

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

Protecting your Intellectual Property in Mexico, Brazil and China

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 lose 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 Brazilian characteristics

- ❑ Brazilian military *does* collect for national security applications.
- ❑ Brazil *is* exhibiting moderate “commercial on commercial” collection.
- ❑ Bribery remains strongly embedded.
- ❑ IP theft is facilitated by high level of corruption.
- ❑ Local conditions engender a “justified catch-up” mentality.
- ❑ Southern Cone becoming dumping ground for cheaper, lower-quality cocaine.
- ❑ Second largest cocaine consumer after the US.
- ❑ Regional threats and actors tip towards destabilization.

Brazil is a mixed threat environment

- ❑ Commercial IP threat is presently from foreign and, to lesser degree, local collectors, and criminal assets.
- ❑ Risks to personnel and facilities coexist with IP risks throughout its regional supply chain.
- ❑ Personnel and facility risk will rise over time despite efforts by state security apparatus.

Ample ungoverned areas, ill-equipped law-enforcement agencies and militaries

- Tri-Border Area (TBA) of Argentina, Paraguay and Brazil:
 - Bounded by Puerto Iguazu, Argentina; Ciudad del Este, Paraguay; and Foz do Iguacu, Brazil.
 - Money laundering, arms and drug trafficking, counterfeiting, document falsification and piracy.
- Southern Cone:
 - Argentina, Chile, Uruguay, and now Paraguay and southernmost regions of Brazil.
 - Cocaine processing, easier route to Europe, drug trafficking and smuggling.
- Andean Spine:
 - Bolivia, parts of Peru, Ecuador and Chile.
 - Cocaine processing, drug trafficking and counterfeiting.

Endemic IP abuse environment

- ❑ Piracy of copyright material and counterfeiting of trademark-protected goods remain widespread.
- ❑ Problems in protecting intellectual property relate to enforcement as much, or more, than policy.
- ❑ Violations persist despite:
 - Signatory to most international IP agreements, including Trade Related Aspects of Intellectual Property (TRIPS) Agreement.
 - Member of World Intellectual Property Organization (WIPO).
 - Industrial Property Law (1996) observes most, but not all, standards in patent and trademark protection.

Moderate anti-IP intellectual environment

- Life sciences products susceptible to Brazilian intervention:
 - Patents broken on branded antiretroviral products with “compulsory licenses” for imported reverse engineered Indian and Chinese generics.
 - Adoption of free software by government (federal, state, city and military) and private sector.
 - Creative Commons project:
 - Move from strict “all rights reserved” to “some rights reserved” model.
 - Development Agenda:
 - Proposed by Brazil and Argentina at World Intellectual Property Organization (WIPO).
 - Developing countries claim that transfer of technology was needed for development.
-

Pressure to remain preferred regional automobile supplier

- ❑ Export potential hurt by appreciation of the real, reducing assembly levels and pressuring manufacturing costs.
- ❑ Import threats from mature North American/EU OEM low-cost vehicles and Chinese and Indian OEMs.
- ❑ Steep competition from other emerging markets in attracting additional foreign direct investment (FDI).
- ❑ Workforce training levels not quite at advertized levels.
- ❑ Technology hubs increasingly necessary to retain assembly operations.
- ❑ Pressure to retain regional preeminence drives local collection efforts.

Brazil is part of China's mercantile strategy

- ❑ Strategic plan creates mercantile structure that secures energy stocks, raw materials, and crops.
- ❑ Can not be interdicted by the US or its allies.
- ❑ Delivers export markets for commercial and military production, redirects regional elites to study in China, and extracts diplomatic obedience.
- ❑ Sends large groups of diplomatic and consular agents that meet counterparts at each level of the target country's bureaucracy.
- ❑ Promotes infrastructure projects using Chinese firms, creating a camouflaged posting for People's Liberation Army (PLA) assets.
- ❑ Veiled PLA works have common pattern: tidewater port presence offering partial or complete opaqueness connected by a *strassendorf* (street city) style of satellite towns connected by new roads to a processing plant at the primary extraction asset, e.g., coal, oil, minerals, timber, etc.

Brazil also has attractive targets

- Invitations to collection are many:
 - Tritec Motors, Campo Largo (Curitiba, Parana).
 - Chrysler-BMW JV to manufacture 1.4- and 1.6-litre four-cylinder gasoline engines.
 - One of the “most technologically sophisticated and fuel-efficient car engines.”
 - Blocked in the US, Lifan Group attempted to purchase and move plant to China.
 - Sold to Fiat Powertrain Technologies including “facilities, manufacturing unit, production lines and the license to produce the current range of products.”
 - Brazilian biofuel conversion.
 - Brazilian oil & gas exploration.
-

Unique Mexican characteristics

- ❑ Mexican military *does not* collect for national security applications.
- ❑ Mexico *is not* exhibiting “commercial on commercial” collection.
- ❑ Bribery remains strongly embedded.
- ❑ Theft is facilitated by high level of corruption.
- ❑ Drug cartels have become states within a state.
- ❑ Regional threats and actors tip towards destabilization.

Mexico is a mixed threat environment

- ❑ Commercial IP threat is less strong than other states, but drug cartels have yet to exploit their capacity to collect.
- ❑ Risks to personnel and facilities coexist with IP risks throughout its regional supply chain.
- ❑ Personnel and facility risk will rise over time despite efforts by state security apparatus.

Piece part/commercial focus fails to include key Mexican factors:

- ❑ Mexico's \$30+ billion USD black market.
 - ❑ \$20+ billion from drug smuggling. Balance from kidnapping, protection, bank/casino robbery, prostitution, fake merchandise, arms and gems smuggling and human trafficking.
 - ❑ Felipe Calderón's massive military crack down on Mexico's drug cartels.
 - ❑ Cartel counterattacks.
 - ❑ Resurgence of Marxist EPR, Ejercito Popular Revolucionario (Popular Revolutionary Army).
 - ❑ Restive López Obrador supporters.
 - ❑ Weakness of PEMEX and Mexican oil production.
-

Something is different

- ❑ EPR's "prolonged people's war" has been rejuvenated, able to operate outside their regular southern sphere of influence.
- ❑ Perps, EPR or other, have sophistication to plan, coordinate and execute simultaneous attacks.
- ❑ Blasts occurred at valve stations where different pipelines intersect.
- ❑ PEMEX is sole target to date.
- ❑ Technical capability for broad industrial sabotage.

- ❑ **Tunable Just-in-time Disruption**

ERP and Cartels analogous to al Qaeda-in-Iraq and nationalists

- ❑ **Iraq:** Iraqi Baathists, nationalists and insurgents vastly outnumber the jihadists.
- ❑ When it no longer serves the larger interests, the smaller will be exterminated.

- ❑ **Mexico:** ERP, paid or autonomous, is educating the cartels.
- ❑ When it is in the cartels' interest, the ERP can be exterminated or co-opted by a combination of money and force.

Cartel counterattacks

- Hyperviolence at the low end.
- Bribery and threats at the high end.
- Expand control of local state police assets.
- Cow and co-opt up the judicial chain.
- Attack the military intelligence community.
- Attack incorruptible senior judiciary.
- Co-opt fractious political opponents.
- Selective state disruption, damaging businesses.
- Isolate, emasculate Calderón.
- Failing that, assassinate him.

Cartels' ability to sever national critical infrastructures

□ Sector specific critical infrastructure:

- Energy
- Transportation
- Communication
- Oil and Gas
- Water
- Chemical
- Telecommunication
- Electricity

□ Domains:

- Physical and Network security
- Transportation security (Air, Ground and Rail)
- Personnel Security
- Disaster recovery, contingency planning and incident response.
- Security Policy and management

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.

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 Mexico, Brazil and China

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>