MAYER·BROWN

Business & Technology Sourcing Review

Issue 11 Q1/Q2, 2008

www.mayerbrown.com

Editors' Note

Mayer Brown Expands in Asia

We are proud to announce that in January 2008, Mayer Brown combined with leading Asian law firm JSM (formerly Johnson Stokes & Master) to broaden our presence in the fastest growing economies in the world.

Our firm recognizes the increasingly important markets for our clients and continues to provide truly global services by strengthening our worldwide platform. We now have more than 1,000 lawyers in the Americas, 300 in Asia and 500 in Europe.

This on-the-ground presence in the Asian market significantly enhances our capabilities to serve your strategic sourcing projects in the region. We have included an article in this edition addressing *Going to China* and the market considerations, challenges and strategies for sourcing from China.

New Guest Column

We are also pleased to launch a new guest column contribution to our Review, which starts on page 29. Our goal is to feature various industry experts who we work with in outsourcing, sourcing or general technology projects. We believe you will benefit from their insights, experiences and trusted opinions.

Our first guest column is from UMS Advisory, Inc., which will cover pricing and risk allocation for mission-critical transactions.

Experience counts in the rapidly changing sourcing marketplace. Mayer Brown brings the depth, breadth, experience, flexibility and tools to drive value in the sourcing process and help you succeed.

We'd like to hear from you with suggestions for future articles and comments on our current compilation. Please email us at marketing@mayerbrown.com.

If you'd like to contact any of the authors featured in this publication with questions or comments, we welcome your interest to reach out to them directly. If you are not currently on our mailing list, or would like a colleague to receive this publication, please email contact.edits@mayerbrown.com with full details.

Going to China

Geofrey L. Master

Geof has broad experience in outsourcing and procurement transactions, including the outsourcing and offshoring of business processes and functions, as well as information technology and services. Geof's clients have ranged from start-up enterprises to national and global firms and government organizations.

202 263 3270

gmaster@mayerbrown.com

"Going to China" is something heard with increasing frequency from companies looking for value and quality in their sourcing of products and services — and with good reason. China is the manufacturer of a significant and increasing amount of the world's products. It is also intent on becoming a leading provider of services.

From its economic opening 30 years ago, China has been driving an economic development that will enable it to create a middle class society of reasonable means. This transformation stands as an undertaking of historic proportions. Initially, China focused its economic development on manufacturing and the successes have been dramatic. Increasingly, however, China has been focusing its manufacturing capabilities on higher-end products and processes, including pharmaceuticals and electronics and other technology.

Despite its success, China needs substantially more economic development. It also needs to address some of the undesired consequences of its staggering growth. Notably, China needs to address a rapidly urbanizing population[1] and the significant environmental issues associated with its current manufacturing industries, including the consequences of heavy polluters and high energy consumption in low-end manufacturing. In the face of these needs and associated domestic and international pressure, the Chinese government has developed its current "Harmonious Society" socio-economic goal of advancing economic growth that promotes better societal balance. As part of its effort to promote such balance, China is now making a very concerted effort to grow its services industry, seeking to leverage its successes as the world's manufacturer to become the world's services provider.

The Chinese market for the sourcing of products and services is dynamic and evolving. Would-be buyers of products and services from China must carefully analyze the market to determine which products or services can be viably sourced from China and the appropriate manner for arranging such sourcing. Approached properly, however, for a growing number of products and services, China ranks as one of the most attractive sourcing markets in the world and indications point toward this trend continuing, if not accelerating.

Fortunately, would-be buyers of products or services from China can draw on lessons learned from many years of sourcing experience, their own and those of others. Although different sourcing environments inevitably present certain unique challenges and combinations of challenges, prior sourcing experience of buyers over many years can be leveraged to enable would-be buyers to approach China sourcing with significantly heightened confidence and capability, positioning themselves not only to benefit from current China sourcing opportunities, but also to grow and evolve their China exposure as further opportunities develop, while maintaining manageable levels of risk.

The China Sourcing Environment

The Chinese government has embraced the notion that developing services capabilities offers significant economic development benefits, consistent with its Harmonious Society objectives. The need to encourage development of its services industry is all the more urgent for China because portions of its current manufacturing base will almost certainly not survive the transition to an acceptable, ecologically responsible production environment. The result has been a trend away from the dominant manufacturing focus, evidenced by a steady reduction of processing trade incentives over the past five years and an increasing emphasis on higher-end production and processes, including services.

With a clear eye toward India's success in its outsourcing services industry, the Chinese government has designated 11 cities to be "Outsourcing Services Base Cities"[2] where it is concentrating infrastructure developments and incentives. Through such efforts, China is seeking to encourage multinational companies to shift offshore outsourcing services to China, as well as to promote the development of large and medium service outsourcing enterprises, with particular focus on software and technology-related service providers. In addition, a number of other regional and municipal governments have taken it upon themselves to implement programs promoting development of services industries in their areas, all in the effort to promote the Harmonious Society objectives.

The Contract – Special Challenge to Sourcing from China

One of the significant challenges facing any buyer interested in sourcing from China involves the sourcing contract. Significant sourcing arrangements, especially those involving services, are typically based upon sophisticated contractual arrangements in which the buyers must have reasonable confidence that their contractual rights are enforceable. Serious limitations on either of these sourcing prerequisites (contract and enforceability) will limit the extent to which buyers will view any sourcing opportunity as viable, irrespective of the actual capabilities of the supplier.

The Chinese government has embraced the notion that developing services capabilities offers significant economic development benefits, consistent with its Harmonious Society objectives.

A supportive contracting environment is dependent upon two factors: first, a level of commercial contracting capability on the part of suppliers to enable buyers (and suppliers) to negotiate and execute acceptable contracts; second, a legal infrastructure that affords reasonably efficient and predictable enforcement of such contracts. Within China, both these factors stand as works in progress. The adoption of laws in China over the past 10 to 15 years supporting commercial transactions has been dramatic. In fact, by many estimations, China has adopted a reasonably adequate base of commercial law. The major challenge facing China in this area, however, is the enforcement of those laws.

The challenges associated with contracting in China are of greater significance in services transactions than in product sourcing transactions. Service contracts are typically more complex than product contracts — reflecting, in many ways, the practical differences between services and products, including the frequently more interactive relationship between buyer and supplier involved in the provision and receipt of services. Thus, as China looks to build its capabilities, effectively building its contracting capacity is a critical challenge. As effective enforcement of law is developed, the scope of both products and services viewed as viable candidates for sourcing from China will almost certainly increase. In turn, the contracting capability of Chinese suppliers to support such broader range of sourcing transactions will undoubtedly develop as the opportunities for such development are presented.

Other Challenges and Strengths of China Sourcing

There are a number of other challenges to sourcing from China that may impact whether, or the way in which, a particular sourcing is undertaken. These challenges include the level of English ability within China, concerns over intellectual property protection and regulatory compliance, and arrangements for effective dispute resolution.

The level of English ability within China is frequently noted as a challenge facing international businesses considering sourcing from China. Despite the prevalence of Chinese as a spoken language (by some accounts the world's most widely spoken language), English continues to be the primary language for international business communication. While a number of the services initially targeted by the Chinese government for development (for example, software services that involve work in common programming languages) are not wholly dependent on broad English capabilities throughout the supplier organizations, English language ability still stands as a challenge impacting the scope and nature of sourcing that many buyers believe can be currently undertaken effectively from China.

As effective enforcement of law is developed, the scope of both products and services viewed as viable candidates for sourcing from China will almost certainly increase.

Significant efforts are underway to increase English capability within China. For example, beginning in 2001, English became compulsory throughout the country from Grade 3, and larger cities such as Beijing and Shanghai have introduced English at Grade 1. Through such efforts, the significance of this issue will no doubt diminish over time. In fact, some have estimated that within a few years there may be more English speakers in China than in India.

Protection of intellectual property is another concern. Despite China's adoption of laws generally consistent with international standards of intellectual property protection, enforcement of these rights remains a significant problem. A variety of best practices can be helpful in protecting intellectual property, including careful due diligence in human resource and business partner selection and thoughtful design, implementation and enforcement of intellectual property compliance programs. Further, practical protections

based in the design and control of the production and performance processes may provide effective protection for critical intellectual property — by not allowing it to be accessed and copied in high risk environments. Such an approach often involves compartmentalizing activities and sourcing different parts or processes to different suppliers or in some cases retain critical portions within the buyer's home organization. Where such arrangements are not feasible, and critical intellectual property will be unavoidably accessible and subject to being copied, the owning company may determine that certain products or services are not currently suitable for sourcing from China.

Actual enforcement of arbitral awards in China present their own set of challenges, which must be considered in any sourcing evaluation and structure.

Another area of concern for prospective buyers considering sourcing from China is regulatory compliance. For example, US buyers must address compliance issues associated with US export control laws, the US Foreign Corrupt Practices Act, and Sarbanes-Oxley obligations that might be impacted through sourcing arrangements. As with intellectual property protection, regulatory compliance can be promoted through care in human resource and business partner selection and well designed and implemented compliance programs. However, certain activities may simply be inappropriate candidates for sourcing due to the regulatory risks. Further, care must be taken that the sourcing contract provides necessary flexibility for addressing changes in applicable regulatory requirements — reflecting the sophistication required in sourcing contracts.

Effective dispute resolution is another concern for companies considering sourcing from China. This concern is particularly pronounced in view of the previously noted challenges associated with contract interpretation and enforcement in China. International sourcing arrangements frequently provide for a governing law other than China's and for a dispute resolution process that is not dependent upon the developing legal infrastructure of China.

Choice of law provisions in contracts are generally recognized in China, although a number of important issues remain subject to local law, including certain issues concerning intellectual property ownership, labor laws, land ownership, insolvency and enforcement of foreign judgments or awards. The process for dispute resolution frequently desired by foreign companies sourcing from China (after efforts at negotiation between the parties have failed) is arbitration conducted outside of China under an international alternative arbitration in China. Such arrangements must be clearly stipulated in the sourcing contract. Finally, however, actual enforcement of arbitral awards in China present their own set of challenges, which must be considered in any sourcing evaluation and structure.

Sourcing Market Considerations in China

Two additional factors respecting sourcing from China present specific challenges to would-be buyers from China. These are the fragmented service provider market and the

challenges of performing effective due diligence on Chinese service providers and other business partners in China.

China's nascent services industry is extremely fragmented, with no reasonably defined set of leading service providers. The government's efforts to develop the services industry have been focused largely on general development in the various designated base cities, without concerted focus on defining and developing specific capabilities. The result is that the market is diffused with competition among the cities and regions that has tended to dissipate any development of a distinctive China services practice or brand. In short, there tends to be more and more to choose from in China in terms of service offerings, but not a strongly coherent pattern of practice or even capability.

Ultimately, success or failure of any product or services sourcing from China is largely dependent upon the quality and capabilities of the supplier, as well as other business consultants and partners used in the China activities. Effective due diligence on Chinese parties tends to be a significant challenge. This is due to a wide variety of factors, including the fragmented market as well as language and cultural issues. It is very important, however, for a company to obtain a clear understanding and adequate comfort level regarding the capabilities and ethical standards of the parties with which it is dealing. Effective due diligence often requires significant patience, effort and expense, but its importance must not be underestimated.

Strategies and Vehicles for Initiating Sourcing from China

China's liberalized investment rules generally allow a foreign buyer looking to source products or services to select from a wide range of sourcing models: including classic third party outsourcing arrangements where the buyer contracts with the supplier, sourcing through joint ventures and even through wholly owned (foreign) enterprises. As with any sourcing, the challenge is adopting the most appropriate model for the particular transaction mix — considering the buyer, the supplier and the subject of the sourcing. Fortunately, buyers seeking to source from China can utilize most of the strategies historically used in offshore sourcing.

Success or failure of any product or services sourcing from China is largely dependent upon the quality and capabilities of the supplier, as well as other business consultants and partners used in the China activities.

For example, a buyer may initiate its China sourcing through any, or a combination of, the following classic entry strategies:

- Utilization of pilot programs to become familiar with and confirm viability of the sourcing (test the waters) — although this approach carries risks of insufficient commitment which can set the stage for failure;

- Providing for an extended transition period to allow for confirmation of successful assumption of responsibility and performance by the supplier — although this approach, like the pilot program, can carry the risk of insufficient commitment, making change management associated with the sourcing more difficult;
- Utilizing of shorter term contracts with extension rights to allow for flexibility in substituting solutions — although this approach can be less attractive to suppliers and nonetheless create a long-term dependence on the part of the buyer despite the shorter term; and
- Limiting offshore direct reliance and exposure by utilizing a US or other home-country supplier with China capabilities — although this strategy necessarily reduces savings opportunities.

Again, lessons learned from prior sourcing experiences can and should be applied in evaluating and approaching the dynamic and evolving Chinese sourcing market.

Expectations for China Sourcing

Despite the challenges currently presented in sourcing from China, the potential benefits are compelling. As China further addresses areas of concern to international buyers, these benefits should increase as the risks decrease. The economic stakes for China are high. There is every expectation that, through its government and growing ranks of suppliers, China is, and will remain, vitally interested in developing and maintaining an environment that will enable international buyers to source from China with increasing confidence and enthusiasm. ◆

Endnotes

1 Urbanization is generally recognized as both a product of economic development and prerequisite for broad-based economic development. China's urbanization remains significantly lower than other developed countries and as a concerted governmental policy, China is promoting very rapid urbanization.

2 The eleven cities designated as Outsourcing Services Base Cities are: Chengdu, Dalian, Shenzhen, Shanghai, Xi'an, Beijing, Tianjin, Nanjing, Wuhan, Jinan and Hangzhou.

Offshoring to India: Are Your Trade Secrets and Confidential Information Adequately Protected?

Sonia Baldia

Sonia, based in Washington, DC, counsels corporate clients in onshore and offshore outsourcing, cross-border technology transfers, strategic alliance arrangements, intellectual property acquisition, development, marketing and distribution agreements, licensing arrangements, and consulting services agreements. A significant portion of her practice involves India-related matters.

202 263 3395

sbaldia@mayerbrown.com

Despite recent growth in other emerging markets, India continues to be the number one destination for outsourcing services involving information technology and business processes ("IT/BPO services"). In recent years, moreover, a new model of global sourcing to India known as knowledge process offshoring or "KPO" has taken hold in addition to the remarkably successful Indian market for IT/BPO services, with India emerging again as the global KPO "hot spot." KPO involves the offshore outsourcing of knowledge-driven or "high end" processes that require specialized domain expertise, including such varied areas as R&D, insurance underwriting and risk assessment, financial analysis, data mining, investment research, statistical analysis, tax preparation, engineering and design, animation, graphics simulation, medical services, clinical trials, legal services, and more. As offshoring of services to India moves up the value chain from IT/BPO services to KPO, protection of intellectual property (IP), including any trade secrets and confidential information, that may be transferred or created in India becomes an even more critical concern for the offshoring customer. IP concerns must be addressed knowledgeably to achieve and maximize the benefits and strategic incentives the offshoring model offers without losing control of critical customer IP. This article raises some of the key issues that any offshoring customer should carefully assess so as to mitigate the risks associated with offshoring trade secrets and other confidential information to India.

When offshoring a "high end" process or functionality to India, often much of the knowledge transferred offshore (for example, source code, formulae, designs, specifications, or experimental data) is confidential in nature and generally not suitable for local registrations in the form of patents. It, therefore, becomes critical for the US customer to seriously consider – before it begins the offshoring process — how it will best protect this information to maintain its competitive advantage. A primary concern for a US customer should be the Indian service provider's ability and willingness to safeguard the customer's trade secrets and other commercially valuable confidential information against misappropriation, misuse, unauthorized disclosure, sabotage or theft.

India's Existing Legal Framework for Trade Secrets

In the US, trade secrets are afforded statutory protection, both at the federal and state levels, with meaningful civil and criminal remedies to counter the misappropriation of trade secrets, including compensatory and punitive damages, injunctive relief, and attorneys' fees. That is not the case in India. India provides no statutory or other legal protection of

trade secrets. This non-legal environment presents a number of challenges concerning trade secret protection and enforcement and can jeopardize a US customer's IP unless it carefully employs certain contractual mechanisms that are enforceable in India. In India, parties must primarily rely on contracts to protect trade secrets. Indian law does recognize the common law tort of "breach of confidence" irrespective of the existence of a contract. But the tort's utility is limited in an offshore sourcing context because the duty of confidence at issue can be enforced only against a party that is either a fiduciary to the US customer or in an employer-employee relationship with the complaining party. Also, the duty arguably only extends to the unauthorized disclosure of confidential information to a third party and does not prevent the recipient's own "misappropriation" of the information.

Perils of Subcontracting

Consider the following hypothetical involving an Indian service provider that has engaged a subcontractor in India to perform the offshored services for a US customer. If the Indian subcontractor discloses or misappropriates the US customer's trade secrets or confidential information, the US customer has neither a breach of confidence claim against the subcontractor nor a breach of contract claim, unless the US customer has contracted directly with the subcontractor, which is typically unlikely. The contract between the US customer and the Indian service provider might well hold the service provider liable for damages caused by the subcontractor's inappropriate disclosure, but that cause of action still does not directly address or foreclose the subcontractor's past and possibly future misconduct. Essentially, the US customer is left without a direct remedy against the Indian subcontractor and without an immediate legal means to effectively stop the disclosure.

This non-legal environment presents a number of challenges concerning trade secret protection and enforcement and can jeopardize a US customer's IP unless it carefully employs certain contractual mechanisms that are enforceable in India.

Employee Misconduct

This concern with third-party subcontractor misconduct unfortunately also exists with respect to the misconduct of employees and ex-employees of the Indian service provider. Surveys reveal that a majority of instances of data misconduct arise from employees or ex-employees of a service provider. Recent instances reported in international media involving theft of trade secrets of western companies offshoring to India further illustrate the gaps in India's IP law that expose the vulnerability of IP in offshore transactions. In 2002, an ex-employee of an Indian software vendor, Geometric Software Solutions Ltd., was attempting to sell proprietary software source code owned by SolidWorks, a US client of the person's ex-employer, to the US client's competitors. Even though the ex-employee was caught red-handed in a sting operation, he could not be effectively prosecuted in India because the source code was considered a trade secret and Indian law did not recognize "misappropriation" of trade secrets and the US client did not have any contractual arrangements with the ex-employee whereby it could directly enforce its rights against the ex-employee. Similarly, in

2004, an employee at an India-based software development center of a US customer, Jolly Technologies, misappropriated portions of the company's source code by allegedly uploading and shipping files that contained source code for a key product to her personal Yahoo e-mail account. The theft was detected in time to prevent the employee from distributing the stolen code but the US customer also could not successfully prosecute the employee because of the same gap in Indian IP law. These cases have drawn close scrutiny and served as a wake-up call to the global sourcing community as well as the Indian outsourcing industry prompting Indian industry to aggressively lobby the Indian government to strengthen India's IP regime and demonstrate to the foreign investor community that India takes foreign IP more seriously.

The perils of subcontractor and employee misconduct as to IP in India are very real. It is critical, therefore, for a US customer to be aware of this enforcement gap and address it in the operative contract with the Indian service provider and in the contracts between the Indian service provider and its subcontractors.

Effective Strategies to Safeguard Trade Secrets and Confidential Information Offshored to India

DRAFTING COMPREHENSIVE CONFIDENTIALITY AND IP OWNERSHIP AGREEMENTS THAT ARE ENFORCEABLE IN INDIA

Trade secrets and confidential information must be protected through the contractual arrangement between the US customer and the Indian service provider and there should also be a contractual relationship between that service provider and its subcontractors that includes an express right of enforcement by the US customer against the subcontractors. The contract provisions should, as clearly and as effectively as possible, prohibit the wrongful disclosure and misappropriation of trade secrets and proprietary data by the service provider and the subcontractor(s); the contracts should make equally clear and expressly acknowledge the US customer's right to enforce violation of these provisions for damages and the customer's right to seek to enjoin such wrongful acts locally.

Confidentiality and non-competition covenants are enforceable under Indian law and offer a line of defense in the US customer's efforts to protect trade secrets and confidential information in India. A US customer must therefore insist upon unambiguous provisions in the operative contract that require the Indian service provider to (i) maintain the customer's trade secrets and confidential information in strict confidence not only during the term of the contract but also after termination, (ii) permit controlled access on a "need to know" basis only, including the customer's right to enforce such obligations directly against service provider personnel having access to the customer's information, and (iii) be contractually responsible and liable for any breach of confidentiality obligation or misuse of such information by itself, its subcontractors, employees or former employees. A service provider's failure to comply with the confidentiality obligations should not only permit the customer to immediately terminate the contract but also result in uncapped financial consequences to the service provider.

PERFORMING DUE DILIGENCE TO AVOID CHAIN OF TITLE ISSUES AND ENSURE PASS-THROUGH NON-DISCLOSURE OBLIGATIONS

Needless to say, because prevention is better than cure, a US customer should conduct thorough due diligence regarding the Indian service provider's track record of maintaining data security. Prior to entering into a final contractual arrangement, a US customer should perform due diligence as thoroughly as possible to make sure that the Indian service provider has written employment agreements in place with its employees and consultants addressing IP ownership and non-disclosure obligations and closely scrutinize such agreements to make sure they are sufficiently protective of the US customer's rights and interests, and are valid and enforceable under Indian law. To the extent practicable, and depending on the nature and sensitivity of the US customer's IP involved in the project, a customer should consider entering into non-disclosure and IP ownership agreements directly with the Indian service provider's employees and consultants assigned to the project. By doing so, the confidentiality and IP ownership obligations should remain in force even after the employee or consultant is no longer employed or engaged by the Indian service provider and the US customer will have contractual privity with such employees and consultants and legal standing to sue in India, as well presumably in other venues, in the event of a breach of their obligations.

Subcontracting by the Indian service provider can dramatically increase the IP risk profile.

IMPOSING NON-COMPETE RESTRICTIONS THAT ARE ENFORCEABLE IN INDIA

The operative contract should also include non-competition covenants that restrict the Indian service provider from using competitive technology or personnel in connection with the customer's competitors. The US customer must bear in mind, however, that India has stringent laws against overly restrictive trade practices and therefore the enforceability of a non-compete covenant is subject to a case-by-case determination and any particular terms cannot in every case be assumed to be enforceable. More specifically, the Indian Contract Act provides that a non-compete agreement will not be enforced to the extent that it restrains a person from exercising a lawful profession, trade or business. Judicial precedent under Indian law indicates, however, that an Indian court will enforce a restrictive covenant if it meets what is known as a "reasonableness" test. For example, a restrictive covenant imposed during the period of the subject's employment is more likely to be upheld than a covenant operating after the termination of employment. In *Niranjan Shankar Golikari v. The Century Spinning & Manufacturing Co. Ltd.*, the Supreme Court of India upheld a restrictive clause in an employment contract, which imposed constraints on the employee not to reveal or misuse during the period of the employment any trade secrets that the employee learned while employed. Another example of the application of the "reasonableness" test is that Indian courts also typically apply a stricter level of scrutiny to non-competition provisions in contracts for the provision of services than to contracts solely for the sale of a business or franchise agreements restraining the franchisee from dealing with competing goods, thus making the drafting of these provisions in offshoring contracts a critical and sensitive task.

ENFORCING PROPER CHECKS AND BALANCES ON SUBCONTRACTING

Subcontracting by the Indian service provider can dramatically increase the IP risk profile. Therefore, proper checks and balances should be placed on the Indian service provider's ability to subcontract any portion of the offshored services. To the extent possible, the US customer should require that subcontractors enter into contractual commitments that are directly enforceable by the US customer. At the very least, the US customer should (i) require prior approval rights with respect to all subcontractors and retain the right to review the terms of all subcontracts, (ii) require flow down of certain mandatory provisions to safeguard the US customer's rights and interests, such as data privacy, IP ownership and assignment provisions and confidentiality obligations, (iii) perform thorough due diligence with respect to subcontractors, (iv) require the Indian service provider to be contractually responsible for subcontracted functions, and (v) insist upon contractual arrangements, to the extent practicable, that maximize the customer's chances in India of being positioned legally to enforce contractual protections regarding data privacy, confidentiality and IP ownership directly against the subcontractor.

IMPLEMENTING EFFECTIVE INFORMATION GOVERNANCE MEASURES

The US customer should perform a risk assessment prior to sending any sensitive information offshore and develop and implement effective information governance strategies and internal security measures to control the access, availability and dissemination of trade secrets and confidential information in India. Key measures include (i) requiring meaningful background checks to be performed on employees and consultants engaged by the Indian service provider and assigned to the US customer's account, (ii) permitting controlled access on a "need to know" basis, (iii) managing attrition and turnover rate of employees, (iv) briefing employees on security measures and conducting exit interviews of ex-employees to remind them of continuing confidentiality obligations, (v) performing routine audits to verify a service provider's compliance, and (vi) to the extent possible, marking hard copy documents and electronic data with "confidential" or "proprietary" legends prior to placing them in circulation. In addition, because most security breaches are generated internally by employees, the US customer should require the Indian service provider to implement personnel security through a three-pronged approach of employee screening, training, and a robust disciplinary process.

ASSESSING NEED FOR LOCAL PATENT REGISTRATIONS IN INDIA

Before embarking on an offshoring transaction involving India, a US customer should determine whether to protect its IP that might be shared or created in India through trade secrets or by obtaining a local patent in India. The fundamental questions are whether to seek local patent protection for any invention that is patentable or already patented outside India that would be made available in India or for any innovation originating in India, and whether to make any subsequent global filings for any India-originated innovation. Through a well thought out patent strategy upfront, a US customer can minimize not only infringement risk but also the risk of potential loss of any global patent rights, particularly given

the differing standards of patentability worldwide. To a large extent, the patent strategy will be driven by the nature of the offshoring project and the degree of critical IP involved. For example, in a KPO in India involving research and development of chemical entities, it may be worthwhile to obtain local patent protection for the chemical entities. Similarly, in a KPO involving the manufacture of drugs in India, the customer may wish to obtain local patent protection for the drug formulations to prevent local generic companies from copying the drug. A key benefit of patent protection is that it provides the patent owner with a bundle of strong statutory rights that may be enforced against any third party in India to stop any unauthorized use of the patented technology, irrespective of the existence of any contractual or fiduciary relationship.

Furthermore, unlike in the case of trade secrets or copyrights, independent development of a patented technology is not a defense to a claim of infringement. While not usually a significant risk, a US customer in India should generally be aware that India's patent laws do empower the government to grant a "compulsory license" to a private party or a government agency under certain circumstances. India's patent laws also provide for broad "research and experimental use" exceptions whereby a third party's experimental use of a patent, even for commercial purposes, without the patent owner's consent does not constitute infringement. Finally, a US customer must keep in mind that computer programs and business methods continue to be *per se* not patentable in India, and so must be protected as trade secrets through the contractual approaches discussed above.

OTHER IP CONSIDERATIONS

As a practical way to manage the risk to IP, the US customer should (i) perform detailed due diligence of the Indian service provider upfront to evaluate the entity's track record for protecting IP, (ii) be extremely particular about which IP must truly be offshored and avoid where possible offshoring critical technology, (iii) maintain core components of the offshored IP in the US, and (iv) require frequent disclosure of work-in-progress and periodic delivery of deliverables during the course of the project to avoid being denied access to such technology in the event of a dispute or bankruptcy. To mitigate risk, businesses may adopt a "distributed R&D model" by dividing R&D responsibility among multiple entities, and sometimes even across multiple jurisdictions, but this can be an expensive operating model as additional capital and resources would be required to manage and integrate results from the various entities.

EXPLORING MECHANISMS TO MITIGATE ENFORCEMENT RISKS IN INDIA

The enforcement of the US customer's rights and remedies is always a vital concern, and those concerns can be exacerbated when dealing with an Indian service provider, particularly one that has few or no meaningful assets in the US against which any judgment could be executed. If the Indian service provider has meaningful assets located in the US and a US plaintiff successfully obtains a judgment in a court of competent jurisdiction, the judgment can be enforced against those US assets. However, even if a dispute with an Indian service

provider is adjudicated in the US, if the Indian service provider's primary assets are located in India and not in the US, the US customer must still seek redress within the Indian legal system to obtain and enforce a judgment against the Indian service provider's India-based assets.

Jurisdiction and enforcement provisions in the operative contract should be carefully considered and crafted.

Because seeking to enforce a foreign judgment in India can be arduous, time consuming, expensive, and unpredictable, it may actually be advisable for the US customer, depending on the circumstances, to institute claims initially in India against the Indian service provider with few meaningful assets in the US rather than pursuing a US judgment and still be faced with the necessity of effectively re-litigating the dispute in seeking to enforce the US judgment in India, particularly if the US plaintiff is seeking injunctive relief and time is of the essence. Therefore, jurisdiction and enforcement provisions in the operative contract should be carefully considered and crafted so as to provide the US customer with adequate and flexible rights and remedies keeping in view the nature of the business or knowledge process and the underlying customer IP being offshored to India.

To assess its likely ability to enforce rights and remedies with respect to an Indian service provider, the US customer should perform due diligence upfront to identify the physical location of the Indian service provider's assets. This exercise should include determining the extent to which the Indian service provider has a US presence and, correspondingly, local assets which would be available for the satisfaction of judgments. Furthermore, to mitigate any enforcement risks, the US customer should explore alternative measures such as insurance, performance bonding, letters of credit or guarantees from the Indian service provider and financially responsible affiliates of the Indian service provider, and retain for itself flexible and rules-based termination rights. To best mitigate the risk of an Indian service provider seeking refuge in an Indian court and being mired in prolonged litigation and subject to unfamiliar procedures, private arbitration is the preferred means of dispute resolution in an offshore sourcing transaction involving India.

CONSIDERING ALTERNATIVE DISPUTE RESOLUTION MECHANISMS TO MAINTAIN CONFIDENTIALITY

In India, litigation concerning the breach of trade secret protection clauses can lead to the open disclosure and consequential loss of the trade secrets at issue if the legal proceedings are not closed. Therefore, among other reasons, the operative contract should require that all disputes relating to the US customer's trade secrets and confidential information be subject to confidential mediation or arbitration rather than litigation and in a non-Indian venue if possible, and that all IP and information involved in the proceeding to be treated

confidentially. The relative ease of enforcing foreign and India-based arbitral awards in India further provide compelling reasons for adopting arbitration as the formal dispute resolution mechanism in India.

DETERMINING THE APPROPRIATE OFFSHORE DELIVERY MODEL

A potential US customer may consider adopting a "captive" offshoring model (which involves offshoring through affiliated legal entities in India) when the adverse impact and cost to the business of losing control over the IP that would be transferred to, or created in, India would be significant. Not surprisingly, a high percentage of captive offshoring transactions in India are in the IP-intensive sectors such as advanced software, high-tech electronics and pharmaceuticals. While establishing a captive in India provides the US customer more control over day-to-day operations and IP, a customer must balance that benefit against the fact that captive models tend to be more expensive and a majority of the legal issues discussed above will nonetheless still exist and therefore must be carefully evaluated and addressed irrespective of the offshore delivery model elected by the customer.

Conclusion

In summary, offshoring to India can not only yield enormous cost savings and increased efficiencies but also leverage India's vast knowledge class to perform "high end" KPO services and functions. However, because of the potential risks to a customer's IP that may be transferred to or created in India, a US customer contemplating an offshoring project in India must carefully assess India's IP legal framework vis-à-vis the business or knowledge process that will be offshored and accordingly determine the necessary and available safeguards to protect its IP, including trade secrets and confidential information. These safeguards may include statutory and common law protections, but carefully crafted and robust contractual provisions combined with practical and enforceable mechanisms to minimize IP-related risk are mission critical and should be an integral component of any offshoring project in India. ◆

New Minimum Standards for IT Security in the European Union –"EuroSOX" to be Implemented

Martin Braun

Martin's work out of Frankfurt involves outsourcing and technology transactions, data privacy and IT security, open source software licensing and e-commerce issues. He serves clients in the telecommunications, biotechnology, pharma, agriculture and new media industries.

49 697 941 2101

mbraun@mayerbrown.com

Legal requirements regarding IT security have been on the agenda of companies doing business in Europe for many years. The need to give serious consideration to these security obligations is currently reaffirmed by Directive 2006/43/EC on statutory audits of annual accounts and consolidated accounts, which is commonly referred to as "EuroSOX." Each member state of the European Union ("EU") has to pass national legislation to implement its requirements by June 29, 2008.

Primarily Statutory Audit Requirements

Like the Sarbanes-Oxley Act in the US, EuroSOX aims to strengthen the transparency and accountability of existing financial control and management systems. Primarily, this directive harmonizes requirements regarding education, approval, independence and registration of persons and audit firms who are authorized to perform statutory audits. Additionally, EuroSOX aims to create a high-level harmonization of statutory audit requirements for certain types of companies across the European Union.

Direct Impact on IT Security

These statutory audit requirements have a direct impact on companies' IT systems. The directive confirms that auditors are required to assess the affected companies' systems of internal controls and confirm the existence of a functioning audit committee, as part of the general risk management strategy. With information technology being a critical component of virtually all companies, IT systems and the security of such IT systems are a vital part of all risk assessment and management. At the same time, at each individual company, internal control and risk management systems themselves rely on the applicable company's IT systems. Unlike the Sarbanes-Oxley Act in the US, EuroSOX does not contain detailed obligations — each company will have to determine which measures are required and appropriate to ensure compliance.

Which Companies are Affected by the Directive?

EuroSOX does not apply to all companies in Europe. Primarily, the directive harmonizes the framework for auditors and their qualifications. At the same time, the directive also defines certain minimum standards for statutory audits of so-called "public-interest entities." Public-interest entities are defined as:

- entities governed by the law of a member state of the EU whose transferable securities are admitted to trading on a regulated market of any member state of the EU,

- credit institutions (as further defined in Art. 1 N° 1 of Directive 2000/12/EC), and
- insurance companies (as further defined in Art. 2 Para 1 of Directive 91/674/EWG).

Individual member states of the EU are free to extend EuroSOX obligations to other companies within their jurisdiction, and they may also, within certain limits set by the directive, choose to exempt certain public-interest entities from the minimum standards.

Companies to whom the directive is not directly applicable will very likely be affected by the directive as well, because public-interest entities will very likely require their suppliers and partners to comply with EuroSOX obligations (e.g., in the context of outsourcing relationships).

Standards in Europe are Already High

EuroSOX was passed on the assumption that companies generally have effective systems of internal control and risk management. These systems exist because of the already considerable number of laws and regulations relating to internal control and/or risk management. As an example, in Germany, such laws include the Federal Data Protection Act (*Bundesdatenschutzgesetz*), the German tax code (*Abgabenordnung*), provisions regarding management liability in the event of insufficient risk management in the German Stock Corporations Act (*Aktiengesetz*), and the Basel II requirements.

In addition, documents such as the International Standards on Auditing, International Accounting Standards, International Financial Reporting Standards and related Interpretations establish general requirements for statutory audits, including as related to

EuroSOX was passed on the assumption that companies generally have effective systems of internal control and risk management.

information technology and IT security. There is a good chance that most of the EuroSOX requirements are covered by these requirements already. Similarly, companies that are already in compliance with the Sarbanes-Oxley Act in the US will very likely only have to make limited changes, as EuroSOX appears not to contain any obligations that exceed those of the Sarbanes-Oxley Act.

Sanctions

Non-compliance with EuroSOX has severe consequences: auditors may refuse to issue audit reports due to these heightened requirements, and company executives may face personal liability under national laws if the internal control systems or risk management systems are considered to be inadequate.

Suggested Steps

For the coming months, it is advisable for companies to do the following:

- Review in detail whether the Directive is applicable to your company and how your company might be affected indirectly by the Directive;
- Closely monitor implementation measures of EuroSOX requirements in the countries relevant to your business;
- Review existing documentation of IT and telecommunications systems at your company;
- Review your company's existing strategy regarding certification under IT security standards such as ISO/IEC 27001:2005;
- Review existing agreements with your company's suppliers and business partners and consider amending contract templates in order to be able to impose IT security and compliance requirements; and
- Review or audit compliance with existing IT security and data protection requirements, particularly in relation to national data protection laws.

Conclusions

EuroSOX needs to be a top priority on the agenda of CIOs and internal legal departments, particularly because of the significant sanctions faced in the event of non-compliance. At the same time, the scope of actual changes due to implementing these requirements in the individual countries is likely to be rather limited, as many companies are already subject to similar obligations. ◆

The Risks of Open Source Software in Outsourcing Transactions

Derek Schaffner

Derek focuses on software licensing transactions, Internet advertising agreements, and finance and accounting functions, among other business process functions. He represents clients in telecommunications, health care and travel, principally on IT renegotiations and post-merger consolidation of services from the Washington, DC, office.

202 263 3732

dschaffner@mayerbrown.com

Open source software (OSS) is far more prevalent in the corporate environment than commonly thought. In fact, current research indicates that open source objects presently fulfill approximately 14 percent of the requirements for custom software development[1]. The open source movement can be especially troubling for clients that have outsourced IT services, particularly those using third parties for application development and maintenance, due to the licensing terms that accompany open source software.

Overview of OSS Licensing Risks

The use of OSS in the corporate environment has grown in response to declining IT budgets while CIOs and IT managers try to balance increased IT deliverables. Integrating OSS components into proprietary software development can be necessary to meet shipment dates while still delivering quality code. In essence, OSS is a shortcut that can speed application development, whether internally developed or obtained from a service provider. In particular, service providers are motivated to use OSS as a way to meet client milestones and reduce internal costs, thus increasing the service provider's margins on the deal.

However, the injection of OSS into proprietary software code can put the entire code base at risk. Whenever any type of foreign code is introduced into a code base, there are license issues and other risks to consider; clients of outsourced IT services should never assume that all code provided by a service provider is original. Moreover, the detection of OSS in complex software development can often be difficult. For example, a prior developer who used OSS may have neglected to insert OSS notices in the proprietary source code that he wrote, thus increasing the likelihood that the OSS components could go undetected during a code review.

Open source software has licensing requirements just like traditional software. Open source software does not mean that the underlying code is free or that users have unfettered rights to do whatever they please with the code. The variations and nuances among different OSS licenses have been well-documented, but the most popular OSS licensing schemes all share some common characteristics.

All OSS licenses require "free distribution" of open source components. While open source developers may charge a fee for their open source programs, they must allow others to make unlimited copies of the open source and (re)distribute it without paying any additional licensing

fees or royalties. This concept is problematic in the outsourcing context because this free redistribution right applies even if the open source code is embedded as part of a larger proprietary program, thereby exposing the entire code base and potential trade secrets.

Additionally, all OSS licenses must allow the user to make modifications (including the creation of derivative works) of the underlying code. The user is not required to distribute any of these modifications if they are made exclusively for internal use, thus granting clients of outsourced IT services some relief from the redistribution requirement. However, if the user decides to distribute any modifications, then the user must do so under the terms of the original open source code and distribute the entire source code for modifications. This represents the greatest risk for clients who have outsourced IT services, as proprietary code could be exposed to the open source community. Note that "distribution" typically occurs when the open source code is shared with any external organization or individual.

OSS is also problematic for the client from a contractual perspective. For example, there is a greater risk of upstream IP infringement because most open source licenses (including the commonly used GNU General Public License (GPL), which governs the distribution of Linux) lack a non-infringement warranty and, consequently, fail to address the viral nature of open source code. To illustrate this point, consider a service provider's warranty that its work product does not infringe any third party intellectual property rights. While the stand-alone GPL code at issue may not infringe any third party rights, the use of open source code may trigger the free redistribution rights mentioned above and expose the entire work product.

The use of OSS in the corporate environment has grown in response to declining IT budgets while CIOs and IT managers try to balance increased IT deliverables.

Some OSS licenses, such as the GPL, also lack performance warranties, therefore offering the code "as is" with no express or implied warranties. As a result, if open source code licensed under the GPL fails or corrupts another system, the licensor has no recourse.

How to Manage OSS in Outsourcing Transactions

It is difficult to monitor and manage what you don't know you have. The management of open source software in outsourcing deals should be part of the larger enterprise-wide framework that ensures that OSS use is consistent with corporate policy. Procedures should be implemented that identify and track the use of all open source applications within the company. These procedures should require prior approval (from both a technical and legal perspective) before any open source use is commenced or any change in contemplated use is implemented, especially if the contemplated use involves sharing the code outside the organization (and thus triggering redistribution).

A sophisticated service provider might be inclined to utilize OSS for the benefits discussed above, and could subsequently disclaim any responsibility for this in the software that it produces. However, this approach would shift the risk of managing all open source issues to the client, who is often not in the best position to make such determinations. The service provider is in a better position to manage these risks, and therefore clients should seek certain provisions in their services agreements to ensure that these risks are adequately allocated between the parties.

There are several approaches that clients can take in structuring the services agreement to manage the risks associated with open source software. A client could simply require that the service provider refrain from any and all uses of open source in the services provided. The willingness of a service provider to agree to such a provision will likely be dependent upon the size of the provider as well as the margins the service provider is expecting from the deal. Another approach allows the use of OSS but requires pre-approval of the client's general counsel.

Clients cannot blindly rely on a service provider statement indicating that any software development is subject to standard open source license terms. While OSS licenses share some common traits, there are too many variations. Therefore, clients should require a review of each open source license being considered for use by invoking the same processes and controls that are used internally for other proprietary software licenses. This understanding can be memorialized in a warranty from the service provider to refrain from using OSS in work product without the client's prior review and approval. If appropriate, a client may also seek a representation and warranty that the service provider's work product does or does not contain any OSS code; such a provision would be beneficial if the outsourcing agreement includes ADM services.

There are several approaches that clients can take in structuring the services agreement to manage the risks associated with open source software.

Likewise, there are other contractual provisions that can help mitigate the OSS risk in an outsourcing relationship. Under most open source licenses, it remains possible for a service provider to modify open source code and provide the modifications to a client on an exclusive and confidential basis. Such an understanding could be memorialized in an outsourcing agreement whereby the service provider would have the ability to make such modifications while being contractually bound to not provide the modifications to a third party. Under the terms of the open source license, the service provider could not prevent the client from

redistributing the modified source code, but that would be unlikely as the client would most likely want to maintain the confidentiality of the modifications. It is worthwhile to note that some service providers might be reluctant to agree to such a provision since it limits their future ability to reuse the modified code for another client.

Clients should also consider requiring that service providers demonstrate that all IT projects meet intellectual property controls, including divulging any OSS code used as well as assurances that licensing requirements have been met.

Finally, clients should also review outsourced code for open source components. While this task is nearly impossible to do manually, automated tools exist that compare code against open source depositories and will flag positive hits. While this method will not catch every occurrence of OSS (especially if the OSS is slightly modified), it will provide further assurances that the service provider is (or is not) honoring its obligations under the services agreement.

Steps if You Have Unapproved OSS

Despite the efforts discussed above, OSS may still find its way into the client's code base. If the OSS license contains redistribution rights, then the clients may be required to either comply with the terms of the license or infringe it by continuing to use the code without complying with the license conditions. The latter approach is intriguing because open source licenses are rarely litigated. Moreover, due to the communal development nature of OSS, the question of which parties have standing to sue to enforce OSS license rights remains unclear.

Clients should also consider requiring that service providers demonstrate that all IT projects meet intellectual property controls, including divulging any OSS code used as well as assurances that licensing requirements have been met.

If unapproved OSS code is discovered, one suggested approach involves remediation of the code, if possible. To evaluate this option, a client's technical staff must ascertain if the open source code can be successfully extracted and replaced. Because many application development service agreements tie payment to certain deliverables, a provision could be inserted into the agreement that ties a deliverable milestone to OSS code remediation, thereby providing increased motivation for the service provider to deliver original code.

Service providers are usually in the best position to remediate the code. Additionally, a "clean room" strategy should be invoked whereby the rewritten components do not borrow protectable expressions from the open source pieces that are being replaced. This can

be accomplished by having a different set of programmers rewrite the functionality. The programmers involved in the original use of OSS can create the specifications for the code to be replaced by the new group of programmers. It is recommended that these specifications be shared with the client's general counsel for review. Once the remediation is complete, the code should be reviewed again, both from a technical and legal perspective.

Clients should also explore any other rights or legal remedies they may have under the services agreement.

Closing Thoughts

The risks posed by OSS in outsourced transactions can be carefully managed without stifling the development process or putting proprietary code at risk. Such risks can be managed via a multi-pronged approach that includes contractual prohibitions, payments linked to demonstrations that third-party components have been properly incorporated, code review, and remediation, if necessary. Clients should also develop and enforce OSS policies, both internally and with service providers. ◆

Endnotes

[1] *See* Jim Johnson, "Open Source with Offshoring a Compelling Cost Formula," (June 2007), available at http://www.softwaremag.com/L.cfm?Doc=1060-5/2007).

Aligning Incentives with Service Level Agreements

Brad L. Peterson

Brad represents clients in a broad range of onshore, nearshore, and offshore business process sourcing transactions out of the Chicago office. These transactions have included sourcing functions such as human resources, finance and accounting, logistics, contact centers and back-office processing.

312 701 8568

bpeterson@mayerbrown.com

Service level agreements are one of the great ideas in outsourcing. In a service level agreement (SLA), a provider agrees to achieve defined performance levels and to reduce its charges if it fails to achieve those performance levels. An effective SLA balances the unfortunate incentive for a provider, in a fixed price arrangement, to increase its profits by cutting service quality.

An effective SLA fills a vital gap in contract law for the customer in a long-term contract for critical services. Contract law provides two primary performance incentives: a right to terminate for material breach and a right to collect damages. However, these incentives both address poor performance, and customers that rely on outsourcing providers for critical services frequently need to provide an incentive for good, or even world-class, performance. An effective SLA meets that need by linking the provider's profit margin to achieving performance standards.

SLAs are also a boon to providers. They replace general performance expectations (and the resultant disputes) with well-defined performance requirements. Providers can use service levels in the sales process to show genuine commitment to performance levels, and thus to make outsourcing as or more attractive than staying with known internal service levels. SLAs also help providers to simultaneously pursue their short-term interest in this month's margin and their long-term interest in being known as a provider of world-class services.

Choosing Service Levels

Service levels can provide incentives for achieving desired quality, speed, availability, capacity, reliability, user-friendliness, timeliness, conformity, efficiency, and effectiveness. Of course, some service levels are more helpful than others. Such service levels are:

- *Controllable.* The provider must have the ability to control the outcome; otherwise, the service level doesn't provide an incentive.
- *Essential.* The best service levels go to the essence or heart of the contract. In a payroll outsourcing, timely payment of accurate wages goes to the heart of the contract, so this is where the service level incentives belong.
- *Measurable.* The parties must be able to agree on, and trust, a measurement process.

Defining the Measurement Process

In SLAs, details matter. A network server can be measured as 100 percent functional while still being completely unavailable to the end user. For example, availability will be different when measured using software continuously running within that server, periodic polling by another server, user complaints about downtime, or a monthly user satisfaction survey asking about perceptions of downtime.

The measurement process must align with the intended incentive. Measuring call answer times by the percentage of calls answered within 30 seconds creates an adverse incentive to give priority to calls that have held for less than 30 seconds (ignoring those that have been on hold for longer). The provider might ignore this adverse incentive despite its own economic interests and the unmistakable signal sent by the service level, but it's a mistake to create the adverse incentive.

In SLAs, details matter. A network server can be measured as 100 percent functional while still being completely unavailable to the end user.

A strong service level measurement process is critical to success. If the measurement process is not well-defined, the provider can report better results by gaming the system well instead of performing well. The problem is even worse if the customer lacks visibility into the provider's actual measurement systems, allowing the provider to hide problems instead of fixing them. Thus, the customer's team must include people with a solid technical and operational understanding of how the performance will be measured and the contact must include well-defined measurement obligations and strong audit and access rights.

Setting Required Performance Levels

The SLA must clearly define the performance levels that the provider is required to meet in order to achieve the customer's established service levels. These performance levels should be established during the period where the provider is bidding on the work and before the price has been set. At that point, the provider has an incentive to work with the customer to identify a value-maximizing price to committed performance level.

Providers often propose that the service levels be set after signing. There are two approaches for doing so, each of which creates poor incentives:

- *Use data from the provider's initial performance.* This approach is problematic, however, because, for example, the customer might set the minimum service level in line with what was the provider's worst performance during its first six months, thus inadvertently creating an incentive for the provider to have at least one terribly bad month in the first six months.

- *Agree to agree on service levels after a "burn-in" period.* The problem here is not a poor incentive but the lack of any incentive for the provider to arrive at an agreement. The incentive created is to make the topic of service levels sufficiently painful that the negotiation does not happen.

Using Service Level Credits

A service level credit is a reduction in the provider's compensation that occurs upon a specified level of service level failure. Because the credits reduce the provider's profit margin, a large enough credit can provide a powerful incentive to meet service levels.

A well-crafted SLA can create incentives that target particular types of performance. For example, the SLA can:

- Define a minimum service level, with a credit payable upon each failure, to create an incentive to never miss that level of performance.
- Define a target service level, with a credit payable upon a series of failures, to create an incentive to keep generally good performance.
- Have credits increase for successive breaches to create an additional incentive to fix problems quickly.
- Have credits increase for larger breaches to create an incentive to minimize the scale of a service level failure.
- Give the customer the right to reallocate service credit exposure over the service levels to allow the customer to realign incentives as its business needs change.
- Have a failure to report actual service level performance be deemed a service level failure to create an incentive for prompt reporting.
- Create the opportunity to earn back service level credits based on annual performance to give an incentive both for monthly performance and annual overall performance.
- Create an opportunity for service level bonuses to create an incentive to meet service level objectives that would be unreasonable as contractual commitments.

If the SLA includes an incentive to exceed service level requirements, consider locking in the improvement by automatically resetting the performance requirement based on the provider's performance. For example, for each year, the target performance could increase to the midpoint between the prior year's actual performance and the prior year's required performance. Note, though, that this dampens somewhat the provider's incentive to exceed the required performance level.

Credits are Not Liquidated Damages

Some providers argue that service level credits should be treated as liquidated damages. However, if service levels are used as described in this article, they should *not* be considered liquidated damages because, while they provide an incentive for good or excellent performance, they are not as effective as typical contract damages at preventing bad performance. Said another way, having credits for a breach of a 99 percent service level be liquidated damages would provide the same incentive to avoid 0 percent performance that it provides to avoid 98 percent performance. Also, if service level credits were to be liquidated damages, the customer would need to make them larger because they would need to reflect the potential harm to the customer instead of an adequate incentive to the provider.

Deemed Material Breach

Service levels help to define the term "material breach." Unfortunately, although material breach is commonly used as a threshold for termination of outsourcing contracts, it is not clearly defined by the law. For example, 23 *Williston on Contracts* § 63:3 (4th ed.) explains that a material breach is a breach that "is so fundamental to a contract that the failure to perform . . . defeats the essential purpose of the contract,"; "go[es] to the 'root' or 'essence' of the agreement," or "touches the fundamental purpose of the contract and defeats the object of the parties in entering into the contract." This allows a provider to argue that any service level breach, particularly in only one of many service levels, would not be a material breach.

The SLA can provide increased certainty by defining particular events that, without argument, allow the customer to terminate the contract for cause. For example, an SLA can set a "termination service level" that, when reached, allows the customer to terminate for cause. Additionally, the SLA could establish a defined amount of accumulated service level failures sufficient to permit the customer to terminate for cause, such as where the provider breaches a single, critical service level three times in succession, or the provider breaches enough service levels that the service level credits reach a percentage of the amount at risk over a period. The effect is to give the provider a powerful incentive to achieve service levels to avoid the risk of a termination for cause.

Conclusion

Service level agreements, if used skillfully, can align the provider's incentives with the customer's business imperatives. They also benefit the provider, allowing it to maximize its short-term profits in ways that support its long-term interest in satisfying its customers. As a result, we expect that they will continue to be a critical component of successful outsourcing transactions. ◆

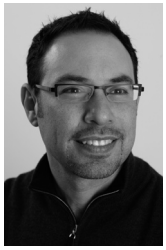
Pricing and Risk Allocation for Mission-Critical Transactions

Rakesh Kishan, President, and Jay Schwartz, Managing Director, UMS Advisory, Inc.

Rakesh Kishan is President of UMS Advisory, Inc., a boutique consulting firm that specializes in outsourcing and operational improvement. He focuses on integrated facilities management contracts, having pioneered methods for developing incentive based contracts.

973 420 7253

rkishan@umscg.com



Jay Schwartz is a Managing Director at UMS Advisory, Inc., and provides strategic direction and client management in the delivery of outsourcing and sourcing initiatives.

206 370 9500

jschwartz@umscg.com

When selecting third parties to perform business-critical services, a number of pricing and risk allocation issues are frequently encountered. In handling these, well-crafted contracts provide an indispensable road map for service providers and customers to follow throughout their relationship. As such, when each party clearly understands its rights and obligations under an agreement, the potential for a misunderstanding to arise is significantly reduced. Some of the common pricing issues frequently encountered include:

- *Price transparency* – the extent to which supplier has an obligation to provide visibility into margin and cost
- *Price certainty* – the extent to which cost is capped and how much financial risk is allocated to the supplier
- *Baseline* – the basis for determining financial impact
- *Performance-based reward mechanisms* – triggering payment on value received

The following business scenario illustrates these key issues and demonstrates where the relationship between risk allocation and pricing is most apparent.

The Scenario

A worldwide athletic footwear and apparel manufacturer, "Victory," is seeking to switch outsourcing providers, from the incumbent to an alternative, for its inventory control and product distribution throughout Japan.

First, we need to construct a basic contracting continuum containing the risk allocation and pricing areas that we want to address. These areas should all be negotiated in a competitive environment to the extent practicable, keeping in mind that there are also significant legal areas of risk that are not addressed here, including limitation of liability and indemnity. The items in Figure 1 on page 30 are typical of those found in the schedules or exhibits of an agreement.

Figure 1 *Basic Contracting Continuum*

Transition

Because Victory is terminating its relationship with an incumbent model and beginning with an alternative supplier, there will be a transition. Therefore, the agreement with the alternative supplier must contain, at a minimum, transition deliverables consisting of conversion testing and implementation. These deliverables carry significant "credits" in the event agreed upon dates and deliverable accomplishments — including sub-contracts transfer, data transfer or headcount transfer — are not met.

Scope

Scope is most easily digested when broken down into broad or operational areas, then specific or core areas. For example, Victory requires warehouse services (operational), which include order selection and packing (core). It is important to understand, and not underestimate, the scope of any deal at the smallest unit level while representing it in an "outcome" and measurable fashion.

Excessive prescriptive detail will stifle innovation and will deliver a process no better than the incumbent model. At the same time, unclear scope could promote a "risk factor" premium in pricing where the supplier increases charges or, alternatively, under-prices and creates sub-acceptable performance liability. Because scope is often distributed across several internal departments, only when a unit level of scope has been defined is a customer in a position to effectively negotiate more elegant types of pricing structures in a transparent environment. Service providers will typically attempt to charge additional fees for all services falling outside of the scope – underscoring the importance of scope.

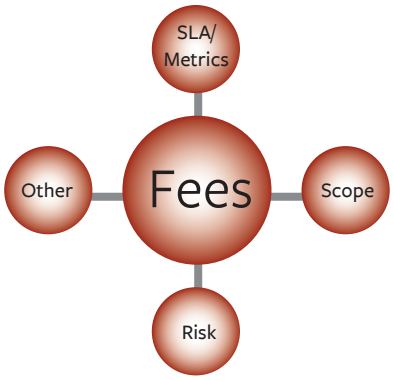
The financial baseline establishes the funding level to produce and deliver the statement of work at an expected level of performance. Issues that complicate scope and baseline are legacy liabilities related to inadequate capital investments or significant changes in scope from the incumbent model.

Fees

There is a deep relationship between fees and the other areas within the contracting continuum, as shown in Figure 2 on page 31. Fees are also impacted by what is left out of the scope. These are the reasons that the fees must accurately reflect Victory's current and potential business requirements. Victory must negotiate pricing with the alternative supplier for

anticipatory services today. For example, currently, 10 truckloads of footwear per day are shipped from the warehouse requiring two-day delivery. However, in year two, Victory anticipates 15 truckloads of footwear and five truckloads of apparel to be shipped from the warehouse requiring one-day delivery. Both the growth in business and the increase in service level must be accounted for in the fee structure or Victory may pay a premium for the out-of-scope services. There are also a variety of efficiency escalators and price deflators that could be negotiated into the fee structure. These provisions are quite specific and should be tied to reductions in an individual service provider's average variable cost.

Figure 2 *Fees Structure*



Setting the fee structure of suppliers can be quite complex and segmented. Types of price structures include:

- *pass-through pricing* – highly transparent, where a significant portion of cost is pass-through and fees are stratified
- *fixed cost pricing* – fixed payments with limited transparency but significant certainty
- *unit cost pricing* – when demand is uncertain

Common issues include:

- carve-outs for critical areas
- creating incentives for performance – reducing, or in rare circumstances, enhancing payments as determined by SLA triggers
- building in scalar or experience curve efficiencies based on the number of units delivered based on productivity curve within the industry

Service Level Agreement (SLA) and Performance Credits

The keys to presenting a service provider with the incentive to maintain an acceptable level of service are SLAs and performance credits. It is impossible to negotiate the fee structure

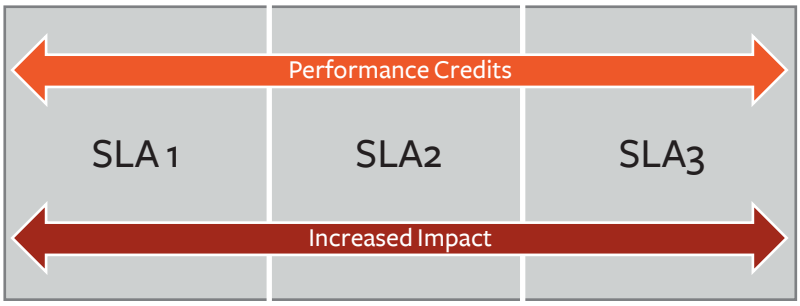
in the absence of a well-defined SLA. There are two key rules to follow when building SLAs: consider using an increased impact structure (Figure 3), and ensure the SLAs surround the most critical functions. Clients should find it useful to reference the core (specific) areas of the scope when constructing SLAs.

A typically complex transaction should have no more than a dozen SLAs. Otherwise, the service levels may prove difficult to manage, may require a more elaborate governance process, and will dilute the performance credit pool. The SLA structure directly impacts the monthly fees paid to the service provider, which could represent significant risk to the service provider's profitability. As a result, there is usually a cap on the percentage of fees at risk each month. However, if too many of the SLAs are triggered, the client may have a termination right. For example, Victory's SLA for on-time footwear and apparel delivery is 99 percent, with an increased impact SLA of 98 percent and a right of termination for Victory below 97 percent. Last month, the alternative supplier had on-time delivery of 96 percent. Even though Victory can reduce its monthly fees by the stated SLA amount, the company also has the right to terminate the relationship. Although this is not likely, the situation provides both parties urgent motivation to work together to fix the problems.

SLAs largely center on payment withholding, but suppliers will frequently argue for enhanced payments if SLAs are exceeded. Here, judgment has to be exercised by considering a few key factors:

- The competitive advantage created by the business critical category (e.g., revenues, market-share and COGS)
- The level of IP deployed by the supplier
- The level of proprietary skills provided
- The capital deployed by the supplier
- The risk assumed by the supplier

Figure 3 *Increased Impact Structure*

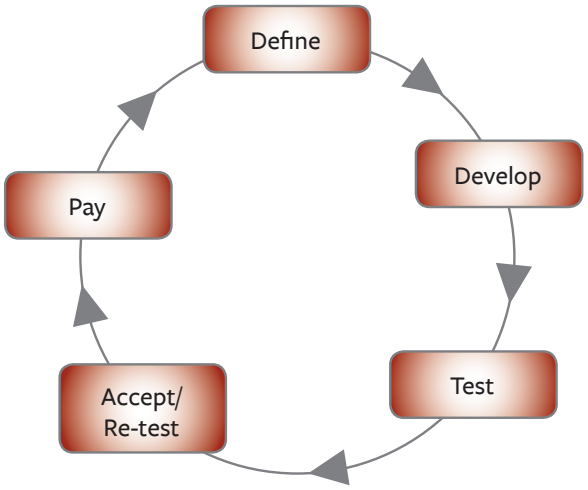


For example, with a low-capital intensive industry such as janitorial services, which delivers semi-skilled labor and does not drive market success, incentive should probably be centered around meeting, not exceeding, SLAs.

Acceptance

Generally, acceptance covers the development of certain technology deliverables and gives clients the right to test the deliverables prior to triggering an obligation to pay the service provider. Most service providers would rather the terms state that the client's obligation to pay vests upon delivery. However, how would a client know whether the deliverable operates as desired? This issue can by avoided be applying the process illustrated in Figure 4. For example, Victory contracts with the alternative supplier to develop a new interface into Victory's SAP order management system. The cost for the work is quoted at $10M. The development work is considered a "one-off" and out of scope. Two months later the alternative supplier shows up with a black box and asks for $10M upon delivery. Victory pays and the interface does not work. The alternative supplier says it works according to the specifications they were given and refuses to re-test without further payment. By negotiating the development and acceptance terms upfront, Victory could have avoided this costly situation.

Figure 4 *Deliverable Process*



Step-in Rights

One of the most powerful tools a client may have with a mission-critical service provider is the right to step-in to the service provider's business in the event the service provider either severely fails in its performance obligations, becomes insolvent, or is acquired by a competing company. These rights will not be given lightly and the service provider will certainly price

for this sort of risk. It is nearly impossible to negotiate these rights in a non-competitive environment, unless the client has an equity position or represents such a significant part of the service provider's business that if the client were to go elsewhere, the service provider would fail.

One can achieve much of the protection sought under inclusion of step-in rights with frequently tested in-house source code escrow, coupled with triggers dissolving non-solicitation provisions. Step-in rights could include a performance requirement to transfer work to a different supplier over the course of a transition period or to transfer it back to an internal organization. The contract should provide adequate protection through appropriate provisions so there is no pressure to concede or retain a supplier under a performance failure scenario.

Benchmarking

No matter how carefully the terms of the contract are negotiated, businesses and industries change in ways that could not have been anticipated by the client. So, forward-thinking companies are sure to negotiate benchmarking provisions into their agreements. Benchmarking allows the client to select an independent third party to periodically evaluate the provision of like services and prepare reports. These reports can be shared with the service provider and if there is a discrepancy, the service provider is required to respond. The written response can be either disagreement or acceptance of the proposed change, which may be as simple as a change in price, a service-level adjustment or the implementation of new technology. Benchmarking is challenging, however, as sources of good information can be difficult to find. However, solutions can be created through industry and supplier account networks and peer groups.

Conclusion

In order to adequately assess the risk and negotiate the optimal price structure for business critical services, one has to consider how the above elements work together. Because most negotiations are affected by this asymmetric information, it is crucial for clients to understand the supplier market maturity, category (supply and demand conditions), pricing structures and mechanisms for risk and reward. All of these elements need to be tied into the overarching framework provided by a well-crafted contract. ◆

About Our Practice

The Business & Technology Sourcing practice at Mayer Brown can take you through your sourcing transactions from concept to contract. With more than 50 lawyers in eight offices around the world, we have handled more than 250 outsourcing and information technology transactions with an aggregate deal value of over $85 billion. We have worked in virtually every country and across the spectrum of industries. We understand the market and have worked with all of the major suppliers. We offer our clients realistic approaches, market-tested views and proven methodologies.

What sets us apart is our breadth of knowledge and proven results. Our practice has been ranked by Chambers in its top tier of recommended ITO and BPO law firms for five successive years. Our lawyers possess the "crucial combination of technical knowledge and the commercial ability and know-how to apply it." *Chambers Global 2008*

For more information about our practice, please visit our website: www.mayerbrown.com/businesstechnologysourcing.

About Mayer Brown

Mayer Brown is a leading global law firm with offices in key business centers across the Americas, Asia and Europe. We have approximately 1,000 lawyers in the Americas, 300 in Asia and 500 in Europe. The firm's Asia presence was enhanced by its 2008 combination with JSM (formerly Johnson Stokes & Master), the largest and oldest Asia law firm. (In Asia, the firm is known as Mayer Brown JSM.) This unequalled on-the-ground presence in the world's leading markets for legal services enables Mayer Brown to offer clients access to local market knowledge on a global basis.

Mayer Brown is noted for its commitment to client service and its ability to assist clients with their most complex and demanding legal and business challenges worldwide. The firm serves many of the world's largest companies, including a significant proportion of the Fortune 100, FTSE 100 and DAX companies and more than half of the world's largest investment banks. Mayer Brown is particularly renowned for its Supreme Court and appellate, litigation, corporate and securities, finance, real estate and tax practices.

OFFICE LOCATIONS

AMERICAS
- Charlotte
- Chicago
- Houston
- Los Angeles
- New York
- Palo Alto
- São Paulo
- Washington

ASIA
- Bangkok
- Beijing
- Guangzhou
- Hanoi
- Ho Chi Minh City
- Hong Kong
- Shanghai

EUROPE
- Berlin
- Brussels
- Cologne
- Frankfurt
- London
- Paris

ALLIANCE LAW FIRMS
- Mexico City, Jáuregui, Navarrete y Nader
- Madrid, Ramón & Cajal
- Italy and Eastern Europe, Tonucci & Partners

Please visit www.mayerbrown.com for comprehensive contact information for all Mayer Brown offices.

www.mayerbrown.com