From Stolen Secrets to Safeguarded Source Code:

The Importance of Trust in International Outsourcing Ventures

by Kiran Ghia

I. Introduction: Trust

Hanging high above the workstations of software developers at Bleum Inc.'s headquarters in Shanghai is a blue and black lettered-sign that reads "Protect Our Customer."[1] This slogan serves to remind Bleum's foreign-based team of software engineers of the urgent need to protect the customer's software code. Along with other preventative measures such as an access-controlled workroom, this wall-hanging takes aim at a growing concern over the lack of intellectual property protection in place by outsourcing service providers in countries such as China, India and Eastern Europe.

For all the benefits derived from international outsourcing, it carries with it several potentially disastrous liabilities. While the sharing and widespread dissemination of intellectual property, whether in the form of source code, trade secrets or other confidential information, is a commonplace and necessary occurrence in the outsourcing industry, theft and misuse of customers' intellectual property by outsourcing vendors have become major security risk-factors for customers seeking to outsource offshore. In fact, the latest CSI-FBI Computer Crime and Security Survey, which surveyed several hundred large US companies, reported losses totaling over $11 million for the theft of proprietary information in the previous year alone.[2]

While many analysts have examined the common concerns and issues that arise in intellectual property protection (IPP) with outsourcing vendors, none have thoroughly addressed the issue of trust—an issue that is perhaps best described as both an underlying cause of intellectual property (IP) security breaches as well as a solution to the problem itself. Trust, in fact, is at the heart of the debate regarding 'alternative workplace' environments and 'virtual organizations.' It seems only natural then, that the issue of trust should be a focal point in the outsourcing debate with respect to IPP. Exploring the nature of trust and how it can be developed with an international outsourcing vendor, as well as exploring the dimensions of the intellectual property concerns themselves from an international perspective, may help to provide businesses and legal counsel with a better framework for understanding how to address these issues.

A culture of mistrust within an organization may be responsible for the lack of loyalty by any given employee. If, for example, employees' behavior is largely shaped by the overarching managerial attitude and corporate culture, the recent trend towards "audit mania" (described as the "urge to have some independent inspection") sends a message to employees that they are not trusted.[3] Charles Handy states that this attitude "becomes a self-fulfilling prophecy. 'If they don't trust me,' employees say to themselves, 'Why should I bother to put their needs before mine?'" If it is at all true that a "lack of trust makes employees untrustworthy," Handy notes that this "does not bode well for the future of virtuality in organizations."[4]

Without nurturing a trust-based mentality, outsourcing vendors, like employees in a virtual organization, have little incentive to remain loyal to their customers, and the security of IP assets becomes a serious concern. Where offshore vendors have minimal contact, if any, with their customers, where they have only known their customers for a short period of time, and where they often have cultural barriers to communicating with their customers, clear structural obstacles exist to developing loyalty and trust. Customers often remain suspicious of vendors they contract with and have a myriad of security measures in place to protect themselves. In turn, employees of outsourcing vendors may feel undervalued and begin to lose faith in the organization. This mentality, combined with different cultural attitudes toward intellectual property rights, can make for a potential IP security breakdown.

How to develop and maintain trust with the offshore vendor

While technology has given us the actual capacity to run organizations with offshore outsourcing vendors, technology is simply not enough. Handy would urge that companies utilizing international outsourcing service providers must learn to run their systems based more on trust rather than on control.[5]

But how does an organization learn to build trust in an ever-expanding corporate environment where managers may not even know their employees, or even worse, where managers may be suspicious of their own employees?

Sociologist Robert Putnam, who has written about the decline of social cohesion and trust in civic society, has used the phrase "coordination and cooperation for mutual benefit" to describe certain features of 'social capital.'[6] In the business context, this phrase provides a key to understanding the building blocks of a trusting organization.[7] Employees must be able to work in an organization that emphasizes *reciprocal* benefits and the *common* good—in other words, they must feel fulfilled and valued by the company. Nurturing trust at the individual vendor employee level will help to create a loyal employee base, which will ultimately result in the protection of the customer's IP. There are several common sense principles that customers can utilize from the outset of their relationship with an outsourcing vendor.[8]

The first principle that can help to foster a trusting environment with an international outsourcing service provider is that a customer must know the vendor it is contracting with. It is simply not sensible business practice to trust employees or companies that you do not know well, or that you have not witnessed in action, or who may not be dedicated to the same goals.[9] For customers, this means getting to know an outsourcing vendor before committing to a contract by visiting its facilities, meeting with managers and employees of the vendor company, and ensuring that both companies are dedicated to the same end-goals. This principle goes hand-in-hand with another core principle of trust: that trust requires contact and touch. No matter how much a vendor might share a customer's commitment, this "commitment still requires personal contact to make it real."[10] More importantly, according to John Naisbitt, the accelerating pace of "high tech" society must be balanced by "high touch" or human contact, in order to foster healthy and trusting businesses.[11]

As a starting point, both customers and outsourcing vendors, as individual companies, should assess whether they already have trusting relationships with their employees, clients, and other business affiliates. Outsourcing vendors should provide this internal information (through surveys, evaluations, etc.) to customers as a prerequisite to engaging in a business relationship. With this information, a customer may be better prepared to approach and get to know the particular vendor. This 'getting-to-know you' process entails meeting with international outsourcing vendors on a regular basis, and not just through videoconferencing or telephone calls, but through live, face-to-face meetings. Further, vendor employees should be given ample opportunity to get to know both the customer's managers and employees. For example, if the costs are not prohibitive, an exchange program in which vendor employees travel to the customer's place of business might be an important way for the customer to initiate a dialogue and a relationship with the vendor. On the other hand, frequent videoconferencing may be a more cost-sensitive means to achieve this same goal. In addition, customers could sponsor promotional events or giveaways, in which vendors get to sample the customers' products, as yet another way to develop a close, trust-based relationship.

Perhaps the key principle in building a trusting relationship with an international outsourcing service provider is making a long-term commitment to cultural awareness and sensitivity. Analysts, however, have typically applied the cultural awareness argument to a discussion of the initiation of an outsourcing relationship and corporate compatibility. Specifically, analysts seem to operate under the assumption that there is a perfect vendor match for every customer in terms of cultural beliefs and values. Not only is this assumption somewhat parochial, but it is also limited in scope. Cultural awareness should signify more to a customer than simply determining initial compatibility—it should be a continuing means of learning about a vendor's corporate culture as well as the offshore country's own nuanced social culture and regional differences. If developing trust comes down to the individual level and valuing the individual vendor employee, learning basic cultural norms and cues, sometimes even something as simple as a respectful bow or a 'Namaste,' can go a long way toward building a trusting and loyal relationship.

It would be naïve to assume that any given international vendor's culture will align perfectly with the customer's, so learning to work with and

around these varying cultural attitudes and values is the best way to build and maintain a trusting relationship with the offshore vendor. Customers can implement cross-cultural awareness training (teaching country-specific cultural norms as well as country-specific IP laws), workshops, partnerships, and exchange programs to give employees and management the opportunity to interact with each other, which, in turn, may foster an environment of trust. Moreover, cultural awareness plays a decisive role in the protection of intellectual property rights in terms of attitudes toward IPP. Establishing an open line of cultural communication can help to build a community of trust and to maintain loyalty to the customer among offshore vendor employees.

Finally, another key principle in building a trusting organization is the idea of membership.[12] Offshore vendor employees must have a sense of belonging to a community even if that community is scattered halfway across the world. This feeling of belonging can help to commit vendor employees to a higher purpose beyond selfishness, and can encourage them to see themselves "as integral to the organization's success."[13] By giving offshore vendor employees a stake in the organization, whether through benefits, incentives, or by an open-book management technique in which customers keep all vendor employees informed about the company's performance and the vendor employees' role in it, customers can cultivate a cooperative environment in which vendor employees are truly working toward the "mutual benefit" of the organization by protecting the customer's IP rights.[14]

II. A Global Legal Perspective: India

Developing and maintaining trust with an international outsourcing vendor is one of the most basic elements of international outsourcing and IPP, but it is certainly not the only part of the puzzle. Understanding the legal framework of the vendor country in terms of IP rights is also a critical element in constructing a practical toolkit for an international outsourcing venture. While international outsourcing requires the sharing of virtually every type of IP asset, including copyrights, trade secrets, trademarks, and patents, each proprietary asset is governed by its own unique set of laws which vary from country to country. And, even in countries that formally recognize strong IP rights, they may lack the means to enforce these rights or may have a general cultural attitude that does not afford the same respect to IP rights as the customer's home country.

India, for example, has emerged as a global player in the offshore outsourcing industry. The latest figures show that Indian software and services exports jumped to $12.5 billion in 2003-2004, up from nearly $10 billion in the previous fiscal year.[15] Studies also show that offshoring is creating wealth for the United States, one of India's largest customers; in fact, "for every dollar of corporate spending outsourced to India, the US economy captures more than three-quarters of the benefit and gains as much as $1.14 in return."[16]

However, the risks and actual losses to customers seeking to outsource in India continue to be ever-present. Just last year, the arrest of a former employee of an Indian outsourcing company, Geometric Software Solutions Ltd., who allegedly stole the source code for a computer-aided design package of a customer and offered to sell it to a competitor, led to the first prosecutorial filing for outsourcing-related IP theft in India.[17] And while outsourcing-related intellectual property theft has arisen largely in the form of stolen source code, the higher-end business process outsourcing market continues to expand through the use of call centers and other claims processing providers, making customer-specific, personal data increasingly vulnerable to theft. India will therefore have to make greater efforts to strengthen its IPP regime by way of data protections laws and trade secret theft laws if its wants to retain its edge in the industry.

Moreover, India's path toward an effective IPP regime has been rather inconsistent. Even after the passage of major legislation initiatives in 1999 regarding IPP, including the Patents (Amendment) Act, the Trade Marks bill, and the Copyright (Amendment) Act, and the efforts made to implement the World Intellectual Property Organization Internet treaties, India has continued to struggle with enforcement of IP rights. In fact, the Office of the United States Trade Representative (USTR) recently placed India on its "Priority Watch List," citing concerns over India's Copyright Act and its three broad exceptions, which weaken the protec-

tion of software, as well as concerns over the protection of foreign trademarks.[18]

In spite of these efforts, concerns over IPP in international outsourcing often boil down to a lack of enforcement. While many countries, including India and China, are members of the World Trade Organization and adhere to the Trade-Related Aspects of Intellectual Property Rights (TRIPS), TRIPS protection must still be enforced locally—in other words, individual countries must enact local laws to protect IP even as signatories to TRIPS. However, many countries have not yet enacted such laws, rendering TRIPS protection somewhat meaningless. India was, until very recently, one such country. But, under extreme pressure from the USTR, and much to the chagrin of many Indian drug companies, the Indian government on December 26, 2004, enacted the Patents (Amendment) Ordinance, under which the government provides patent protection for certain products including pharmaceuticals and agricultural chemicals, among other things, in order to fulfill its promise of becoming TRIPS-compliant.[19] However, unless the new Ordinance obtains approval by the Indian Parliament, it will lapse, thus further dragging out the process towards creating a comprehensive IP regime.[20] In addition, access to the court systems in many of these countries is limited and / or cumbersome, making compliance and remediation an unlikely possibility. Cultural attitudes are also a barrier to the enforcement of IPP. China, for example, has been criticized for a cultural attitude that seems to disrespect intellectual property, treating it somewhat like communal property.

Nonetheless, India continues to push towards better protection for IP rights in order to maintain its edge in the international outsourcing industry. To further this effort, India's National Association of Software and Service Companies (NASSCOM) recently launched an initiative to evaluate India's information security system called "Trusted Sourcing," as well as a partnership to prevent cyber crime and related issues with local enforcement authorities, called the Mumbai Cyber Lab.[21]

Overall, as India and other major offshore players continue to create new IP laws and tighten up their existing laws, customers will increasingly become more comfortable placing their valuable proprietary information in vendors' hands. However, laws or no laws, enforcement will remain a serious concern. One possible alternative to enforcement of IP rights in actual courts is to pursue arbitration or mediation. To this end, it is critical that a customer creates, from the outset, a team of local and regional attorneys who are knowledgeable in the IP laws of the particular vendor's country as well as familiar with the general cultural and legal environment of that country. The lawyer can help the customer to draft an arbitration clause into the original offshoring contract, mandating, for example, that all disputes arising out of the contract are to be settled by arbitration according to the International Chamber of Commerce, which provides international dispute resolution services.[22] However, it is vital that companies and especially legal counsel pay close attention to the site of the arbitration itself, as this can often bear heavily on the outcome of the proceeding.

III. Risk Management: "Trust Plus"

Building trust between a customer and an outsourcing vendor also requires detailed knowledge of the intellectual property rights involved in the business relationship. There are two main concerns associated with international outsourcing and intellectual property rights, the first of which is the ownership of IP. Many companies often overlook this vital part of a comprehensive IP protection program, and thus fail to identify, account for, and specify ownership rights of IP assets improved upon or created during the offshoring relationship.[23] These issues should be discussed and settled from the outset of the venture, and can be resolved through the use of licensing agreements and other similar instruments. The second major concern in regards to international outsourcing and IP rights is the misappropriation or theft of confidential information, trade secrets, and other proprietary information. As illustrated by the stories of Geometric Software Solutions and others, such as Jolly Technologies—where it was reported that one of the employees at Jolly's Indian research and development center had misappropriated valuable trade secrets in the form of source code and other confidential documents—customers' fears are indeed legitimate. However, there are a number of preventative steps that customers and vendors can take together to help minimize, and hopefully, eliminate these concerns.

Due diligence is certainly an important initial step in building a strong IPP program. If, after conducting background checks on employees, looking at the company's history, financial stability, retention rates for employees, and whether or not the company does

business with a chief competitor, a customer determines that the vendor is simply unfit or untrustworthy to do business with, the relationship should not be pursued. However, if a customer finds that the vendor is sound, there are a variety of controls that can be put in place to help protect the customer's IP rights. Non-disclosure agreements and confidentiality agreements, for example, are effective legal tools that can be used to prevent against the accidental or willful loss or disclosure of confidential information. Individual employees of both the customer and the vendor should be required to read and sign such agreements before engaging in any outsourcing venture. Trade secret indemnification agreements with the vendor may also be used to protect valuable proprietary information. As a last resort, customers may think about getting insurance for their source code. In addition, various security measures such as using electronic tags to mark digital property, using internet access controls, segregating the manufacturing process into separate components and outsourcing to multiple vendors, and internal auditing, may help to mitigate the risk of loss.

While it is important for customers to plan ahead, in considering whether to implement these preventative strategies, customers should also think about adding an element of trust into their otherwise standardized "Due Diligence" checklists. Customers must begin to incorporate trust into their outsourcing ventures to ensure that they are working towards a healthy, trusting business relationship with the vendor, rather than simply creating a lockdown environment of controls and access-card entry, which may only breed mistrust and disloyalty. Therefore, it is critical for customers to create a "trust plus" security environment with their vendor, working primarily to build a relationship of trust with the vendor, balanced with only the necessary and appropriate means of IP security measures for that particular vendor, or for that matter, for the individual employees of the vendor. In practice, for example, this would entail the customer getting to know the vendor and its employees, visiting the facilities, conducting exchange programs and cultural awareness trainings, as well as restricting access to certain workrooms, if this was found to be an appropriate control device for the specific vendor employees. Rather than subjecting a given vendor to an entire battery of security measures, the customer should choose appropriate controls tailored to the individual vendor's situation. Starting the outsourcing relationship on a foundation of trust will foster a kind of loyalty that restrictions and surveillance cannot guarantee on their own, and can thus serve as a critical means of protecting valuable IP rights in the international outsourcing industry.

[1] Sumner Lemon, *Overcoming the Piracy Stigma in China: Providers 'overcompensate' for the risk* (Aug. 30, 2004), *available at* http://www.computerworld.com/managementtopics/outsourcing/story/0,10801,95536,00.html.
[2] Computer Security Institute (CSI), CSI / FBI Computer Crime and Security Survey 2004, *available at* http://www.usdoj.gov/criminal/cybercrime/CSI_FBI.htm.
[3] Charles Handy, *Trust and the Virtual Organization*, Harvard Business Review 40, 44 (May-June 1995).
[4] Handy at 44.
[5] *Id.*
[6] Robert Putnam, *Bowling Alone: America's Declining Social Capital*, Journal of Democracy 6:1, 65-78 (Jan. 1995) (discussing the concept of 'civic disengagement' for which Putnam uses the metaphor of bowling: from 1980 to 1993, the number of individual bowlers rose by 10% while league membership decreased by 40%).
[7] Douglas Smith, *Are Your Employees Bowling Alone? How to Build a Trusting Organization*, Harvard Management Update 3 (Sept. 1998).
[8] *Id.* at 3.
[9] Handy at 44.
[10] *Id.* at 46.
[11] *Id.*
[12] *Id.* at 48.
[13] Smith at 3.
[14] Customers should proceed with caution, however, in extending such benefits to offshore employees, and should be aware of the pitfalls of triggering "joint employer" status over offshore employees.
[15] *See* http://www.nasscom.org.
[16] *Offshoring: Is it a Win-Win Game?* McKinsey Global Institute (Aug. 2003); *see also* Martin N. Baily and Dana Farrell, *Exploding the Myths of Offshoring*, The McKinsey Quarterly (Dec. 2004).
[17] Michael Fitzgerald, *Big Savings, Big Risk: Offshore Software Development puts Intellectual Property at Risk* (Nov. 2003), *available at* http://www.csoonline.com/read/110103/outsourcing.html.
[18] *See* http://www.ustr.gov.
[19] *See* Patents (Amendment) Ordinance, 2004 *available at* http://lawmin.nic.in/Patents%20Amendment%20Ordinance%202004.pdf.
[20] P.T. Jyothi Datta, *Date Kept, Now for the Devil in the Detail*, The Hindu Businessline (Dec. 27, 2004)
[21] *See* http://www.nasscom.org.
[22] Dana H. Shultz, *What Every Business Lawyer Needs to Know about Outsourcing*, California Bar Journal, Nov. 2004, at 1, 4.
[23] Donna Ghelfi, *The 'Outsourcing Offshore' Conundrum: An Intellectual Property Perspective*, available at http://www.wipo.int/sme/en/documents/outsourcing.htm.

Kiran Ghia is an associate at Wiggin and Dana. *She would like to thank her colleagues, especially William Simons, for his terrific ideas and guidance, as well as Dale Carlson, Stephen Harris, Elizabeth Galletta, Katarzyna Przychodzen, and Ana Oman for all of their efforts.*