Gordon Housworth
Intellectual Capital Group LLC
phone: +1 248.626.1310
email: ghidra@icgpartners.com
1 November, 2007

Low cost is not low risk: Intellectual Property and Outsourcing Risk in India

India is unlike other outsourcing and manufacturing regions

- India is unique in that risks to personnel and facilities coexist with IP risks throughout its regional supply chain.
- Personnel and facility risk will rise over time despite prodigious efforts by the Indian security apparatus.
- Commercial IP threat is presently more from foreign collectors and careless outsourcing in the Indian supply chain – which will include outsourcing to China.
- Indigenous commercial IP threat is largely "entrepreneurial."

Defining IP and its loss

- Intellectual Property: Exclusive rights to the conversion of a unique application of people, capital, technology, and information into shareholder value.
- Intellectual Property Theft: Loss of exclusivity.

Think asset, not country, in assessing IP risk

- While certain assets are at risk in any country, the key is to think “asset” instead of “country.”
- Risk cannot be based on countries or “risky areas” but ***wherever a sufficiently valuable asset is accessible at any tier in any country*** - as the collector will move to the least defended point that contains the IP.
- We see collection efforts on US assets long before they are transferred offshore.
- Commercial and dual-use technologies are high on the collection list.
- “Country” is only part of integrated IP protection.

Difficult to omit certain countries

- Unworkable to isolate “risky countries” with respect to IP migration.
- Revenue loss and market share erosion when presence is withheld.
- Host nations demand you be there with competent products and technology in order to do business.
- Three key vulnerability areas in any country:
  - **Pricing model compromise** (supplier outsourcing, subcontracting, etc.)
  - **Data citadel attack** (R&D hives and data warehouses).
  - **Human resources** (HR) churn.

Global risk to both domestic and offshore facilities

- Most firms don’t know they’re at risk.
- If they do become aware, they don’t know where to turn for valid assistance.
- Deprived of competent advice, firms employ non-solutions that lull themselves into a false sense of security.
- Firms silently surrender, fearful of negative consequences to business continuity or souring relationships with a host government.
- A firm's management may not confront a threat despite awareness and even presence of internal champions for improved protection.

Why and how firms outsource

- Firms usually devolve the problem to a divisional or unit level, thus means, omissions and results vary on a case-by-case basis.
- Same problem solved in differing ways “to avoid some organizational consequence” such as:
  - Cost savings.
  - Headcount reductions (protect existing staff or get credit for a reduction).
  - Functionality (missing, failing or inconvenient).
  - Personal need (positive annual personnel rating).
- Each ‘solution’ may be measured against suboptimizing criteria.

What is missing from outsourcing

- A decision making framework that integrates global and national aspects of need, technology, business considerations, risks, scope, duration, cost implications and ultimately solutions.
- There are always multiple solutions depending upon desired outcomes and bounds of monies, mindshare, and timing.
- Outsourcing and manufacturing risks and remediation are not harmonized.

IP and outsourcing

- Firms effectively loose control of IP when it is outsourced as little as two levels.
- Observed IP theft by nations both in-country and in adjacent countries where they've either penetrated or bought stakes in local firms.
- Countries without strong police powers permit entry of secondary collectors that use a permissive environment to collect what they could not feasibly or financially obtain in a stronger security environment.

Unique Indian characteristics

- India *has not* exhibited wide or state sponsored IP collection, being content at present to compete in terms of lower cost
- Indian military *does* collect for national security applications.
- Much IP theft is local “entrepreneurship.”
- Over time, expect IP attacks to shift to “commercial on commercial” collection.
- Bribery remains strongly embedded.
- Physical threat to core outsourcing facilities in India.
- Threat to IT and outsourcing assets in Bangalore and Hyderabad should be taken seriously despite denials from Indian authorities.

Lashkar-e-Toiba (LeT), Army of the Pure

- Rose as part of Mujahideen resistance against Soviet occupation in Afghanistan; military wing of Markaz-ud-Dawa-wal-Irshad (MDI), an Islamic fundamentalist organization from Pakistan.
- Goals go far beyond regaining Muslim control of Jammu and Kashmir to recreating Islamic governance of India in union with other predominantly Muslim states surrounding Pakistan.
- Active in Jammu and Kashmir, India, Chechnya, Afghanistan, Iraq, Bosnia and elsewhere.
- More educated and skilled than peasant groups; cadres are well networked and computers savvy.
- History of orchestrating attacks in India.

Lashkar-e-Toiba (LeT) lethality

- LeT cadres characterized by a level of brutality surpassing all other Pakistan-sponsored terrorist outfits active in Jammu & Kashmir.
- LeT ranks alongside the Chechens, the Algerian GIA (Groupe Islamique Armé) or Armed Islamic Group.
- LeT unlikely to engage in serious terrorist operations outside the Indian subcontinent.
- LeT's potential to strike Western targets in both Pakistan and India is all too real.
- LeT will continue to attempt to destabilize India's commercial and political elites.

“Twofer” attack on Indian state and US/European outsourcing assets

- Attacks on outsourcers directly damages the Indian state and its economic capacity, and indirectly damages US and European firms -- where an attack on US soil would be prohibitive.
- Attacking software offices hits most international symbol of Indian success.
- Potential for panic from foreign investors and multinationals that could hobble rapid pace of India's economic progress.
- Economic and cultural destabilization seeks targets inflicting maximum damage to people and delivering a symbolic message.

Attack progression

- Extending the “twofer” concept, we forecast this attack progression (2005):
  - Personnel and symbolic targets.
  - Expat data and business process outsourcing (BPO) centers.
  - Manufacturing and development centers.
- Latter two target groups can cause supply chain disruptions.

Overlooked leverage, the embedded “twofer”

- Great numbers of US banks have Indian data centers, attacks against which have multiplier effect in that the bank and all its customers are affected.
- Targeting data, BPO and manufacturing facilities:
  - Leverages operations and business continuity of US/EU firms that would otherwise be difficult to attack.
  - Demonstrates that the Indian government cannot protect its offshoring endeavors.
- Unfortunately, relocating from India elsewhere in Asia merely exchanges direct attack risks to more intellectual property loss risks.

Iconic attacks commence; LeT strikes India's "MIT"

- LeT attacked Indian Institute of Science (IISc), Bangalore, Dec 2005, a "temple" of Indian "knowledge society."
- Shock waves reverberated through Indian high-tech community:
  - One of India's more prestigious educational and research institutions.
  - Presence in Bangalore "a key reason that the city became India's technology powerhouse."
  - Does R&D for multinational and local technology companies.
  - Alumni occupy key positions in the country's outsourcing industry.

Damage control commenced immediately to placate US/EU outsourcing clients

- Nandan Nilekani, CEO of major Indian outsourcer, Infosys Technologies Limited, was quick to attempt to play down risk to US firms:
- *"Our campuses are physically secure. We have all kinds of checks that we do. The entire perimeter is guarded which we believe enable us to be fully secure."*
- *"Even after American companies factor in additional security costs, doing business in India is still far cheaper than staying home."*
- Today, perhaps. Tomorrow, not clear.

LeT attacks India's financial capital, Mumbai (Bombay), 2006

- Mumbai Suburban Railway has highest passenger density of any urban railway system.
- Seven bombs placed in first-class “general” compartments (some reserved for women) targeting professional classes.
- Trains were running from Churchgate, the city-centre end of the western railway line, to the western suburbs.
- Analogous to the Madrid and London train/tube bombings, 209 killed, over 700 injured.

Were it not for Indian intelligence…

- Indian intelligence has made sustained effort to penetrate and disrupt LeT and other Muslim jihadist groups, even on Pakistani soil.
- Despite remarkable effort, jihadists are shifting assets south and east of the *Line of Control* (de facto border dividing disputed zones of Indian and Pakistani controlled Jammu and Kashmir)
- Goal of targets that offer a force multiplier against the Indian state.

Iconic, symbolic and personnel targets

- Bangalore's Indian Institute of Science (IISc) was a premier symbolic target. Expect others to follow from both jihadist and Naxalite Maoist attackers.
- Equally vulnerable:
  - Indian Institutes of Technology (IITs) (Delhi, Kanpur, Mumbai, et al).
  - Indian Institutes of Management (IIMs) (Ahmedabad, Bangalore, Calcutta, et al).
  - Virtually every expat outsourcing facility and personnel compound.

Key for expat firms with no viable options for relocation

- Conduct a rigorous vulnerability assessment, then implement the appropriate risk mediation interventions for personnel, facilities, data and IP.

Defend, defer and deflect for IP, plants and personnel

- Technologies migrate and threats emerge; firms assume risk by default in:
  - Not identifying what is already compromised or at risk.
  - Identifying what assets need to be protected.
  - Defining dollars and effort needed to realistically protect those assets - wherever they occur in the supply chain.
- If a collector obtains a critical IP asset, or an attacker targets a key facility, the owner's ROI justification can collapse along with its expected revenue stream.
- When the IP asset is the core of a system or subsystem that often contains more mature, less competitive technology, the entire system revenue stream truncates.

What does work: Design Basis Threat

- Design Basis Threat (DBT) works regardless of whether the threat is counterterrorism (CT) or Intellectual Property (IP) theft:
  - Asset Value Assessment.
  - Threat/Hazard Assessment.
  - Vulnerability Assessment.
  - Risk Assessment/Risk Management.
- DBT defines a coherent view of risk tolerance, and a response strategy that interdicts the adversary's preparation, surveillance and collection.
- Beware use of scenario analysis as it is dangerously omissive, has no end as it has no scope-like business risk statement to bound it.

Implementable, teachable, effective processes exist

- Prudent, non-adversarial business practices to identify current exposure and to combat collection efforts.
- Achieve success with strategies drawn from proven Counterterrorism (CT) practices applied to IP, personnel and facility risk evaluation and remediation.
- Experience shows these processes can be taught and embedded as company best practices performed by its employees, not outside consultants.
- Properly done, protection becomes a crucial business attribute, like quality, lean manufacturing or robustness.

Fiduciary implications

- Firms that do not understand this landscape and industrial progression are ripe for IP harvesting and worse.
- Legal remedies largely ineffectual and rewards moot as the IP is already lost and all expected downstream revenue is attenuated.
- Asset/personnel attacks are supply chain disruptors.

Predictions for the Indo-Chinese IT sector

- India will, for the foreseeable future, become the low-cost IT counterpart to China low-cost manufacturer.
- India and China will complete a shift to Linux, of increasingly indigenous versions, that, given the region's user volume and technical expertise, could see the center of Linux development shift to Asia.
- India will use its IT expertise to develop “asymmetrical” low-cost efficient computing devices driven by its 'disadvantaged' position on the Digital Divide. (Much like Japanese vehicles in the 1960s, those devices will mature and expand out of Asia.)

Predictions for the Indo-Chinese IT sector, part 2

- India's IT-based products will take advantage of both rising local manufacturing efficiency and Chinese low-cost manufacturing (rising price-volume efficiencies in both nations) along with their rising broad based consumerism.
- India will increasingly outsource to, and acquire, IT/tech resources in China such that supply chain risks will reach similar proportions in both countries.
- India will become the recipient of Chinese attentions in IT intellectual property (IP) much as have US and European firms in the heavy manufacturing segment.

Low cost is not low risk: Intellectual Property and Outsourcing Risk in India

Gordon Housworth
INTELLECTUAL CAPITAL GROUP LLC
26775 Crestwood
Franklin MI 48025
phone: +1 248.626.1310
email: ghidra@icgpartners.com
website: http://www.icgpartners.com
weblog: http://spaces.icgpartners.com