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

Intellectual Property and Investment Risk in Russia

Unique Russian characteristics

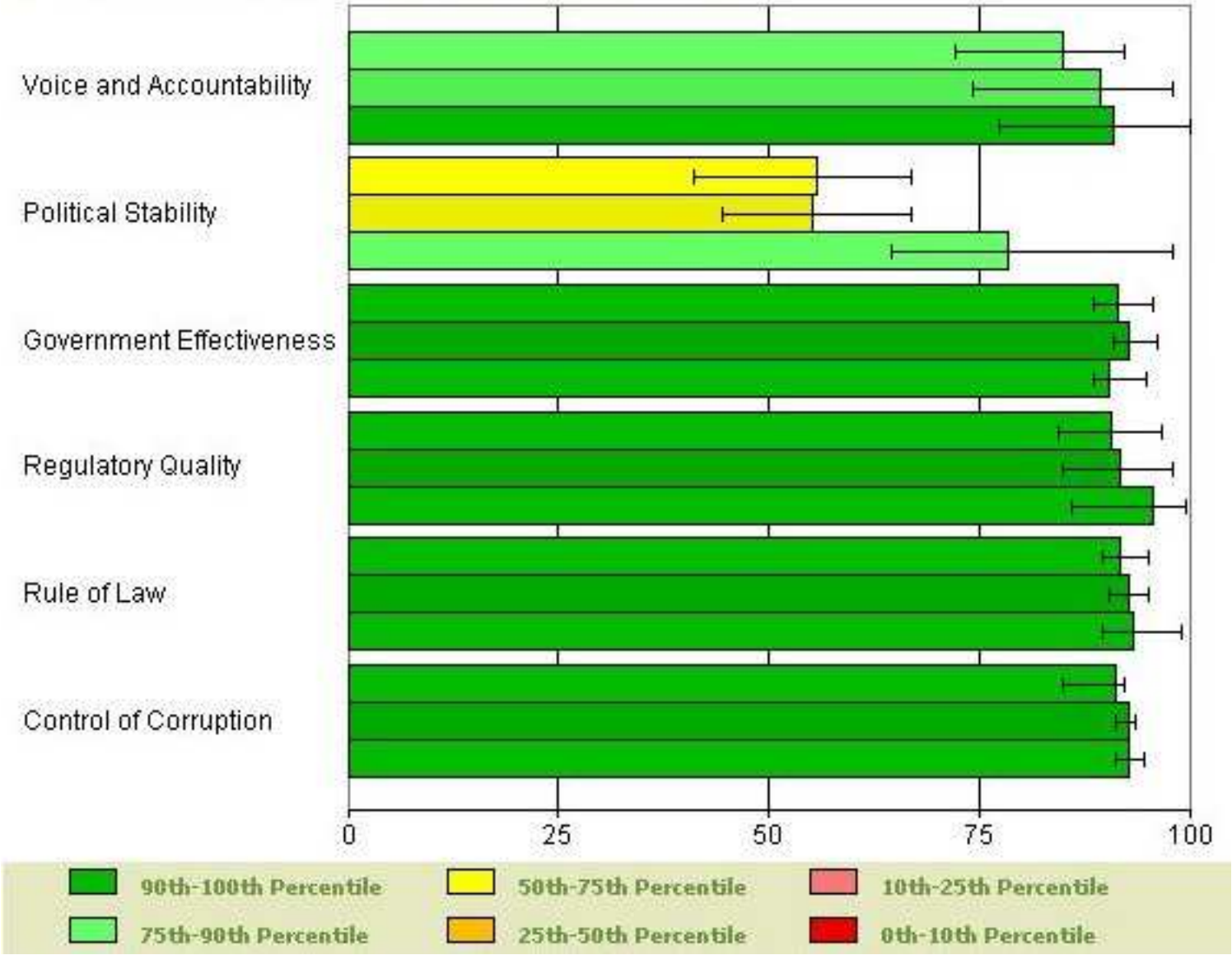
- Russia executes wide, state sponsored IP collection.
- Low protection for both transaction counterparties and IP.
- Key industries controlled by few politically connected persons/groups.
- Foreign investors confront continued lack of transparency.
- Bribery and corruption remain endemic.
- Low bank disclosure, very low against global peers; lower than largest Russian nonfinancial firms.
- Rapidly changing laws and unclear limits on foreign investments increase unpredictability.
- Current economic issues will increase predatory attacks.
- Protective investigation is essential for any entry.

Russian governance in global context

- **Voice and Accountability:** Ability to select government, freedom of expression/association, and free media.
- **Political Stability and Absence of Violence:** Likelihood of destabilization by unconstitutional or violent means.
- **Government Effectiveness:** Quality of public services, capacity of civil service and its independence from political pressures.
- **Regulatory Quality:** Ability of government to provide sound policies and regulations promoting private sector development.
- **Rule of Law:** Extent of confidence in rules of society, including quality of contract enforcement, property rights, police, courts, and likelihood of crime and violence.
- **Control of Corruption:** Exercise of public power for private gain, petty and grand forms of corruption, “capture” of the state by elites.

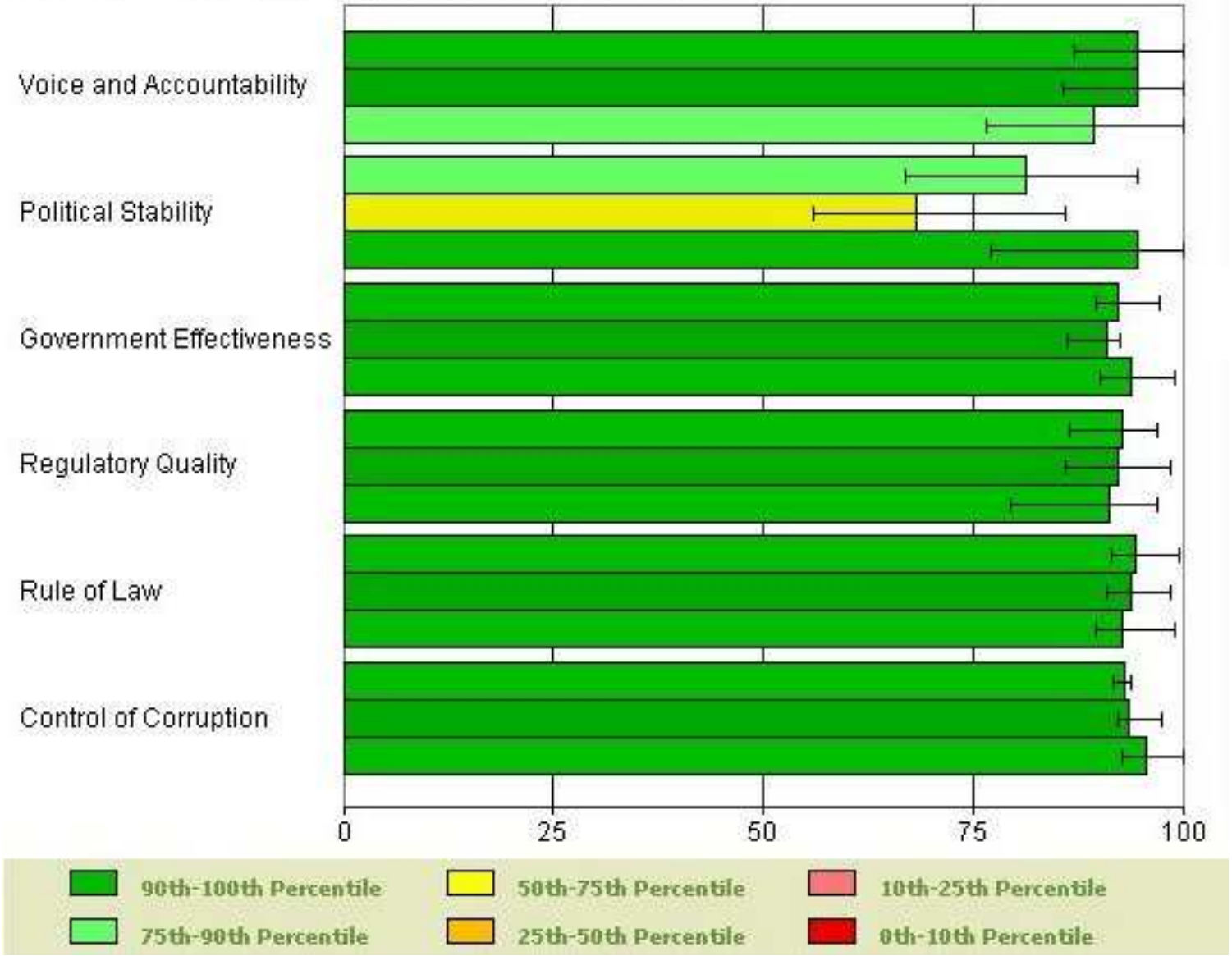
UNITED STATES

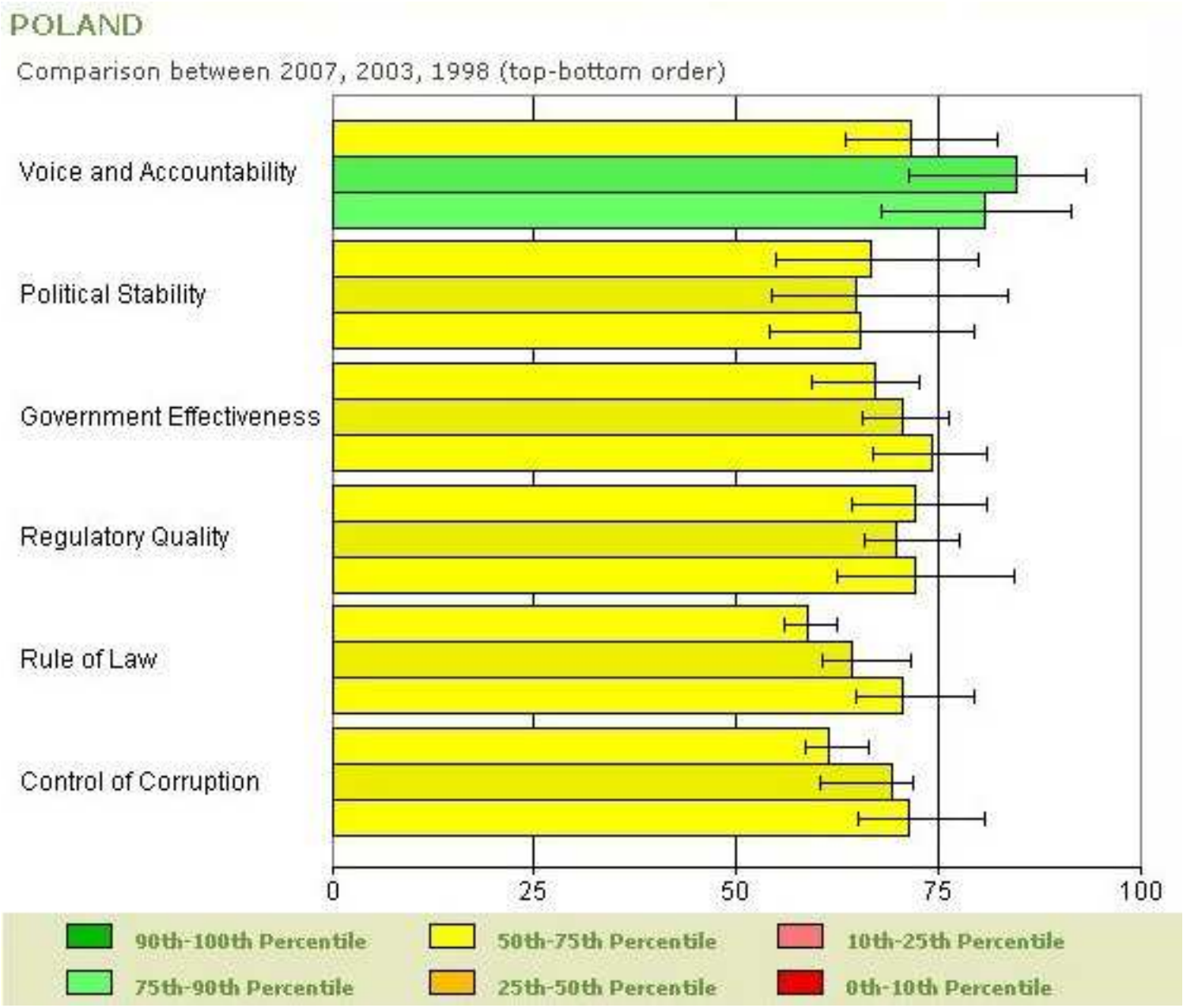
Comparison between 2007, 2003, 1998 (top-bottom order)



GERMANY

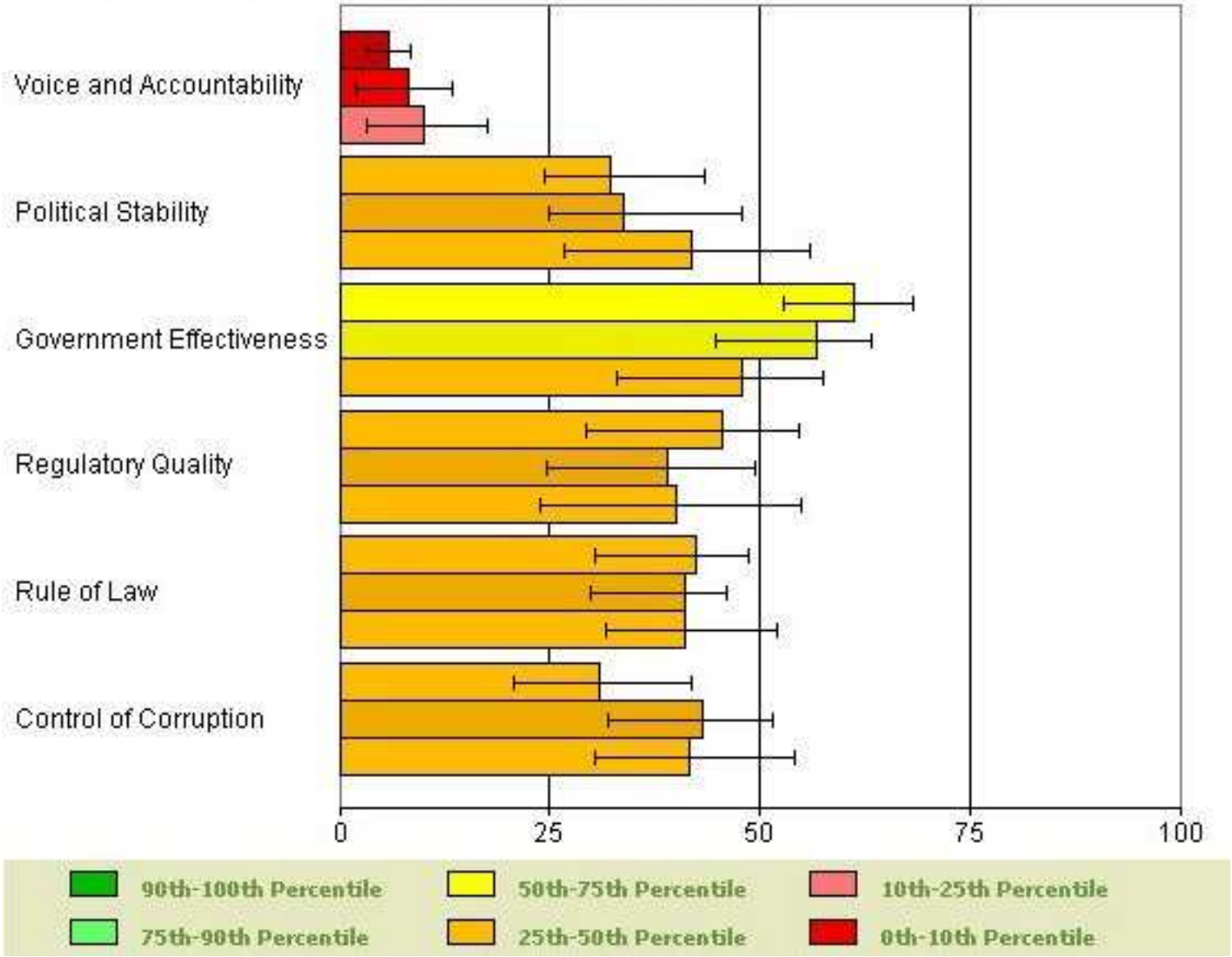
Comparison between 2007, 2003, 1998 (top-bottom order)




POLAND
Comparison between 2007, 2003, 1998 (top-bottom order)
Voice and Accountability
Political Stability
Government Effectiveness
Regulatory Quality
Rule of Law
Control of Corruption
0
25
50
75
100
90th-100th Percentile
75th-90th Percentile
50th-75th Percentile
25th-50th Percentile
10th-25th Percentile
0th-10th Percentile

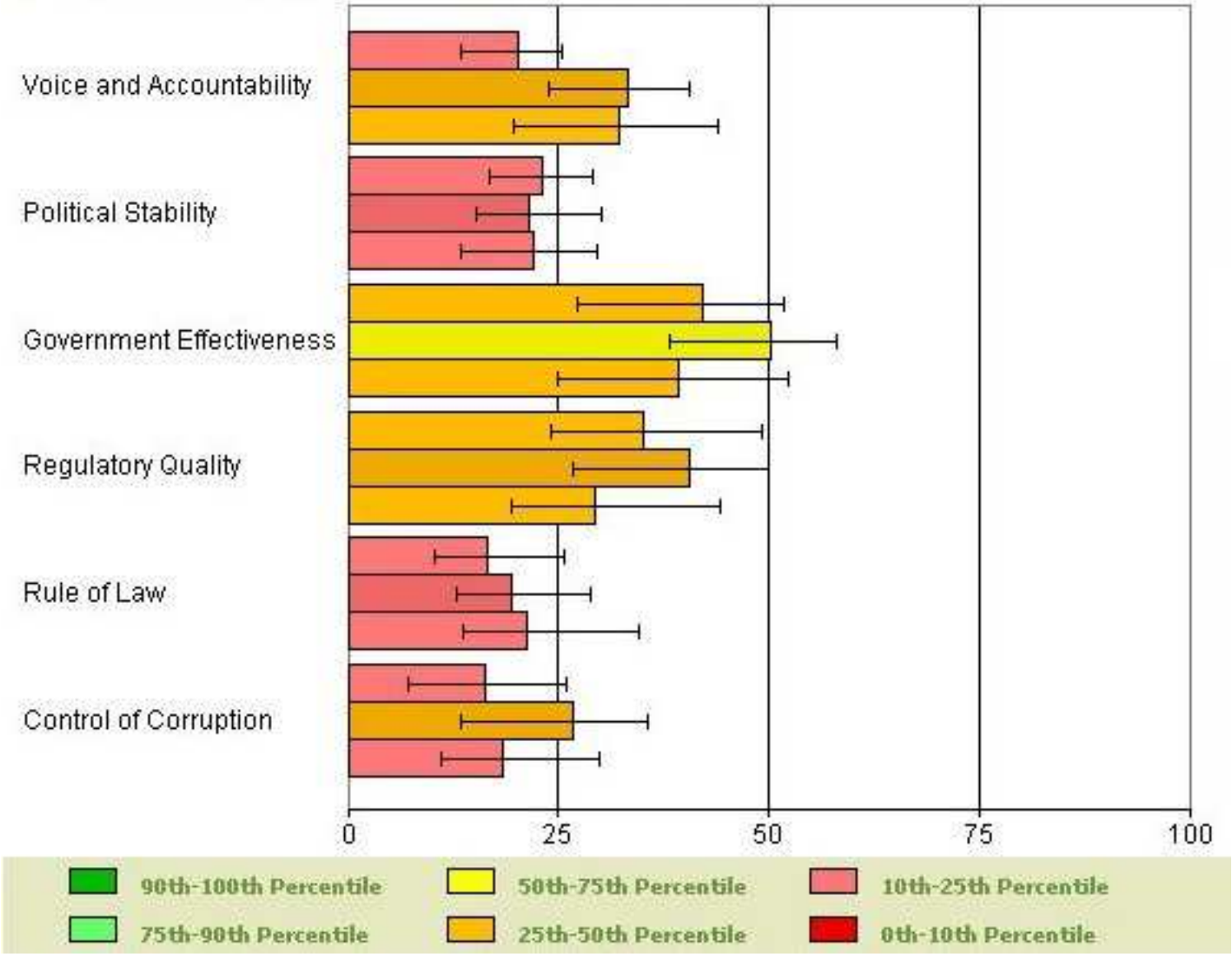
CHINA

Comparison between 2007, 2003, 1998 (top-bottom order)



RUSSIA

Comparison between 2007, 2003, 1998 (top-bottom order)



More risk, less transparency, than China

- Russia entails more risk than China with less transparency.
- Active state sponsored IP collection by multiple actors at multiple levels.
- Obsolete industrial infrastructure.
- Problematic supply chain consistency.
- Severe labor force issues, e.g., alcoholism, health issues.

Independent raters contrast with invested consultancies

- World Bank's Doing Business 2009 ranks Russia 120th of 181 economies in overall "Ease of Doing Business"
- Transparency International's 2008 Corruption Perceptions Index ranks Russia 147th of 180 countries.
- Transparency International's Bribe Payers Index for 2006 ranks Russia 28th of 30 countries.

Independent raters, cont'd

- World Economic Forum's 2008 Global Competitiveness Report ranks Russia 51th of 134 in the growth competitiveness index.
- MasterCard 2007 rating ranked Moscow 50th of 50 cities as desirable places to do business.

Wide variance in commercial ratings

- Different methodologies and target audiences.
- Non-transparent (confidential) methodology.
- Consider only publicly disclosed information.
- Detection/flagging of manipulated data.
- Conducted by market player.
- Subjective internal analyses.
- Rates only owned company shares.
- Does not consider Russian market specifics.
- Non-comprehensive sample set.
- Analyzes only listed (“liquid share”) companies.

Putting Standard & Poor's in perspective

- No dramatic improvement on disclosure despite rise in S & P transparency index.
- S & P upbeat picture due to studying transparency of largest companies, many of whom:
  - Have ADRs traded in the US.
  - Are registered in US, requiring US-level disclosure.
- Lesser, smaller firms have gaping information holes:
  - Information not disclosed for fear of state interference or unfriendly takeovers.
  - Disclosure purpose is search for strategic investors.

Standard & Poor's 2002 Russian transparency findings

- 42 Russian firms; total capitalization >90% of Russian stock market.
- Average disclosure: 34% - less than Pacific Rim and developing Asian countries, comparable to Latin America.
  - Management remuneration information: 11%.
  - Only 26 prepare annual reports in accordance with international standards.
  - 24 of 42 firms disclosed 50% of performance information.
  - Strong correlation between capital raising and information disclosure.

Russian-US Cooptation

- Cooptation - Cooperative competition
- Cooperation: Chechen insurgents, Islamic militants, DPRK, WMD materials.
- Competition: US/EU military and industrial secrets, Near Abroad, energy supply chains.
- Western espionage dipped 1989-1991, has not recovered operational levels.
- Soviet espionage dipped 1991-1993, has recovered operational levels.

Russian versus Soviet intelligence collection

- Operatives use more and varied covers.
- Morale near mid-1980s high.
- Diaspora created pool of co-optable, coercible émigrés.
- Restoration, even intensification, of activity in North America and Europe.
- Military technology 10 years behind US, now 25 years behind.
- Supply chain collection focus: Technology, components, operations, automation, assembly, manufacturing skills.

Federal Security Service (FSB)

- Successor to Committee for State Security (KGB).
- Estimate that 78% of top 1,000 political leaders worked with FSB or its predecessors.
- Vast network of former KGB/FSB officers permeates all sectors of Russian government and society.
- Acquired the Special Communications and Information Service – equivalent to the US NSA.
- Unlike US agencies, KGB/FSB collects and disseminates commercial intelligence.

Foreign Intelligence Service (SVR)

- Successor to former KGB First Directorate.
- Responsible for gathering of foreign intelligence through open and covert means.
- Structure comprises “lines” within geographical “directions” and separate task-specific directorates.
- Separate directorate dedicated to economic espionage and counterespionage.
- Separate directorates dedicated to specific countries, e.g., US and PRC.

SVR economic intelligence activities

- Threats to Russian interests.
- Emerging opportunities and market trends:
  - Scientific research, technologies, commodities and raw materials.
- Determine reputation and business potential of foreign firms and individuals intending to do business with Russian entities.
- Identify foreign firms attempting to conduct illegal activity with Russian partners.
- Track Russian capital going abroad.

SVR and KGB leverage Russian nationals

"Virtually every successful private company in Russia is being used as a cover for Russian intelligence operations"

- Russian nationals have little choice but to comply:
  - Russian entrepreneurs.
  - Russian nationals in-country.
  - Russian émigré communities abroad.
- Direct information sharing; response to tasking.
- Embedded operatives in legitimate firms.
- Front companies/shadow companies.

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.

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.

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.

Choose your advisors carefully

- 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.

Fiduciary implications

- Firms that do not understand this landscape are ripe for IP harvesting and investment losses.
- Legal remedies largely ineffectual and rewards moot as the IP is already lost and all expected downstream revenue is attenuated.

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.

Misadventure Analysis
Choose components wisely

- Asset market value trends downward from high value to commodity. Value loss can be mitigated if mature IP is integrated into systems led by high value assets.
- Difficult to isolate newer assets from the older in the production of integrated systems.
- Damage from IP loss moves progressively up the value chain, to newer and more vital IP as collectors retask to acquire more valuable IP.
- Compromise of high value asset compromises lead asset, maturing and mature components in the system.
- When IP loss occurs, it is likely that discovery will show damage to the business is not isolated and broader than anticipated.

Misadventure Analysis
Choose components wisely, 2

- No “build your own plant” option. Brownfield or Greenfield, owned or leased, someone else erects the building, installs HVAC, electricals, electronics and contracts security function and hires guards.
- Local option delivering protective control is feasible only with a complete IP asset protection program (including asset vulnerability assessments), and significant preparation in selecting and developing local supply chain relationships.

Misadventure Analysis
Break up assemblies

- Location-specific IP protection is a partial approach that rarely, if ever, adds much protective value for a global asset.
- Location-specific approaches often creates false sense of comfort on the protective side. Accessibility of the asset to hostile IP collectors at any tier, at any location, is key question.
- Asset-specific protection is global, requiring comprehensive view of asset accessibility in the supply chain.
- Becomes optimally effective on the basis of a complete asset (value chain) exposure assessment to be effective.

Misadventure Analysis
Select partners carefully

- Partnering merely shares risk of IP loss but does not control it.
- Partnering is not controlled and generates additional risk. (Note levels of IP transfer that already occur in any joint venture.)
- Education and a clear delineation of joint interests is usually required, but frequently hard to affect and enforce.
- Customers may not pre-disposed to cooperate with supplier IP protection efforts.

Misadventure Analysis
Exploit all legal options

- Unfortunately, any legal remedies come after the economic damage is done or is underway, i.e., the ROI and revenue loss are unrecoverable.
- Legal remedies are ineffective outside the US, parts of the EU and Australia, and may in fact be damaging to the litigating party.
- Legal strategy may be useful for asset sales or portfolio management (disposition), and will likely be necessary part of US-based due-diligence for Sarbanes Oxley compliance.
- It will have limited deterrent value at best for clandestine IP asset collectors.

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.

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.
- Avoid use of scenario analysis (omissive, has no end or scope-like business risk statement to bound it).

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.

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.

Due diligence, compliance & business strategy support

- Non-financial support:
  - Third party valuation (undisclosed valuation-relevant issues).
  - Investment/counterparties (factors that transfer risk).
  - Exposures beyond contractual and financial risk management.
  - Support requirements for governance and Foreign Corrupt Practices Act (FCPA).
- Business strategy:
  - Actionable information about specific industries, markets, prospects, and counterparties.
  - Due diligence on indigenous staff, review development prospects in-country.

Intellectual Property and Outsourcing Risk in Russia

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