

Offshore Outsourcing and Intellectual Property Protection

By John C. Checco, CISSP

Entering into the world of IT some decades ago, the typical employment process consisted of a written comprehension exam, two days of interviews, drug screening and even fingerprint registration with local authorities. My most bizarre experience included a multi-task evaluation, where the candidate was enclosed in a small room with a written exam while new-age music was piped through room speakers at extraordinary levels, broken intermittently by verbal instructions to do some really odd tasks (i.e. "...put six pencils and two pens in the coffee mug labeled 'Bob' and place it in the bottom left-hand drawer, but only if you answered 'yes' to question 35..."). All this effort to ensure that as an employee, a candidate was proficient for the needs at hand as well as loyal to the employer; how times have changed!

"Offshore business process outsourcing (BPO) is expected to reach \$3 billion in 2004, a 65 percent increase from the 2003 total of \$1.3 billion. In 2004, offshore BPO is expected to represent 2.3 percent of the total BPO market."

- Gartner Research, May 18, 2004.

Given the exponential rise of IT outsourcing by U.S. corporations, it is easily justified to promote offshore outsourcing within your company for several well-known reasons, the majority being:

1. Breadth of knowledge can be adjusted dynamically to the needs of each project, so the technologies utilized merely become another variable to accomplish a business goal.
2. Cost of development moves from overhead budgets (full-time head-count) to operational budgets. This expense can now be justified by showing greater flexibility to increase/decrease manpower over the short-term.
3. Offshore manpower costs are often substantially lower than domestic rates.

For all inherent benefits of offshore outsourcing, there exists a powerful liability that, when left untreated, can have disastrous results. The dissemination of intellectual property occurs every time one business outsources another -- whether for payroll, advertising and especially IT development.

Consider these statistics. From the "2003 CSI/FBI Survey on Computer Crime and Security", 61 of 398 respondents acknowledged theft of proprietary information which resulted in financial loss totaling \$70M¹. In the "2003 BSI Computer Theft Survey" of 676 participants, 9.2% of respondents who acknowledged theft of proprietary information stated the financial loss at \$1M and 2.3% valued the loss at \$10M². Would any company hand over intellectual property to an unmitigated risk? Yet, it happens, as exemplified by the source code leaks for both Microsoft and Cisco. Could they have been avoided? Not completely, but it should serve as a wake-up call to all businesses to review their IP protection policies with all their partners, especially those which exist outside a company's base operating country.

How one approaches intellectual property protection (IPP) can affect the overall effectiveness and efficiency of any outsourcing effort. A traditional project manager will start with a baseline savings of efficiency (time, expenses, et al) and reduce each benefit by applying the cost of risk factors in the 80/20 fashion. A security professional will always start with a baseline cost of

protection planning and overlay the benefits to assess a spectrum of “best-case” to “worst-case” scenarios. From these scenarios, a risk / remediation analysis is presented to management, whereby the business can make an informed decision on the amount of risk it is willing to expose. Given the extra up-front planning efforts needed by multiple business branches to implement the security professional’s method, which would in reality get the most support from the decision-makers in your company?

IPP assessments for outsourcing can be daunting, but by breaking the effort down into the risk areas below, much of the assessment needs to be done only once, and can be re-used for subsequent outsourcing projects. Following is a pared-down checklist that can assist in the planning effort for IPP and outsourcing:

Business Assessment

(What are the official host company’s security policies for IPP?)

- Where is the company's base of operation?
 - Does the company have international offices with legal representation?
- Does the company currently outsource IT development efforts?
 - Within those countries with international offices?
 - In countries without the company’s international presence?
- How does the current project rely on trade secrets or other intellectual property?
 - Are these IP assets considered tangible or intangible?
 - What amounts of risk are attached to these IP assets?
 - What methods of assessment were applied to arrive at these figures?
- What existing policies are in place to protect IP during development?
- Does your company specifically address IP protection and outsourcing?
 - What IPP compliance does the company require from outsourcing companies and other partners? (bonding, et al)
 - What is the cost of creating/supporting such policies?
- What existing experiences with IPP can be drawn upon?
 - Are these experiences formally documented?

Legal Assessment

(What legal tools support international protection of IP?)

- What types of legal agreements are in place for:
 - Opening IP to outside parties? (NDA, et al)
 - Doing sensitive business internationally?
- What legal options are available for non-compliance or breach of these agreements?
- What international laws are provided to pursue non-compliance?
- What protections does the outsourcing company’s host government provide?
 - In what venue must legal proceedings occur?
- Have there ever been any accusations of breach or threat of legal action?
 - If so, how was it handled?
 - What internal actions were taken as a result (change of policy, et al)?

Outsourcing Assessment

(What are the official outsourcing company's security policies for IPP?)

- How does the outsourcing company approach the topic of IP-based contracts?
- What internal policies are in place to protect their clients' IP?
- How do the outsourcing company's protection policies compare to those of the host company?
 - Where do the policies go above and beyond your policies?
 - What specific points do the policies lack?

Accountability Issues

Accountability, as a management tool, is necessary to measure project flow, define remediation procedures for any fallout, and provide root cause analysis for future prevention. Accountability methods work best within controlled environments (i.e. within the enterprise). When uncontrolled factors are introduced, normal accountability methods can actually create a false sense of completeness. Two major issues exist when an accountability matrix includes outsourced personnel.

The first issue with accountability is the lack of host company presence at outsourced work offices. Much of traditional compliance validation comes implicitly from direct (formal and informal) contact with employees. Since the loss of intellectual property can cause irreparable damage to your company, careful planning is needed to validate compliance early and often, especially in the absence of direct contact with the outsourced employees. Scheduled as well as unscheduled onsite visits are crucial even if other travel budgets are frozen. First-hand documentation of compliance is a necessity. To highlight this point, the New York State Department of Environmental Protection relies almost solely on company-generated reports for water pollution control compliance; whereas in another realm, the Department of Defense has inspectors sent to every vendor facility to ensure spec compliance on *each batch* of materials purchased. Which method of compliance validation matches the needs of your project? (I personally avoid swimming in NYS waterways.)

The other major issue with accountability is remediation. An IT manager has not only the power but also the responsibility to enforce all company policies with respect to protecting company property. An IT manager may even have the power to choose outsourcing companies based on their policies and past experience. But once a contract is determined to be out of compliance, an IT manager may need to turn to the legal staff to enforce remediation. In other words, even if an offshore outsourcing firm has identical IPP guidelines as the host company, compliance is ultimately determined by the laws in the country of arbitration defined in the outsourcing contract. Accountability is no longer an issue of meeting deadlines, but rather a basis for possible legal action.

What Are the Next Steps?

(Document, Document, Document)

- Modify your accountability methods to ensure compliance by focusing on three areas: validate formally, validate consistently and validate often.

- Determine the measurement criteria that would positively identify an intellectual property breach. *This cannot be overstated.* These criteria become the pinnacle for any investigation or legal actions. Too ambiguous: no legal case can use them. Too detailed: a breach may not be caught because all the identifiers were not triggered.
- Ensure that these findings are well communicated with all decision-making parties.
- Ensure the legal support staff includes these aspects with all written contracts. The legal department will most likely define the company's host country as the point for arbitration.
- Ensure the outsourcing parties understand these aspects. This is most effectively accomplished by having the outside parties present a formal document on how they comply with your IPP guidelines.

Creating your "IPP Guideline for Outsourcing" now can save many troubles years down the road. Regardless of any business partners' guidelines and procedures for IPP, it is still *your* company that is held liable for compliance with SOX and HIPAA.

John C. Checco, CISSP (john.checco@checco.com) is a member of the American Society for Industrial Security (ASIS) NYC Chapter and president of bioChec™ (www.biochec.com), a division of Checco Services, Inc

¹ "2003 Computer Crime and Security Survey", FBI / Computer Security Institute., pp 10-12.

² "2003 BSI Computer Theft Survey", Brigadoon Software Inc., pp 17-20.