

Commentary

What You Should Do About the India/Pakistan Crisis

The tension between India and Pakistan has affected the IT outsourcing market in India. Gartner offers guidelines for how enterprises and vendors should deal with this situation. Business continuity plans are key.

The possibility of war between India and Pakistan has flooded the worldwide media. The concern stems from the unprecedented buildup of troops by both sides on the Kashmir/Pakistan border, talk about nuclear weapons and fear of terrorists who may want to destabilize the region. Apart from the human and political crisis, these tensions have already hurt the IT industry in India, a leading destination for enterprises that want to outsource software development.

The media frenzy has created a great deal of confusion and spread some inaccurate information. The most basic thing to recognize is that the outcome remains uncertain — no irreversible chain of events has been set in motion. *Therefore, enterprises and vendors should resolve to deal with the crisis methodically.* They should base decisions on knowledge, not fear or media reports. Furthermore, they should keep things in perspective. Tension between India and Pakistan has persisted for more than 50 years. Although the present crisis is serious, the situation is at least familiar. Gartner believes India's software industry will continue to grow, although it must change some of its practices.

Nevertheless, not acting out of fear does not mean enterprises and vendors should ignore risks. The Sept. 11 attacks showed that the worst sometimes does happen. Crises like this one between India and Pakistan have the salutary effect of pointing out weaknesses in business continuity plans (BCPs), so enterprises and vendors should seize this opportunity to improve operations. To help enterprises and vendors understand the situation and how they should respond to it, Gartner has put together the following material:

- A survey of what has happened
- The view from inside India
- The issues the India/Pakistan crisis raises for business — in particular, BCPs and communications
- How the crisis will affect the global software outsourcing market
- What enterprises should do to reduce risk

Gartner

- What India's software vendors should do to reduce risk

What Has Actually Happened

Enterprises should make the effort to separate fact from fiction. In addition to reporting facts, the world media has sometimes sensationalized the smallest issues and repeated incorrect facts. For example, the U.S. government has denied media reports that the U.S. State Department has a plan to evacuate 60,000 U.S. citizens from India and Pakistan.

Concerned over the rising tensions, several governments around the world, including that of the United States, China and Russia, have put significant efforts into facilitating potential solutions with an aim to reduce the tensions. The tensions dominated the regional security summit that was recently held in Kazakhstan.

However, many countries have issued advisories — from telling citizens to exercise caution and delaying nonessential travel to instructing them to leave — and withdrawn nonessential government personnel. On 5 June 2002, the U.S. State Department strongly urged American citizens in India to depart the country.

The perception of India and Pakistan as dangerous has caused Indian software vendors' customers to delay, cancel or ban travel to India. Many companies have withdrawn nonlocal staff from India and Pakistan, while some multinational organizations have told their Indian and Pakistani staff that they can travel to other countries if they feel uncomfortable in their own countries (where they would go remains unclear).

The immediate effects on the Indian software vendors include:

- Vendors have sent letters to clients reassuring them about their BCPs, recommending that clients delay travel if they feel uncomfortable and explaining the situation from the local perspective.
- Customers continue to sign contracts that have been under way for some time. However, many clients have delayed due-diligence trips, which has reduced the number of contracts being signed. Some prospects are considering alternate offshore locations for outsourcing.
- Foreign embassies in India (for example, the U.S. embassy) have stopped issuing visas for Indians to visit other countries. This move has hurt business travel to the United States by vendor personnel as only those already holding visas can travel. However, many leading vendors have visa- and travel-ready staff.
- Some outsourcing vendors outside of India and Pakistan are promoting themselves as safer alternatives.

The View From India

In 50 years of tension, Indians and Pakistanis have learned how to live with the threat of war. India and Pakistan have fought three wars over Kashmir, the most recent between 1999 and 2000, and Indians and Pakistanis view the present crisis as little different than the previous ones. After the United Kingdom and United States upgraded their travel advisories, some in India and Pakistan wondered whether their governments have given them the full picture or whether the Western allies have simply used this as a ploy to pressure the two countries to ease tensions.

Nevertheless, Indian vendors realize that perception is reality for many customers, and they worry that, if the crisis drags out, it could damage their booming business. They have, therefore, begun to address clients' concerns.

Business Issues

Obviously, no one knows how long the crisis and travel advisories will last, so enterprises face much uncertainty when making new outsourcing decisions and in setting tactics for critical projects that are already under way, as well as those that depend on meetings in India.

An outbreak of hostilities would primarily affect:

- Application development
- Contact centers
- Business process outsourcing (BPO) activities performed at the vendor's site in India

Access to human capital with the appropriate customer knowledge would be the major problem in continuing these activities.

The biggest issues enterprises and vendors must address are BCPs and communications.

BCPs represent enterprises' major concern in the short term:

- Vendors reviewed their BCPs after Sept. 11, but the completeness of BCPs varies from vendor to vendor. In general, the largest vendors have the scale, redundancy and capital to create the most comprehensive plans.
- More complete scenario planning needs to occur. Most BCPs today do not adequately address the issue of human capital, the most pressing issue for enterprises affected by the Sept. 11 attacks. Nor do BCPs adequately address the issue of a catastrophic event or major disaster immobilizing a major city, region or an entire country.
- *Most enterprises don't have specific action plans in case a disaster affects their offshore vendors.* Enterprises need enterprise- and project-level plans that address the availability of workers, knowledge, data, applications, documentation, communications and passwords. Many enterprises now ask for specific scenarios. For example, what should the enterprise and service provider do if a location goes down, a link goes down, travel is restricted, business comes to a halt in a city or key project personnel become unavailable? Because they need specific details for their projects, not just documentation, enterprises have begun to map their own BCPs to those of their suppliers.

Communications, data and backup come to the forefront as issues for enterprises creating contingency plans in case of a large-scale disaster:

- If a disaster occurs, vendors will not have the ability to resume work on all projects for all clients immediately — perhaps not for some time. Prioritization of projects must take place by vendors and clients.
- A disaster will create a rush on voice and data telecommunications systems. Even if data is safe, enterprises may not be able to access it or communicate with the vendor to access the situation. *Also, the vast majority of Indian software firms' BCPs are India-centric, with backup sites only within India.* Although leading vendors may have robust, redundant data communication links with the

United States, they don't necessarily use them to back up to client sites there. Thus, a disaster at a national level would leave U.S. clients with significant problems accessing backed-up information

- As a result, delays in projects will occur while waiting for new communication channels to be formed to replace face-to-face communication that has been delayed due to travel concerns. Miscommunication will likely occur due to the lack of presence in India of key project staff.

Market Implications

The crisis will affect the outsourcing development market in increased costs, enterprise attitudes and vendor opportunities.

Increased costs: The cost of strengthened BCPs will eventually be passed on to the customer, diminishing the cost advantage of Indian providers; however, providers everywhere should also strengthen BCP plans. Already some vendors are changing their BCPs. Infosys just announced that it will have daily movement of data, documentation and code to backup locations in India and weekly movement to locations outside India. Wipro and others have also indicated they have a greater frequency and scope of backup activities. Long term, we expect enterprises will demand that more key project personnel remain onshore, a costlier option that lowers the advantage of the offshore model.

Enterprise attitudes: In the long term, enterprises may question India's viability as a major source of IT activities. However, crises and uncertainties abound throughout the world, so if enterprises really want to adopt global delivery models, they *must* build skills and competencies to manage political instability in *any* country or region:

- Enterprises cannot assume that there is a totally "safe" alternative. Thus, Gartner does not advise immediately moving work to other countries perceived as safer, such as the Philippines or China. Instead, BCP and scenario planning must play increased importance in any offshore activities.
- Nevertheless, enterprises should accelerate efforts begun after Sept. 11 to diversify their geographic risk.

Vendor opportunities: Smaller Indian providers will have the most trouble due to continuing fallout since they don't have the capital or resources to provide the scale and redundancy for comprehensive BCPs. However, the crisis will mean new opportunities for others:

- Service providers can benefit if they have the ability to pass work between dispersed global centers as the geopolitical situation requires — for example, Indian firms that establish global delivery models or create large U.S.-based external service provider (ESPs). Some of the leading Indian vendors already planned to increase their global coverage; this crisis will spur them to accelerate these plans.
- Risk diversification in terms of country is prudent — we already stated this after Sept. 11, but we expect this will accelerate. Countries deemed "safest" will undoubtedly get a closer look and thus will gain new opportunities (for example, Canada, Northern Ireland and Panama). They will put together a comprehensive case for enterprises doing business there. We expect a portion of BPO investments will divert to the Philippines, Canada and Latin America.
- ESPs headquartered in North America that provide offshore services (for example, CGI, Keane, Syntel, Covansys and Cognizant Technology) can also benefit, particularly those maintaining a much lower percentage of people offshore (for example, Covansys, Syntel, Keane).

Advice to Enterprises

- *Confirm media reports* — Reconfirm news with reports from your vendors. Be aware that political commentators and government officials in India and other countries may have their own goals and perspectives when reporting news on this issue.
- *Overcommunicate* — Gartner always emphasizes communications to address normal issues (cross-cultural issues, virtual team dynamics, organizational resistance to change, capability maturity differences as well as time zone and physical location). The present crisis calls for communication beyond the usual, including talking with vendors, clients and prospects as well as with the enterprise's employees. Apply the three "R's" — rigor, re-enforcement and repeatability — to reach all key stakeholders.
- *Revisit the offshore provider's BCP* — Understand the scope, limitations and risks of the offshore provider's BCP. Conduct an in-depth review of the components of the plan and ensure the enterprise is comfortable with the key elements: data, platforms, connectivity and succession planning for workers. The vendor should have done "dress rehearsals" to show proof of concept for its BCP. Work with the vendor to create customizations to its BCPs to meet specific needs on a company and project basis.
- *Reinforce standard redundancy planning* — Enforce all approved policies and procedures at all sites in India and, of course, at the ESP's sites. The most important aspects include timely execution and safe storage of backups offsite, physical security of personnel, facilities and technology equipment as well as data, logical security of technology access, and connectivity access for voice and data, including multiple carriers, alternate channels (routing of lines) and mediums (fiber, satellite).
- *Don't rely on country resources* — All the largest ESPs in India and many smaller providers today do not rely on the country's infrastructure such as power and telecom. Thus, if some type of conflict occurs, the enterprise shouldn't rely on Indian resources either.
- *Understand the risks and limitations* — Even the largest ESPs in India don't have complete backup as well as redundancy capabilities outside of the country. Many of the largest vendors have significant facilities outside of India, but they don't use them for backup or as redundant locations. No matter how comprehensive a vendor's backup capabilities outside India are, none of the backup sites can absorb more than a portion of its total employees. Therefore, the entire workload cannot be processed for every customer. Each customer should determine what its position will be in a worst-case scenario.
- *Review contracts* — Where necessary negotiate adjustments with vendors to accommodate the changing environment. Key areas include frequency of delivery, backup plans, location of version-control servers and rates for onshore staff. Enterprises may need new agreements to determine the level of service provided in the event of a disaster in India and which projects should be prioritized.
- *Work with the ESP* — Crises are also opportunities to build stronger bonds. Enterprises should demonstrate their commitment to working through these issues with their vendors. Doing so will create a closer relationship that will work better for both. Voice concerns early and work with staff and the vendor to mitigate the risk. It's too early to pull out of India, so work to resolve issues, not to create new ones by moving projects out of India.

Advice to Vendors

- *Overcommunicate* — Talking with clients remains crucial, of course. Vendors should also increase the level of internal communication to alleviate fears and update staff of the issues and concerns of clients, actions being taken to address these concerns, and changes in priorities and procedures.

- *Develop a comprehensive BCP framework* — Include scenarios for site, city and country outages. Have backup plans within India (in different cities) and outside of India. Re-examine BCPs often, look for possible flaws that may have been overlooked or need revision due to a changing environment or client needs.
- *Address BCPs now* — Proactively communicate BCP plans and updates to clients. Work with each client to review its BCP and provide customized options, if requested, at both the client and project level. Perform dress rehearsals to ensure the BCP can be executed and to identify flaws.
- *Be understanding* — Show commitment to clients by working with them to resolve their problems. Understand the new perception that clients have and work with them to educate them on the realities. Explain to clients the view "from the ground" in India and reassure them of measures to mitigate risk. Ensure that they know the proximity of facilities to likely areas of conflict and all other relevant information so that they can make informed decisions. If clients are uncomfortable traveling to India, suggest they defer their visit and try to get the work done in other ways (for example, videoconferencing or meeting in other locations, such as Singapore, Thailand or Australia).
- *Deliver more often* — Deliver intellectual property, including code, applications, data, passwords and documentation, more regularly to the client.
- *Prepare for project relocation* — Maintain a limited development environment in a location outside of India for each major project, with all passwords and other access keys available to an executive sponsor outside of the region. Ensure that all intellectual property of the project is constantly updated and can be transferred smoothly to another project team if necessary. U.S. ESPs with offshore investments and enterprises collaborating across borders should use their U.S. business to mitigate risk.
- *Work with the National Association of Software and Service Companies (NASSCOM)* — The industry should display a common front to clients. A clear, concise message explaining the situation and how the industry as a whole is addressing problems will avoid conflicting statements emanating from different ESPs.
- *Obtain temporary work visas* — Wherever possible, obtain visas, even if they are not needed at this time, for staff involved in critical projects (especially for the project leads). Having the ability to travel to the United States, Europe or other Asian countries to perform work on-site and ensure service continuity is a critical part of an ESP's BCP.
- *Understand all risks* — Several other risks in addition to geopolitical concerns affect enterprises' offshore service decisions. Long term, success depends on ESPs alleviating this broader set of risks.

Additional Research

"Tactical BCP Lessons Learned From Sept. 11" (TG-15-3991)

"Jump-Start the Business Continuity Plan: A Checklist" (TG-14-5245)

"The Ripple Effect: Disaster's Indirect Impact" (TG-14-5298)

Bottom Line: We believe the current situation in India and Pakistan does not warrant enterprises pulling their projects out of India. Moving projects out of India will create more problems than it solves. However, enterprises should also develop plans to move out of India in case the situation worsens and there is a need to do so.

For now, enterprises should focus most on resolving and anticipating problems raised by the crisis. In particular, enterprises and vendors must prepare robust BCP plans, but they must also become more agile. The level of planning and the resulting agility that they can demonstrate will directly correlate to the level of trust and confidence that will help determine growth.

Gartner believes that, in the long term, the top-tier Indian IT service providers with adequate investment in BCPs and other risk-mitigation strategies will continue to outpace the overall global IT service market in revenue growth and operating margin.