or Used by the Wrong Party – Data Confidentiality

Keeping the confidentiality of data is the act of ensuring that only those legitimately granted access can see personal information and that anyone legitimately granted such access to personal data uses it only for the purpose for which such access was granted. A successful structure will ensure that persons with access to social security numbers or other personal information cannot provide this information to organized crime to perpetrate identify theft. In general, measures to protect confidentiality involve both administrative and human resources (HR) measures, as follows:

1. *HR measures* are designed to ensure that persons given responsibility to handle personal information are not tainted by any background issues that might indicate a criminal record, susceptibility to blackmail or other types or coercion.[40] Background and criminal checks, e.g. police arrest records, are an essential element, but there are supplementary administrative measures that are in use as well: (1) extensive testing; (2) handing over of authority and access only gradually; and (3) personality assessments.

[40] An example might be a bank policy that would discourage hiring compulsive gamblers because their inevitable pile of debt would provide a very powerful motivation for engaging in theft of funds.

2. *Administrative measures* are actions taken to ensure limited access to information, or to allow regular audits and other measures to verify that the data has been used correctly and not compromised. For example, it is common practice today for the first 5 digits of a customer's social security number be made invisible, even to employees engaged in processing very personal information. The general theory behind administrative measures to protect confidentiality of data is that as much as possible, the information system is configured to limit access to data and applications to a need-to-know basis.[41]

C. Data Might Be Corrupted or Made Useless – Data Integrity

Whether or not data is protected, or regardless of how it is used, there always is a question of its fundamental correctness. Data can lose its integrity through a variety of mechanisms, but primarily through (1) corruption and (2) human error.

1. Corruption can occur when there is a failure in the information system such that data is changed improperly. For example, disk errors could result in data being written improperly. Other problems, usually far more serious, can occur when malicious code (viruses, worms, Trojan horses) somehow gains access to the system and corrupts the data files. Protection against data corruption is a technical matter, handled by the operating system and supplementary utilities. Virus protections and patches must be updated regularly. These measures are available regardless of where the system is located, i.e., whether in India or the U.S.

2. *Human Errors:* It is estimated that in any data entry job, there is a measurable error rate. The effect of this is that no organization can be 100% sure that its data is completely accurate. There are many measures taken to ensure data integrity. These include (1) system interface designs that may use a system of rules to prevent employees from entering invalid data. (For example, if one enters "100A2" into a zip code field, it will be rejected). (2) Checks and verification for human error in which steps are taken to double-check information.[42]

[41] Since, however, organizations tend to have very large amounts of sensitive data, there can be a very large administrative burden involved if the organization needs to distinguish different classes of users who have access to data, and provide to these classes separate levels of access to information, e.g. [for each class of users] "You can see this, but you can not see that; you can change this, but you can not change that."

[42] Since this by necessity is a labor-intensive job, and thus more costly, the advantage goes to low-wage countries. Cheaper labor allows economies of scale that funds additional personnel to reverify entries, thereby reducing the chances of error. (Having such a system in place reduces the chance of recommitting the error considerably, to 0.09 %.)

PERSONNEL SELECTION, TRAINING AND MONITORING

One of the great attractions of sourcing in India is the sheer availability of human resources. Jobs such as data entry, telemarketing, or programming are highly sought after in India, and are performed by the better and brighter graduates from leading schools in the country. Pay in this sector is considerably larger on average than in other sectors.

Personnel selection, security training, and monitoring are therefore a core competency of information security. In the firms we surveyed, the few breaches that took place usually involved employees.[43] Indeed, approximately 70% of the information security breaches of personal information that take place in the industry are "inside" jobs by employees.[44]

A. Selection

Background checks in India are generally more invasive than in the U.S. They can include visits to the home and family, questioning of neighbors, and verification of school activities. The hiring process is also lengthier because of these checks. (One company in India reported that the background check for a new hire takes 30-45 days.)

The invasiveness of background assessment practices are meant to compensate for the lack of easily accessible information, such as credit histories and criminal information. (There is no central criminal database in India and credit registries are recent and limited to a small set of consumers.) Conditions of underdevelopment make a comprehensive and fully accurate check very difficult, and this fact explains the personnel selection procedures employed by many of the leading firms. Some companies conduct the background checks themselves, but most Indian companies and U.S. captives use a third-party that specializes in vetting and criminal background inspections. These are Indian firms which screen new hires, often going through their financial and social history. These checks are invasive, but the extensive intrusions are to make up for the lack of easily accessible information about an individual.

Background checks usually begin at the candidate's schools with on-site verification of records and interviews with school authorities. All the companies interviewed conducted educational checks that generally include interviews of professors and school administrators. Likewise, companies verify the actual residence of the applicant, often by an in-person visit to the listed address.[45] It is important to note, however,

[43] Two companies reported breaches which consisted of employees memorizing credit card numbers.

[44] This finding was reported by Judith Collins of Michigan State University. "Stop, thief! Protecting Employee Records from Identify Theft - IHRIM Webinar Focuses on the Fastest Growing Crime in the U.S." www.emediawire.com/releases/2004/7/prweb138756.htm

[45] Nine of the companies interviewed required new hires to sign NDAs that cover client data and intellectual property. Some firms also conduct drug tests.

that it is required that employees work through a full notice-period, of 1-2 months before an employee quits.[46]

Criminal background checks are more difficult to execute in India than in the United States. This is in part due to poor record keeping, the absence of computerized systems in many areas, and difficulty accessing the records that do exist. In the U.S., a host of information services, like Accurint or AutoTrackXP, provide access to public record data and address histories. Others specialize in the provision of public record data, and conduct on-line searches of various state and local criminal data bases.

Instead, in India, investigators go to locales listed by employees to verify addresses and to local police officials to uncover any criminal past. The procedures are lengthy, and poor record keeping limits its thoroughness and accuracy. For this reason, criminal checks were conducted by only three of the firms we visited. Four others conduct them only at the request of the client. Of course, given the limited effectiveness of criminal background checks, their value is limited.

Passport checks may be used as a proxy for a criminal background check because passports are never issued to those with criminal records. There is an issue of timing, namely, the period between the issuance of a passport and being hired must also be examined.

The use of third-parties for background checks in not without potential problems. Given the relatively lucrative nature of the BPO jobs relative to police work, there are opportunities for applicants to bribe investigators in order to pass the checks. Some clients have been informed by their vendors of instances of payoffs.[47]

To cope with the remaining potential problems with personnel, the industry in India is considering moving towards the use of “Grey Lists” that identify risky employees.[48] The lists have been proposed by NASSCOM to serve as an additional safeguard. This proposed system, however, would at first have to rely on the relatively small size and geographical concentration of the BPO sector in India and low labor mobility. As the number of firms grows and as they become more dispersed throughout the country, lists may become more difficult to maintain and access.

[46] In the case of a disgruntled or unhappy employee, this practice poses some risks.

[47] Of course, for the BPO firms any misbehavior on the part of the employee, including the falsification of a resume or any other related documents, leads to immediate dismissal.

[48] To date, this is a proposal for the maintenance of a list of name of employees that have been deemed to be risks based on their behavior and fired. Another suggestion would create a data base which employees and potential employees would opt-in to. As “envisioned, the program would allow tech workers, either those with jobs looking for new ones or people trying to get one, to voluntarily register in the database, said NASSCOM Vice President Sunil Mehta. The registry would be administered by a third party, who will hire a professional reference-checking company to conduct background checks on the workers.” Patrick Thibodeau, “Firms in India Seek Better Background-Check System.” ComputerWorld. April 18, 2005. www.computerworld.com/managementtopics/outsourcing/story/0,10801,101141,00.html?source=x50.

Personnel issues, especially the problem of determining security risk, are perhaps the system's weakest point. The fact that jobs in the sector pay relatively well provides an incentive to employees to do what it takes to retain their positions.

B. Training, Certification, and Testing

Indian firms place emphasis on testing and training. Given that liability is passed down through contracts, BPO firms have a strong incentive to regularly train and monitor employees. Moreover, to the extent that there is lower job turnover in India, the benefits of training are better captured, and incentives to bear the costs of training are greater.

In the Indian firms we visited, workers were given general courses on data privacy and data security, as well as project specific training that covers the implementation of privacy procedures. Where appropriate, workers are made aware of the processor's legal obligations. And steps are built into the process to ensure compliance with the applicable law. There is a review of each of the required processes for a project to remain in compliance with U.S. privacy laws. Furthermore, project specific directions cover privacy policies.

Among those Indian BPOs processing data for U.S. financial services companies, most conduct a review of the required processes for a project to remain in compliance with U.S. privacy laws. Eleven of the firms had ongoing testing and re-testing programs for their employees. Follow-on training comprised classes on new regulatory obligations, pop quizzes, and updated security information on screen savers. Regular examinations are common, though time periods vary. For some firms, tests are sporadic, taking place only with process changes, but some retest as frequently as every 6 months. Most use a company intranet regularly to keep employees updated on security issues. Clients can and do specify the content of training and, in fact, this aspect is sometimes included in the contract.

C. Monitoring of Employee Compliance

In India, there are few legal barriers to monitoring employees, and workers in the firms we inspected were heavily monitored. We found closed circuit television in all 14 firms we visited, and guards posted at the relevant sections of the building. In 11 of the 14 firms, there were separate client facilities. In 6 of the 14 firms, we were able to assess the supervisor to employee ratio. And for these 6 firms we found an average of one supervisor for every 14 employees. In all cases, clients and their relationship managers are able to listen in on call center operations.

The following table (Table 1) lists the personnel security features we found at the 14 firms we visited. All of these firms conducted background checks, and trained their employees on security issues, including project specific concerns and procedures. The use of temporary employees was very rare. And most regularly tested employees on security issues. The table also shows that criminal checks remain infrequent for reasons mentioned above, namely the absence of centralized criminal information.

Table 1: Personnel Security (N=14)

	Background checks	*Background checks include criminal records (◆ = when requested by client)*	*Employees required to sign non-disclosure agreements*	*Hire temporary employees for specific projects*	*Training includes security and privacy responsibilities*	*Employees required to understand project specific responsibilities (e.g., FCRA, Sarbanes-Oxley)*	*Regular drills and tests for employees*	*Component of hiring process outsourced*
Company A	➼	◆	➼		➼	➼		
Company B	➼				➼	➼	➼	
Company C	➼		➼		➼	➼	➼	
Company D	➼		➼		➼	➼		
Company E	➼	➼			➼	➼	➼	➼
Company F	➼		➼		➼	➼	➼	
Company G	➼	◆		➼	➼	➼	➼	
Company H	➼				➼	➼		➼
Company I	➼	◆	➼	➼	➼	➼	➼	➼
Company J	➼		➼		➼	➼	➼	
Company K	➼		➼		➼	➼	➼	➼
Company L	➼	◆	➼		➼	➼	➼	➼
Company M	➼	➼			➼	➼	➼	
Company N	➼	➼	➼		➼	➼	➼	➼
TOTALS	**14**	**7**	**9**	**2**	**14**	**14**	**11**	**6**

Although Indian companies are eager to adopt the levels of security required by their customers, they may not be as experienced as their counterparts in the U.S in doing so. Input by the client on security matters compensates for this lack of experience.

Where data resides at the vendor firm, companies often begin network security by replicating the client's network practices "as is" unless otherwise specified in the contract. This includes all desk practices and personnel policies (for example, access to recording devices or the scope of background checks). If the vendor's network security policies are more stringent, then the tougher standard is used.

The firms we visited usually send information over international private leased circuits (IPLC); some also use Virtual Private Networks (VPNs) over the Internet. An IPLC is a dedicated circuit used only by the company leasing it. In contrast, the VPN uses the Internet but with encryption, digital certification, and other security mechanisms to simulate a private network that can be accessed only by authorized users. Six of the firms interviewed used VPNs. (Transmissions were encrypted as a matter of course.)

In addition to the use of firewalls and other standard security practices, some companies use a Demilitarized Zone (DMZ) approach to insulate their core systems from "trusted servers" facing the public Internet.[49] Four of the firms we visited noted they used a dual firewall system. All but one of the firms visited confirmed the use of an intrusion detection system (IDS) to monitor all incoming and outgoing network transmissions, which looks for data transmission patterns that are out of the ordinary. Virus counter-measures are universal, and virus definitions and other security patches are updated as they become available.

Five of the BPO firms in India maintained extensive access logs of processes, agents, locations, times of log-ons and log-offs, and security alerts. One company claimed that it maintained a log online for 3 months and logs on disks for 3 years.[50] For some firms, file level access is not generally kept, though it can be reconstructed if necessary. Interviewees all claimed that they had the ability to generate complete audit trail for breaches within 6 months of the breach.

Those interviewed indicated an eagerness to adopt whatever security technologies were needed in order to maintain very high levels of security and reliability. Some client firms suggested that reaching these levels of security require them to push vendors to adopt ever more stringent measures, and one suggested that in the absence of its insistence, security would be too lax. By contrast, one vendor indicated that it refused

[49] A "trusted server" is one where the receiver/transmitter is sure, via certification and other authentication measures that it is in fact the server that is the intended recipient/sender.

[50] One client reported an instance in which a vendor had failed to do so. This failure led to changes in how the client monitored the vendor.

to take on a client because it was concerned that the latter's security practices would expose it to too great a liability. Generally, both clients and vendors reported best results when both share responsibility for data security and coordinate efforts.

Finally, it is common for client firms to maintain relationship managers on the ground at vendor operations to monitor the activities of the latter. A relationship manager is an employee of the client firm that oversees the activities of all contractors. In environments in which clients can face substantial liabilities and loss of reputation in the market, the regular monitoring of a vendor's security practices is sound business sense.

SYSTEMS ACCESS

A "trusted server" is one where the receiver/transmitter is sure, via certification and other authentication measures that it is in fact the server that is the intended recipient/sender. One client reported an instance in which a vendor had failed to do so. This failure led to changes in how the client monitored the vendor.

Many vendors maintain at least two levels of access controls: first, to the network, and next, to the application. As noted above, clients increasingly are retaining control over access to the network on which data and applications are kept.

We found a strong focus on password expiration policies among the vendor companies. In most companies, passwords log on to the vendor systems, but additional passwords are needed to access the data and applications. At some, three unsuccessful logins will lock out access to the system and applications. Passwords expire at regular time intervals, and new ones are allocated. Interviewees told us that sharing of passwords is prohibited, and violations of this prohibition are disciplined. Of nine firms that provided the data:

2	firms retired passwords every 2 weeks
3	firms retired passwords every month
3	firms retired passwords every 45 days
1	firm retired passwords every 2 months

All of the interviewees claimed that they had never been the victim of an external hack. Where breaches had occurred, they were committed by rogue employees.

To limit breaches, clients themselves or third-parties hired by the client historically have conducted vulnerability analyses. Vulnerability analyses might include "ethical hacks" whereby a third-party attempts to hack into the system but solely for the purpose of identifying vulnerabilities. Other aspects of such reviews might include analyses of IT security practices and processes.

Another trend is adopting measures that prevent any transfer of data outside of the U.S. More U.S. firms no longer transfer data, but instead rely on terminal-type solutions, including access technologies such as Citrix and Windows Terminal Server. Indian information workers access the database and applications remotely, but the data resides with the U.S. financial institution. They cannot download the information onto their servers in India, nor do vendors use applications at their locations to process information. Remote access leaves control over security in the hands of the U.S. firm.

Of the 14 firms we visited, nine stated that they relied almost entirely on remote access programs to access the data they processed, four stored information and remote accessed data in roughly even combination, and only one stored all the data in process on site with the vendor. Of the large U.S. clients that we interviewed, one did not allow any external access into their system. Instead, data was extracted and encrypted to a CD before being sent overseas. The data is then “peppered” with other security measures that will indicate if it is abused.

Remote access applications also are used by captive subsidiaries of many firms. One firm used Citrix for its captives in India, Ireland and Canada. Another firm reported it was using the same technique for all data access, whether conducted overseas, or in the U.S.

A common security component is to design processes that restrict data according to “need for use”. This means that an information worker can access only that data necessary for the specific task they are performing.

Table 2 below summarizes the data access policies of the 14 firms we visited. Only one of the fourteen outsources any aspect of their network security, and it outsourced it to the client firm. Generally, all the firms restricted access to data and applications.

Table 2: Data Access Policies (N = 14)

	Data and Applications Accessed Remotely (e.g., Citrix, Windows Terminal Server)	Data stored on site (not exclusive of remote access)	Recording devices restricted	Data Access log kept for at least 6 months	Outsource aspects of network security	Access restricted to project only Regular drills and tests for employees
Company A	➽	➽	➽	➽		➽
Company B	➽		➽	➽		➽
Company C	➽		➽	➽		➽
Company D	➽	➽	➽	➽		➽
Company E	➽		➽	➽		➽
Company F	➽		➽	➽		➽
Company G	➽	➽	➽	➽		➽
Company H	➽		➽	➽	➽	➽
Company I	➽		➽	➽		➽
Company J	➽	➽	➽	➽		➽
Company K	➽		➽	➽		➽
Company L	➽		➽	➽		➽
Company M	➽		➽	➽		➽
Company N	➽		➽	➽		➽
TOTALS	**14**	**4**	**14**	**14**	**1**	**14**

Local physical security

While our visits were expected, physical security appears to be stringent. Discussions with U.S. clients suggest that these procedures are generally effective but that surprise visits can occasionally reveal that practices are more lax. (These lapses can lead to stricter client control.) On the other hand, one U.S. firm we interviewed told of an instance in an Indian subsidiary in which the firm's CEO was denied entry because he had forgotten his identity card.

The facilities we visited had strict access controls. Eleven of the fourteen companies we visited maintain physically separate client areas. Employees usually are dedicated to only one company at a time, and employee training includes client-specific policies. All of the 14 firms employed closed circuit television to monitor client areas, and movement from one client area to another is generally restricted. In addition, we observed security personnel devoted to specific client areas.

Data removal is a major concern. Various policies are designed to ensure that data is not taken or transmitted off-site. For example, firms generally prohibit employees from carrying into work any pieces of paper, pagers, cell phones, or other personal electronic devices that could store information. It is also very common to disable digital interfaces such as USB ports and disk drives, unless authorized by the client. Internet access is usually restricted, as employees cannot access sites outside of the system facility. Print screen functions are commonly disabled, and access to printers is restricted.

This system is not foolproof. In three instances, unscrupulous employees were able to compromise information. But in all three cases, they did so by memorizing account data. And such methods of theft do place considerable limits on the amount of data that can be stolen.

In some instances, large amounts of paper documents are sent overseas so that the data they contain can be keyed into the client's information system. If chits (or other paper-based records) are used in the offshore location, then after data entry has finished, procedures must be in place to ensure that the paper copy of the data remains protected. The companies performing these services in India reported a range of policies regarding handling, storage, and secure destruction of documents. In some cases, the paper is shredded immediately under the supervision of a relationship manager. In other cases, the paper is stored and kept on the shelf for a year as a matter of policy.

One firm bypassed this problem altogether and used scanned (image) files to enter data from paper originals. In the event that the image on the screen is not legible, hard copies were printed. This “clean desk” policy ensures no documents are accessible when the employee is not working with them, and digital files are destroyed (or returned) after they’ve been used.

Core physical security policies, as Table 3 summarizes, are common across the 14 firms we visited. Monitoring and clear desk policies are in place in all of them. And separate client environments are found in most of them.

Table 3: Physical Security (N=14)

	Video Monitoring (Closed Circuit TV)	*Separate Client Environs*	*Clear desk rule*
Company A	➼	➼	➼
Company B	➼	➼	➼
Company C	➼	➼	➼
Company D	➼	➼	➼
Company E	➼		➼
Company F	➼	➼	➼
Company G	➼	➼	➼
Company H	➼	➼	➼
Company I	➼	➼	➼
Company J	➼		➼
Company K	➼	➼	➼
Company L	➼	➼	➼
Company M	➼		➼
Company N	➼	➼	➼
TOTALS	**14**	**11**	**14**

B. Business Continuity and Disaster Recovery

Disaster recovery procedures are specified in contracts. Moreover, conformity to "7799" standards requires that drills be run to test business continuity and disaster recovery procedures.

Disruptions and disasters can include a host of contingencies: power outages, earthquakes and even the possibility of a regional war. Contingency plans to recover data and maintain operations are a crucial element of consumer data protection. These issues are extensively examined by both vendors and clients because such disruptions can have a considerable impact on costs, reputation, and liability.

In developing societies, unreliable electric power is a significant issue. For example, one interviewee maintained that several "line-cuts"—disruptions in the power provided by public utilities—had occurred during the course of a short visit to their facilities. Indian BPO companies generate their own power and all the facilities we surveyed had multiple power back-up systems. Such redundancy is a standard part of operations. These measures appear to be effective: all the companies we interviewed claimed that due to these measures, they had not experienced a power failure.

The firms we interviewed all had at least one backup processing center. It is common for firms to maintain backup centers both in the same city and in another Indian city. One vendor firm also kept a facility in South Africa in the event of regional catastrophe. Many of the Indian vendor firms we interviewed had or were in the process of acquiring facilities in North America, Eastern Europe, and in Southeast Asia, partly for reasons of expansion and partly for reasons of contingency planning in the event of war.

Disaster recovery drills and assessments are common. Two firms ran drills each quarter, and one of these drills was conducted with the assistance of one of its largest clients. It involved a process shut down, data transfer, and personnel relocation to an alternate site. Four firms ran drills every six months to test for disaster recovery and business continuity.

Client firms also take measures to insure business continuity and disaster recovery. The U.S. client firms we interviewed keep backup centers in the U.S. or have business continuity contracts with a processor in the U.S. One client firm had capped the amount of data it sourced to half in order to maintain redundant facilities in the United States.

Interviewees described a number of cases where these plans had been put to use. In one instance, following an earthquake, data and staff were transferred to an undamaged facility in the same city with only a brief disruption to processing. In another case, data was transferred to another city following terrorist attacks in Mumbai. The attacks had prevented much of the staff from getting to work. In a third instance, workers and families were relocated after flooding in southern India.

In all of the firms we interviewed, the maintenance of excess and redundant capacity is a high priority. The firms we interviewed claim that this excess capacity is important for both maintaining data security and business continuity.

Redundancy is used in other facets of infrastructure. One company had communication lines that ran through both the Pacific and the Atlantic Oceans. When connectivity was through a virtual private network, it used two separate service providers, each serving as a backup for the other. Another maintained both satellite and fiber-optic connections.

ADMINISTRATION OF SECURITY

Interviewees described the administrative apparatus for security as generally comprised by an information security committee or council that drafted policies, monitored security and privacy practices, and revised policy as needed. This monitoring takes place in addition to the audits performed by the clients that hire the firms. (One firm averaged an audit every 3 weeks.) Information security committees consisted of the Chief Technology and/or Chief Security Officer, the Vice President of Human Resources, and the Head of Operations, and often included the CEO. Furthermore, the firms we interviewed ran security drills, although their frequency varied from firm to firm. These drills simulate data breaches, or physical disruptions that would involve the migration of staff and data to secondary facilities.

Legal requirements, contractual obligations, liability, standard IT concerns, and market reputation all serve to make data privacy and security a core aspect of BPO relations. This institutionalization takes the form of dedicated departments within the firm and regularized assessments of data security and privacy measures.

For captives, security policy is established in the home country. Local teams of top managers ensure compliance with the policies established by the parent. Reports and audits of captives by the parent firm are regular. In one firm, the committee received weekly metrics of privacy and security, in addition to overall performance analyses, which are shared with the parent in the U.S.

Table 4 summarizes our findings on the administration of security and drill practices. Internal risk assessments are conducted by only five firms, but it should be noted that clients as a matter of selecting vendors are obliged to assess risk by U.S. regulations. Many vendors use client assessments.

Table 4: Administration of Security and Practice Drills (N=14)

	Has a Chief Security Officer	*Formal body in place to assess security and privacy issues*	*Conduct regular risk assessments (independent of assessments by clients and insurance firms)*	*Practice security procedures/drills*
Company A	➽	➽	➽	➽
Company B	➽	➽		➽
Company C	➽	➽		➽
Company D	➽	➽	➽	➽
Company E	➽	➽		➽
Company F	➽	➽		➽
Company G	➽	➽		➽
Company H	➽	➽	➽	➽
Company I	➽	➽		➽
Company J	➽	➽		➽
Company K	➽	➽	➽	➽
Company L	➽	➽	➽	➽
Company M	➽	➽		➽
Company N	➽	➽		➽
TOTALS	**14**	**11**	**5**	**14**

LEGAL DEVELOPMENTS IN THE U.S. AND INDIA

Indian lawmakers are seeking to enhance the overall privacy protections afforded Indian citizens, without unduly increasing compliance costs for Indian and multi-national corporations. NASSCOM and the U.S.-India Business Council recently completed a “gap analysis”, which examines common types of cyber crimes and attempts to determine what existing Indian laws are applicable.[51] The crimes considered include: identity theft, stolen credit card data, and the use of “marketing” data to deny services such as credit and insurance. Protections for Indian consumers do appear to be modest and with the exception of “The Information Technology Act of 2000”, appear to fall under the jurisdiction of broad laws that predate the growth of the Indian information technology enabled services industry.

Indian legislators are expected to enact a number of measures designed to close these gaps. This is not likely to involve the creation of a new stand alone Indian Data Privacy Act, but will focus on modifications to the Information Technology Act of 2000.

The elements of existing E.U. and U.S. privacy law that are receiving the most consideration from Indian lawmakers involve:

- the concept of “data controller”;
- the minimum level of standards necessary for domestic contracts;
- the appropriate choice mechanisms to apply to various sensitive information flows, including financial data.

Indian lawmakers and legal experts appear to agree there is no need for static transborder data flow standards. Already it is possible for two firms party to a contract to enhance the standard of data privacy protection by changing contract terms, rather than relying on legislation. Indian lawmakers appear to intend that the focus of new legislation be Indian consumers.

[51] U.S.- India Business Council internal analysis, Rick Rossow editor.

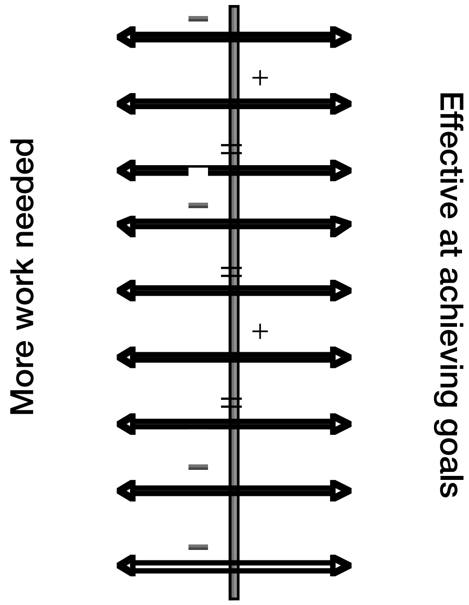
CONCLUSION

As far as we can ascertain, breaches of sensitive client data (account number, identifiers, PIN, etc.) are rare. The apparent infrequency of breaches stems primarily from three factors: well structured and well monitored contracts; the reliance on international data security standards; and, fear of being punished by the market in the event of a breach. The means employed may differ, but through different combinations of practices, security in leading Indian BPO operations is comparable to that found in leading U.S. firms.

The following figure summarizes our assessment of key aspects of the data security and privacy environment in India.

Background Checks	C
Training	A
Network access controls	A-
Disaster recover	B+
Systems access security	A-
Physical access security	A
Administration of security	A
Law enforcement/ Criminal investigation	C
Regulatory efficacy	D

Relative to practices in the US



An industry sponsored awareness campaign aimed at those looking for an offshore vendor. Studies that examine what factors to consider when selecting and managing and information services provider exist. For example, BITS, the business strategy and technology division of The Financial Service Roundtable has looked at these issues. Industry campaigns can help to disseminate this kind of information. The campaigns would make companies aware of the technological, logistical, and legal issues that they should keep in mind when selecting a vendor, especially those which concern personal data security and privacy.

Model offshore outsourcing contracts should be made easily available to U.S. firms looking to source globally. Model contracts are avaliable and are increasingly being propagated. Nonetheless, given the crucial role of contracting in securing personal information, wider dissemination can only help. Each industry should develop and promote suggested contract language for the data privacy and data security sections of BPO contracts. These sections should address each requirement mandated by U.S. law on consumer information.

Improve coordination between U.S. and Indian law enforcement agencies. INTERPOL has a section on information security crime. But as economic ties between the U.S. and India grow, especially in information technology enabled services, stronger bilateral ties between U.S. law enforcement and Indian federal police sections on information technology crime can help to improve the performance and capabilities of the latter. Indian police infrastructure concerning information technology related crimes is only now being developed. The assistance of U.S. experts can accelerate the development of this infrastructure and assist in the investigation and prosecution of crimes involving personal consumer data.

Form an inter-governmental working group on policy development and coordination in order to develop greater "policy coherence". The formation of a public working group comprising American and Indian regulatory officials, along with industry representation and consumer groups on both sides, can help to improve the development of Indian law in its early moments and help to develop processes and regulations that minimize the possibility of regulatory conflict. The involvement of experts with the benefit of experience in advanced market societies can help to accelerate the development of better laws and regulations in places such as India.

APPENDIX A: METHODOLOGY

Our assessment of data privacy and security practices in Indian BPO operations had three elements: (i) a survey fielded to Indian vendors of BPO services; (ii) on-site visits of Indian BPO operations and interviews with chief security, information, technology, financial and privacy officers; and, (iii) interviews and supplementary surveys with U.S. firms that offshore or outsource to offshore vendors. The survey asked standard questions which examined security practices concerning the information network, the physical on-site security procedures, the administrative safeguards, and elements of the contract that governed data security, including dispute resolution. The on-site visits were designed to verify security procedures and to develop a more qualitative understanding of security practices, and of how the involvement of the client or parent company shapes security policy. We interviewed and surveyed U.S. firms in order to better understand: how they select vendors; contract and dispute resolution procedures; how they monitor vendor firms; and how they recover data once the business relationship was terminated. The interviews and on-site inspections constitute the core of the study. The survey was designed largely to provide a benchmark profile for the activity and security practices of BPO service firms in India relative to those employed by U.S. financial services firms.

The issue of data security is complex. Data security concerns are tied to situation specific factors such as geography, the business process, and the sensitivity of the data being processed. Because of this, procedures for regularly monitoring, evaluating, and updating security practices are more important than any single technological solution. For this reason, quantitative representations of the presence or absence of particular technologies can be misleading.

A. Selection of Indian Companies

<u>Selection by Domain of Activity and Regulation.</u> The Tier 1 and Tier 2 Indian BPO operations (see footnote 8) to which we fielded the survey and visited on-site are all members of the National Association of the Software and Service Companies (NASSCOM). The survey was restricted to firms that processed personal financial information. The firms had to engage in activities that are governed by FACT Act (The Fair and Accurate Credit Transaction Act), GLBA (the Gramm-Leach-Bliley Act), Federal Debt Collections Practices Act (FDCPA), and/or HIPAA (the Health Insurance Portability and Accountability Act). The former three laws govern the uses of consumer financial information, placing restriction on the person or entities and the uses for which personal financial information can be accessed. HIPAA similarly governs the access to and uses of personal health information. These laws regulate data security, data privacy, and the responsibilities of firms in subcontracting work that involves personal information and any instance in which they share this data. The laws are

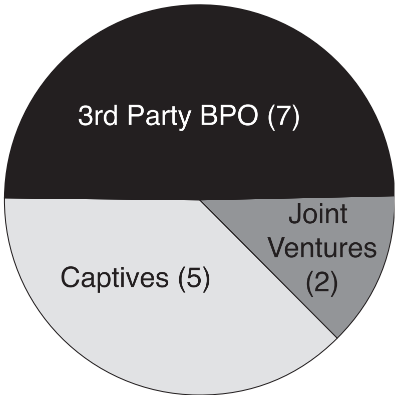
broad and also cover, for example, payroll and other employee information. The object of privacy concerns is the information governed by these laws. For example, BITS, the business strategy and technology division of The Financial Services Roundtable, has examined those functions and exchanges which are regulated by GLBA, FACT Act, FDCPA, and HIPAA, as opposed to say the offshoring and outsourcing of software design which may involve intellectual property issues and trade secrets.

We also included, in our survey and on-site interviews, software companies that come into contact with consumer information, e.g., in the creation of a new database management system.

Spectrum of Business Models. We visited and surveyed firms that span the spectrum of business models. We sought to interview a broad array of business models in our survey. This would allow a qualitative assessment of whether differences in business models have an impact on data security and data privacy.

Within the industry, there are four types of business models. They are, in order of managerial control from the perspective of a U.S. firm: (1) wholly-owned subsidiary or "captive" operation; (2) a partially owned subsidiary or joint venture; (3) a partially owned subsidiary or affiliate operated by the subsidiary or affiliate, but which the U.S. firm reserves the right to assume full managerial control and ownership, known as a "build-operate-transfer"; and (4) an independent third-party business process outsourcing vendor.acy practices.

Figure 3: On-site inspections, by business model type[52]



These 3rd party vendors we interviewed are not necessarily Indian firms. Almost all either had assets in the United States or belonged to companies which had assets in the United States. The subsidiaries, or "captives", of U.S. firms we examined are either business subsidiaries established by U.S. companies in India or BPO companies that had been purchased by U.S. firms. These firms largely processed the information of their parent companies, but they also often process generally to a much smaller extent the information of other firms. We also examined two joint ventures, firms in which a

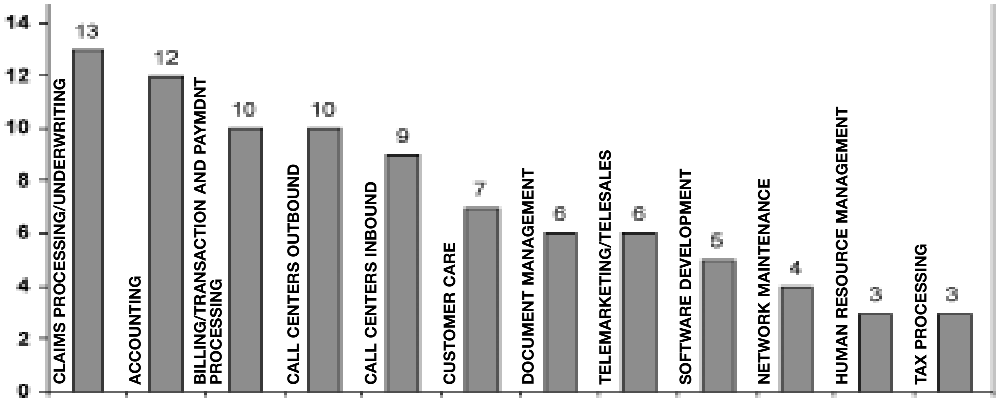
[52] We also visited firms that processed European data — one captive and two 3rd party BPO. These are not included in the figure.

major U.S. company owns a significant, occasionally controlling, share. These firms are limited liability companies and act for all intents and purposes as a vendor. We did not examine any a partially owned subsidiary which the U.S. firm reserves the right to assume full managerial control, the “build-operate-transfer”.

Processors of European Data. Included in our survey and on-site visits were firms which processed European consumer financial data. The activities of these firms would be governed by the FACT Act, GLBA, and HIPAA, were the data subjects American rather than European. As processors of European consumer information, they are governed by European law, notably the European Data Protection Directive. (Firms which processed U.S. consumer data and European consumer data are, of course, subject to European law in processing the latter.) We examined these firms for a point of comparison, to see whether there were any noticeable differences in security practices that stemmed from differences in national law.

Selection by Range of BPO Activity. The firms we inspected engaged in a wide variety of activities that brought them into contact with the personal information of U.S. consumers. Firms were selected also according to their activities. We based our visits towards activities which involved credit decisioning (loan processing), which gave individuals access to large amounts of a consumer’s financial information, and towards relations that brought employees in contact with information, such as credit card numbers, which made it easier to engage in fraud. (See Figure 1 below.).

Figure 1: BPO Activities of Indian Firms Visited On-Site, by type (multiple responses possible)[1]



B. Survey Instrument, Interview Structure, and Site Inspection

Surveys (see below) asked a broad array of questions. These covered company profiles — types of activity, value of contracts, number of employees, etc. — to

[1] This tally is of the 17 tier 1 and tier 2 BPO firms we inspected on-site in India plus three additional firms that provided us with answers to a detailed questionnaire.

security experiences and practices such as breaches and methods of data transfer through the structure of contracts. Many questions, especially concerning demographics such as the total value of contracts, met with a non-response owing to strategic positions. Information on security procedures was generally provided by all.

A caveat is in order. These were not surprise inspections. The firms we visited in India were aware that we would be inspecting facilities. Some U.S. clients have informed us that surprise inspections by clients do occasionally yield different results. U.S. companies have increasingly instituted routine inspections, many of which are unannounced. Indian firms complained that they were subject to too many inspections at times.

Our on-site inspections took note of the structure of access into the firm, the structure of access to work areas (ID cards, biometrics), the monitoring of employees (guards, cameras), and network access. We interviewed relationship managers, chief security officers and executives in charge of privacy. We paid attention to the role of and access given to the relationship manager of the client firm in order to assess the quality of coordination between the vendor and client, in 3rd party vendors, and between the parent company and its subsidiary, in captives. We also analyzed training programs, inspected workstations, security around servers, and data storage operations.

Finally, we conducted a series of structured interviews around a set of questions that were formulated by the Institute staff with input from Congressional staffers, U.S. regulators, academics, industry experts, and noted data privacy experts. The initial interview questions resembled the broader questions in the survey. These were used as starting points for each area of security and for each officer we interviewed. Follow-ups and a line of question then ensued according to the response given.

C. Selection of U.S. Companies and Interviews

The interview of U.S. firms was designed to capture the considerations that went into the selection of vendors, the concerns that informed the security and privacy clauses of contracts, the system of monitoring and reporting, the formulation of information security policy in instances of cross-border data flows, dispute provisions, and the procedures in place to retrieve (destroy) data once the relationship is concluded. We also sought to measure the importance of personal data security and privacy concerns in the decision of U.S. firms to offshore/offshore outsource. We interviewed those in charge of (i) data security, (ii) chief privacy officers, (iii) relationship management, (iv) legal department section responsible for the formulation of vendor contracts, and (v) relations with government and regulators.

As in the interviews in India, initial questions followed from survey questions. Interviewees were provided with a U.S. variant of the survey instrument. The answers were used as an initial starting point to discuss the issues listed above.

The four U.S. firms we interviewed reflected a diversity of factors in the offshoring/offshore outsourcing phenomenon. All are large firms, whose activities offshore ranges from simple telesales to comprehensive credit decisioning and financial asset portfolio management. The value of offshored operations ranged widely, from less than $500,000 to tens of millions of dollars. All the firms have offshored/offshore outsourced activities in more than one country, including India, Costa Rica, the United Kingdom, Ireland, and Canada. We supplemented these interviews with survey results from additional U.S. financial institutions.

APPENDIX B: REGULATORY ISSUANCES

The financial services industry increasingly relies on information technology (IT) service providers (“Service Providers”) to support the delivery of financial services. Evaluating and reducing risk to ensure safety and soundness is a cornerstone of the financial services industry. This approach, combined with regulatory requirements and review, ensures the security of customer information and the continued provision of high-quality services whether processed internally, externally, domestically or internationally. The following is an overview of the regulatory requirements (by date) that address in full or in part outsourcing issues.

- **FFIEC Outsourcing Technology Services** (July 2004). The Federal Financial Institutions Examination Council (FFIEC), which is comprised of the Federal Deposit Insurance Corporation, Federal Reserve Board of Governors, Office of Comptroller of the Current, Office of Thrift Supervision and the National Credit Union Administration, is working on a booklet on out sourcing which will include guidance on foreign outsourcing. The booklet will be used by regulators in conducting examination of financial institutions. The booklet will incorporate guidance on foreign outsourcing previously issued by the OCC. www.ffiec.gov/ffiecinfobase/booklets/outsourcing/Outsourcing_Booklet.pdf

- **Basel Committee on Banking Supervision Risk Management Principles for Electronic Banking and Report on Management and Supervision of Cross-Border Electronic Banking Activities** (July 2003) The principles state that the board of directors and senior management should establish a comprehensive and ongoing due diligence and oversight process for managing the bank’s outsourcing relationships and other third-party dependencies supporting e-banking. www.bis.org/publ/bcbs98.pdf and www.bis.org/publ/bcbs99.pdf

- **FFFIEC Booklet on Supervision of Technology Service Providers** (May 2003). The booklet covers the role the FFIEC agencies will play in examining the largest and most significant third party service providers. There are three themes in the Supervision of Technology Service Providers booklet that are consistent with prior FFIEC documents and BITS’ dialogue with the regulators on outsourcing issues: a) financial institution's board of directors and senior management are responsible for ensuring that outsourced activities are conducted in a "safe and sound manner;" b) financial institutions are expected to have a risk assessment process in place to evaluate risks from selection to ongoing relationship management; and c) FFIEC agencies will base their examinations on the concept of "RiskBasedSupervision."www.ffiec.gov/ffiecinfobase/booklets/tsp/tech_ser_provider.pdf

- Office of Thrift Supervision Bulletin: Third Party Arrangements TB 82 (March 2003) www.ots.treas.gov/docs/8/84261.pdf

- **FFIEC Information Security Booklet** (February 2003). The booklet describes how an institution should protect and secure the systems and facilities that process and maintain information. The booklet calls for financial institutions and technology service providers (TSPs) to maintain effective security programs, tailored to the complexity of their operations. www.ffiec.gov/ffiecinfobase/booklets/information_security/information_security.pdf

- **OCC Bulletin 2002-16: Bank Use of Foreign-Based Third-Party Service Providers** (May 2002). This bulletin provides guidance to national banks on managing the risks that may arise from their outsourcing relationships with foreign-based third-party service providers. www.ffiec.gov/ffiecinfobase/resources/outsourcing/occ-bl2002-16-bk_use_foreign_3-party_providers.pdf

- **Establishing Standards for Safeguarding Customer Information and Examination Procedures** (July 2001). The Guidelines were issued jointly by the OCC, FDIC, OTS, Federal Reserve Board and FDIC. Similar regulations were issued by the SEC and FTC. The Guidelines implement section 501 b of the Gramm-Leach-Bliley Act. www.federalreserve.gov/boarddocs/SRLETTERS/2001/sr0115a1.pdf

- **OCC Bulletin 2001-47: Third Party Relationships: Risk Management Principles** (November 2001). www.ffiec.gov/ffiecinfobase/resources/outsourcing/occ-bul_2001_47_third_party_relationships.pdf

- **FFIEC Risk Management of Outsourced Technology Services** (November 2000). www.ffiec.gov/PDF/pr112800_guidance.pdf

- Other guidance: The FDIC published three informational documents on outsourcing that cover a) selecting a service provider, b) service level agreements, and c) multiple service providers. The Federal Reserve Bank of New York has published a paper on "Outsourcing Financial Services Activities: Industry Practices to Mitigate Risk."

- **OCC Bulletin 98-3: Technology Risk Management** (February 1998) The bulletin provides guidance on how national banks should identify, measure, monitor, and control risks associated with the use of technology. The bulletin states that the OCC will assess bank management's efforts to ensure that all necessary controls are in place to manage risks associated with outsourcing and external alliances. www.occ.treas.gov/ftp/bulletin/98-3.txt

Customers benefit from worldwide sourcing as savings flow from financial institutions to initiatives that directly impact customers and their communities. Financial institutions have strong controls in place to safeguard customer information and to manage the risks of outsourcing domestically and abroad. Moreover, federal financial regulators examine both financial institutions and major U.S.-based third party service providers to ensure that both comply with safety and soundness requirements. The Financial Services Roundtable strongly opposes any efforts at the federal or state level that impose restrictions or requirements on where companies may choose to source business operations.

APPENDIX C: BS779 AND ISO17799 SUMMARY

ISO17799, or BS7799, is "a comprehensive set of controls comprising best practices in information security". The first iteration of the standard, BS7799 Part 1, was published in 1995 by the British Standards Institute. In 2000, the International Standards Organization published the BS7799 standard as ISO17799, at which point the standard gained widespread acceptance. While BS7799 (part 1) and ISO17799 are merely a code of best practice, Part 2 of BS7799 precisely describes what an organization and an auditor need to do in order to ensure successful certification under the 7799 standard. In short, part 2, specifies the implementation of an information security management system, as opposed to simply describing best practices.

BS7799 is comprised by 10 major sections. Below find a brief description of what the 10 sections of the standard cover:

Business Continuity Planning – This component concerns ways to avoid or deal with interruptions to business activities that arise from the effects of major failures or disasters.

System Access Control – This component prescribes methods to control access to information; to ensure the protection of networked services; to detect unauthorized activities; and, to ensure information security when using mobile computing and networked facilities.

Personnel Security – This component provides methods to mitigate problems caused by human error including deliberate acts such as theft and fraud. It also covers educating personnel as to policies and procedures, and how firms can minimize the damage from security incidents.

Asset Classification and Control – This deals with methods to categorize assets and determine the appropriate level of security for those assets.

Security Policy – This component is designed to provide management with direction and support for information security.

System Development and Maintenance – This section ensures that security is built into operational systems. It also provides methods to prevent loss, modification or misuse of user data in application systems; to protect the confidentiality, authenticity and integrity of information; to ensure IT projects and support activities are conducted in a secure manner; to maintain the security of application system software and data.

Physical and Environmental Security – This section is designed to avoid damage and interference to business premises and information and to prevent loss, damage or compromise of assets and interruption to business activities.

Computer & Operations Management – This section provides means by which a company can ensure the correct and secure operation of information processing facilities and the attendant technologies.

Compliance – This section provides method to ensure compliance with applicable criminal or civil law, statutory, regulatory or contractual obligations, security requirements, and ensures compliance of systems and processes with internal security policies and standards.

Security Organization – This component provides methods to maintain the security of facilities and information assets accessed by third parties and to maintain the security of information when the responsibility for information processing has been outsourced to another organization.

Other resources on this topic can be found at www.BITSINFO.org

BITS Framework for Managing Technology Risk for IT Service Provider Relationships and the BITS IT Service Provider Expectations Matrix

These documents were created to promote a common understanding of the financial services industry's needs related to information technology practices, processes and controls. The Framework establishes best practices for assessing and managing outsourcing relationships, and addresses regulatory and industry issues, including considerations for disaster recovery and cross-border relationships. The Expectations Matrix is a 33-page worksheet used by financial services companies to identify and document outsourcing risks; financial institutions, service providers and audit and assessment organizations use the Expectations Matrix to eliminate gaps in the audit and assessment processes. BITS currently has a project underway to explore the development of a consistent and objective process for performing assessments on service providers based upon the Expectations Matrix.

Key Contractual Considerations for Developing an Exit Strategy

Planning an exit strategy before ever signing a contract with a service provider may seem counterintuitive. However, without a well thought out strategy that is consistent with your overall sourcing strategy, your institution risks becoming locked in to an unsatisfactory relationship or paying more to part ways and minimize operational impact. This short paper outlines critical issues financial institutions and other organizations should consider in planning a strategy to exit a service provider relationship.

BITS Key Considerations for Global Background Screening Practices

This document is an outstanding tool for financial institutions and other critical infrastructure companies seeking to mitigate risks related to global outsourcing. The paper is divided into three sections - each section outlines financial institutions' top considerations for global employee screening policies, programs and requirements.

- Overview of the financial industry's legal and regulatory requirements;
- Strategies for evaluating the risks and mitigating controls for outsourced environments and activities; and
- Information to validate identity and background, listed by country.

THE FINANCIAL SERVICES ROUNDTABLE
1001 Pennsylvania Avenue, N.W., Suite 500 South
Washington, DC 20004
202.289.4322 T
202.628.2507 F
e-mail: info@fsround.org
www.fsround.org