OUTSOURCING:

IDENTIFYING AND MANAGING RISKS

THE OPEN GROUP
San Diego, CA February 5, 2004

Francoise Gilbert

650-804-1235

fgilbert@itlawgroup.com

Managing Director

IT Law Group

www.itlawgroup.com

555 Bryant Street Palo Alto, CA 94301

OUTSOURCING MODELS

- On-site
- Off-site
  - Within US
  - Off-shore
- Domestic, limited to US entity
- Global, for US company, its US and foreign subsidiaries
- Contract for services of an independent entity
- Contract for services of a controlled subsidiary

WHAT IS BEING OUTSOURCED

- Business Process Services
  - Data entry
  - Accounting
  - Customer relations, call center, customer support
  - Professional services; telemarketing
- Technology Services
  - Engineering design
  - Software development
  - R&D
  - Ecommerce
  - IT support

SUCCESS RATE?

- Outsourcing deals fail 50% of the time *(Computerworld November 3, 2003)*
- Half of outsourcing projects fails and must be renegotiated after 12-18 months *(Silicon.com, 11-21-03)*
- According to a survey by Diamond Cluster (Chicago consulting firm) 78% reported having prematurely ended at least one outsourcing contract (*Kansas city.com, 02-02-04*)
- To get the most from any outsourcing deal requires a lot of homework. Companies are not doing enough homework *(G. Tramacere - Gartner, quoted on Zdnet.com,11-21-03)*

SELECTED CONCERNS

- Poor quality of service; employee turnover
- Cost of managing the relationship: Businesses often focus on the short-term cost-cutting benefits of opting for outsourcing, without realizing the process may actually mean having to take on extra people in order to ensure there is staff with the right skills on hand to make the deal a success
- Standardization; one size fits all model. Outsourcing vendors require standardized operations and repeatable model
- Loss of business knowledge. Most organizations have substantial business knowledge that resides with their developers. This expertise may be proprietary and create a competitive advantage
- Loss of control over the Intellectual Property
- Loss of control over clients' personal information

OVERVIEW OF TODAY'S PRESENTATION

- Quality Control and Scope of Services
- Cost
- Employee Turnover
- Intellectual Property Protection and Ownership
- Privacy and Information Security
- Government Regulations
- Due Diligence and Contract Checklist

QUALITY ISSUES

- Quality problems with the outsourcing vendor may cause substantial problems:
  - Delays
  - Loss of customers
  - Returns
  - Obligation to terminate contract, and reinstate the prior operations

DEFINE SCOPE AND NATURE OF SERVICES

- Scope of services, and parties responsibilities
- Performance
  - Service levels
  - Standards of performance
  - Excuse of performance (force majeure)
  - Correction of processing errors
- Whether the vendor may/may not subcontract some of the services to third parties
- Qualification of employees

COST OF OUTSOURCING

- Companies expect that outsourcing will save money. However, there are additional / hidden costs
  - Vendor selection
  - Duplication of equipment
  - Travel
  - Communication; time zones
  - Additional management, supervision
  - Customer relationship
  - Transition; technology transfer; training
  - Lay off; US morale
  - Balance cost v. quality v. leading edge products

UNDERSTAND THE COST

- In the budget, and in the contract, identify to total cost
  - Fees
  - Expenses
  - Change in requirements
  - Taxes current and potential changes:
    - Indian income tax authorities have recently served notices on some Indian service companies engaged in telemarketing services asking them to furnish the particulars of the foreign principals. The income-tax authorities are trying to establish that foreign companies that have outsourced their jobs to India have a permanent establishment in India, and thus are responsible for the payment of taxes in India.
  - Hidden costs outside the contract payments, e.g. travel, supervision.
  - License restrictions. License to existing technology may not be assignable, transferable or sublicenseable to the vendor. Additional fees may be required.

RISK OF LOSS OF INTELLECTUAL CAPITAL - Employee Turnover

- Employees who are trained in the company's operation are key to the smooth operation of the outsourced service. When employees leave, quality suffers.
- In certain countries (e.g. India) there is a high demand for IT professionals. Vendor's employees may be tempted to switch jobs, This, in turn may result in disclosure or misuse of IP or trade secrets.
- Consider:
  - Designated employees allocated to the company's project
  - No solicitation clauses; no raiding clauses
  - Confidentiality, ownership, non competition contracts with personnel
  - Verifying that the local employment and labor laws will would help support the company in case of defection, competition

LOSS OF CONTROL OVER IP - IP Exposure

- When outsourcing, a company may have to disclose sensitive information to the third party
  - Risk that vendor will take company's IP and use it to help a competitor
  - Risk that vendor use its knowledge of the company's IP to enter into direct competition with company.
  - Risk of piracy and counterfeiting (e.g. Printer and ink cartridges; motherboard; integrated circuits)
  - Risk that vendor will not fully disclose developed or modified IP

RISK OF LOSS OF INTELLECTUAL PROPERTY - Trade Secrets

- Trade secrets are confidential business information that provides an enterprise with a competitive edge, (e.g. customer list, consumer profiles, sales methods, distribution methods, advertising strategies, list of suppliers).
- In order for a trade secret to maintain its status as a “trade secret”, it must be protected from disclosure to third parties through adequate safeguard

Trade Secrets (2)

- Theft or loss of trade secrets could occur
  - Internally:
    - Outsourcer does not have proper internal security policies
    - Outsourcer's employees work for several clients, including companies that are competitors
    - Source code or client list is used for improper purposes or transferred to a third party
  - Through disclosure to outsiders
    - Company technology is leaked out of outsourcer’s place of business (e.g. employees working from home)
    - Outsourcer’s employees leave to work for a competitor

RISK OF LOSS OF INTELLECTUAL PROPERTY - Copyrights

- Copyright laws protect work of authorship. Laws vary from one country to the other. Not all same types of works are protected. E.g. database are protected in the EU (sui generis protection), but not in the US.
- Copyrighted materials could be misappropriated
  - Piracy
  - Misuse, e.g.
    - Source code is used for other purposes
    - Client list is sold or disclosed to third parties
    - Employees working from home have access outside company's premises and may “share” IP with third parties.

RISK OF LOSS OF INTELLECTUAL PROPERTY - Patents

- In general patent protection is limited to the country in which the patent application is filed and maintained. To obtain patent protection in a foreign country, additional filings are required.
- Patent laws differ from one country to another. Some countries require that the invention be kept confidential prior to filing.
- Ensure that the outsourcing company is not entrusted with developments that might be subject to patents, or if it is, ensure that patents rights are preserved (e.g. shop rights, assignments, confidentiality requirements)
- Don’t outsource key technology work until a patent is filed.
- If you want to do innovative work offshore, establish your own R&D center.

RISK OF LOS OF INTELLECTUAL PROPERTY - Trademarks

- Trademarks are protected only in the country where the trademark application was filed
- To obtain trademark protection in a foreign country, there must be an additional filing in that country (or through Madrid Protocol filing)
- Ensure that the outsourcing company is protecting the trademarks, and not misusing them or helping others (counterfeiting, piracy)
- Filing trademark application(s) in the country or region may help protect against piracy.

RISK OF PRIVACY RIGHTS VIOLATIONS (1)

- In the United States:
  - Some laws preclude or limit entities operating in certain fields (e.g. finance, healthcare) from sharing personally identifiable information with third parties (e.g. GLB, HIPAA Regs)
  - Prior notice to and/or consent of the customer may be required
  - Written agreement with the subcontractor or outsourcer may be required, with specific provisions, dictated by law (e.g. HIPAA Business Associate Agreements)
  - Adequate security measures must be in place

PRIVACY (2)

- Currently, over 50 countries have substantial data protection laws with strong privacy protection requirements, and data rights for the data subjects.
- If a US company has operations abroad that will be outsourced as well, it must *in addition* ensure that outsourcing is not contrary to the local laws that govern its subsidiaries
- EU Countries prohibit transfer of data to a third party located outside the country's border unless specific requirements are fulfilled (e.g. customer consent, contract with the third party with strenuous requirements), or unless the country where the data is transferred has been deemed to offer "adequate" data protection
- Similar restrictions in non EU countries with strong privacy laws based on the EU model

PRIVACY (3)

- Even when there are no laws prohibiting data transfers to a third party, the company may have made representations in its privacy policy that it would not transfer personally identifiable information (e.g. which it collects on its website) to a third party.
- Attempting to transfer or disclose the database of client information to a third party may be a violation of the privacy policy.

PRIVACY (4)

- Many countries that provide outsourcing services do not have privacy laws currently include India, China, Malaysia, and others.
- Absent adequate privacy laws:
  - There is no recourse against private parties for improper processing or use of data.
  - An off-shore company would have no guidance regarding which standard to apply to ensure that electronically transferred data are adequately protected.

IP EXPOSURE

- Before outsourcing off-shore, ensure that the foreign country has in place adequate measures to fight piracy, and intellectual property protection laws.
- Absent adequate intellectual property protection laws, laws, a company would have no recourse against a third party that would sell counterfeit goods made using technology or dies provided to an outsourcer. Only a breach of contract action would be possible against the outsourcer itself, if actual contract provisions had been violated to permit the piracy.

DEFINE THE SCOPE OF USE OF CRITICAL ASSETS

- Software; Documentation
  - Assignment of licenses
  - Scope of use of software, documentation
  - Escrow of source code
  - Right to modify
- Data and Personal Information
  - Scope of use of data
  - Ownership of data
  - Return of data upon termination
  - Privacy and security
- Confidential and Proprietary Information
  - Trade secret protection
  - Information privacy and security protection policies
  - Intellectual property protection policies

COMPLIANCE with Government regulations

- Certain companies are subject to government regulations (e.g. financial, healthcare)
- Certain activities may require audits from government agencies
- Sarbanes Oxley increases the requirements for reporting, monitoring, and requires assurances as to data quality and accuracy
- 13+ states (including California) have bills pending that would forbid government contract providers from outsourcing offshore
- Export control laws may restrict the exportation of certain sensitive data

DUE DILIGENCE BEFORE OUTSOURCING - *selected issues*

- Are there restrictions to company's giving access to its technology or customer information to a third party? E.g. license restrictions, contracts with third parties, confidentiality agreements
- Can company's licenses be assigned, transferred or sublicensed to a third party?
- Are there export control restrictions?
- What would be the actual cost of outsourcing, e.g. transition, supervision, control, travel to site
- What are the tax consequences?

DUE DILIGENCE (2)

- What are company's privacy, security, confidentiality needs?
- Are company's needs and requirements compatible with vendor's current operations? The vendor's subcontractors?
- Does the vendor have sufficient resource to fulfill these needs? Respond to an audit? Comply with individual rights of access to and amendment of personal information?
- What data protection and IP protection laws are in place in vendor's country? Are they enforced? How?
- What conflicts does the vendor have? Are any of company's competitors clients or protects of vendor ?
- What are the political risks?

THE OUTSOURCING CONTRACT - selected issues

- Allocation of responsibilities
- Change process, pricing and other consequences, e.g.changes in requirements, company size, laws
- Guidelines and policies for confidentiality, security, integrity, accessibility of the data, IP protection
- Disaster recovery and business continuity procedures; and audit thereof
- Pricing, exchange rate, inflation rate, tax, royalty issues, expenses, travel expenses
- Vendor’s assistance in fulfilling company’s obligations to clients, employees or law enforcement authority

CONTRACT (2)

- Scope of use of company's IP and personal data
- Ownership of PII and IP collected or created during the relationship
- Vendor's ability (or not) to subcontract portion of its obligations to third parties
- Warranties and remedies
- Periodic audits to ensure compliance with contract
- Termination of the relationship
- Disposition, allocation, transfer of the databases upon termination or at any time during the relationship

QUESTIONS?

Francoise Gilbert

IT Law Group

fgilbert@itlawgroup.com

650-804-1235

www.itlawgroup.com