Gordon Housworth
Intellectual Capital Group LLC
phone: +1 248.626.1310
email: ghidra@icgpartners.com
31 January, 2008

Protecting your Intellectual Property in China and India

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 China, 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 the US west coast against electronics assets before they are transferred to Asia.
- Commercial and dual-use technologies are high on the collection list.
- “Country” is only part of integrated IP protection.

Going offshore without consistent plan

- Firms often devolve the problem to a divisional or unit level, thus means, omissions and results vary on a case-by-case basis.
- No decision framework integrating global and national aspects of need, technology, business considerations, risks, scope, duration, cost implications and ultimately solutions.
- Same problem solved in differing ways “to avoid some organizational consequence.”
- Each ‘solution’ may be measured against suboptimizing criteria.
- 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.

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.

Four tiered model of IP violation

- "Piracy" is an imprecise term in describing the risks and impacts to Intellectual Property (IP):
- **Simple piracy**
  - Copy with no effort to hide piracy - the audio/video model.
- **Substitute product**
  - Pirated/stolen IP used to create a "no name" or "other name" product competing with legitimate offerings, usually on price.
- **"Badged" substitute**
  - Pirated/stolen IP used to create products masquerading as legitimate offerings by legitimate supplier.
- **Supplier substitution**
  - Original legitimate supplier is forced from the market, replaced by copier.

Rising collection levels in China

- US and EU IP is being harvested at an intense rate by a hierarchy of collectors.
- Chinese firms are being pressured for increased margins while Chinese scientists and researchers are being pressured for national breakthroughs that create native Chinese advances not subject to foreign control and/or royalty payments.
- Feeling of impunity on the part of collectors in the face of feeble or ineffectual responses from targets.

Unique automotive characteristics

- US and EU automotive OEMs have largely surrendered desirable IP via their joint ventures with Chinese partners.
- Recognition by collectors that much of the state-of-the-art IP is in the Tier One and Two base.
- Toyota/Denso remain a dedicated target by virtue of their retaining hierarchical design and manufacturing knowledge base.

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.

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.”

Global IP 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.
- 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.
- Firm's management may not confront a threat despite awareness and even presence of internal champions for improved protection.

Your advisers are likely vulnerable

- Management consultancies, banks, investment houses and law firms tend to share three characteristics:
  - Actionable IP protection guidelines are absent; in their place are ineffectual guidelines conferring false sense of security among clients.
  - IP often missing among key characteristics that offshoring clients are urged to address.
  - Fear of reprisal by host government refusing them business restrains level of advice offered to clients.

Use advisors wisely but make IP protection your own

- Big Four have commenced unofficial, uncontrolled joint ventures (JVs) with the Chinese state:
  - Providing consulting and training at various levels.
  - Seconding staff to bodies such as the finance ministry and the China Securities Regulatory Commission.
- De facto strategic advisory JVs expose virtually anything in the Big Four's inventory without accountability.
- Consider everything they transfer to China, or make accessible in China, as open to compromise.
- IP nightmare will only be perceived after damage is done.

What doesn’t work

- PRTM surveyed global US automotive suppliers for 2006 SAE World, distilling supplier attempts at IP protection.
- None offer protection against even modest collection efforts. Even less effective against an Asian style method of collection.
- Commercial supply bases lack effective protection and whatever attempts are being made at a ‘solution’ to IP risk are only lulling the targets into a false sense of security.

Misadventures in IP protection

"Choose components wisely"

- Mature items, little "design know-how," build own plant…

"Break up assemblies"

- Limit suppliers, disperse assembly, withhold details…

"Select partners carefully"

- Check integrity history, choose partners "with vested interest in protecting your IP"…

"Exploit all legal options"

- Strong legal contracts and NDAs, use Chinese lawyers to detail needs, aggressively prosecute offenders…

Trends in Chinese IP collection

- Explosion of “Copy-cat cars” and subsystems; quest to leapfrog limits of local design/concept IP.
- Asian ‘snippet’ collection method continues for both detail and concept.
- Quest for mathdata (CAD data) and high-order product definition:
  - Massive white light scanning (White Light Interferometry).
  - Specific targeting of vendors and technologies that do not respond to white light scanning.
  - Dual loyalties of Chinese design-engineering firms.
- Virtual reproduction of scanned family of parts, subsystems and vehicles.

Trends in Indian IP and US/European outsourcing assets

- India will receive Chinese attentions in IP much as have US and European firms.
- Attacks on outsourcers to damage Indian economic capacity, and indirectly damage US and European firms.
- Attacks on software offices, BPO/data centers and manufacturing hit symbols of Indian success.
- Targets chosen to inflict maximum damage to people and deliver a symbolic message.
- Attempt to panic foreign investors and multinationals.

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.

Overlooked leverage

- US/EU banks and firms have Indian data centers, attacks against which have multiplier effect, i.e., the bank and all its customers are affected.
- Targeting data, BPO and manufacturing facilities:
  - Leverage operations and business continuity of US/EU firms that would otherwise be difficult to attack.
  - Demonstrate Indian government's inability to protect its offshoring endeavors.
- Unfortunately, relocating from India elsewhere in Asia merely exchanges direct attack risks to more intellectual property loss risks.

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.

Required actions for an SEC-regulated IP-dependent client

- What is a corporate SEC-regulated IP-dependent client to do in the age of Sarbanes Oxley?
- Independently build up credible IP protection program:
  - IP-focused exposure or assessment program, especially for IP upon which future revenue depends.
  - Establish IP-driven carve-outs for business critical valuations.
  - Start with knowing what has been compromised; although painful it can staunch an IP hemorrhage and evolve into a tool for allocation of suitably-valued IP protective measures.

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.

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.

Protecting your Intellectual Property in China and 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