

# Security Risks of I.T. Offshoring

**Brian Stygar, Principal**  
**Kore Federal**  
**bstygar@korefederal.com**

## 1.0 Introduction

Offshore outsourcing is a trend that most American businesses can no longer ignore. Once used only by application vendors to reduce the cost of software development, outsourcing to offshore development firms has matured into a standard practice for many U.S. companies. Although cost savings is the predominate reason for this trend, higher quality, faster development lifecycles, highly educated technical resources and time-zone advantages are becoming increasingly compelling factors.

Though the leading offshore outsourcing firms provide an array of IT services including application hosting, datacenter operations, data processing, and helpdesk support, application development and maintenance services are on the forefront. Moving application development and maintenance tasks offshore however introduces many risks, many of which are security related. The risk of security breaks and intellectual property protection are and will continue to be a major concern when working in an international setting. Fortunately, these risks can be mitigated with proper planning and management of the outsourcing relationship.

## 2.0 Industry Trends

In the last 8 years the industry has witnessed a growth rate of 20% - 25% per year, with no evidence of slowing. [1] According to Gartner, by year-end 10% of all information technology based jobs in the United States will move to emerging markets and more than 80 percent of American companies will have discussed offshore outsourcing. More than 40 percent of U.S. enterprises will have tried a pilot program or actual outsourcing either offshore or nearshore. Forrester Research predicts that by 2020 more than 3.3 million IT jobs will have moved offshore. [2]

Through 2007, transformational services, such as business process outsourcing will segment along horizontal (function commonality) and vertical (specialized) business service outsourcing functions. [1] This trend is especially prevalent for services related to application development and maintenance. According to a survey developed by Forrester, custom application development and maintenance are the two most predominant services outsourced to offshore providers, over COTS implementation and maintenance, helpdesk support and IT infrastructure management. [3].



The benefits of this model are compelling to almost any business that has a significant IT budget set aside for developing applications that automate critical business processes. Major offshore vendors have proven that they can deliver high quality levels by becoming certified by industry accepted standards bodies such as the Software Engineering Institute's Capabilities Maturity Model and the International Organization for Standardization. These firms have demonstrated over the last several years that they can meet tight deadlines by dedicating resources for particular projects. They have also proven to be flexible development partners by supplementing existing domestic teams with skilled technical resources in a short time frames. Of course the most compelling advantage of this model is related to labor costs. In a recent CIO magazine survey, the majority of IT executives cited lower IT costs as the main reason for outsourcing offshore with the greatest savings realized in the area of labor costs. [5] Despite the fact that offshore application service costs are on the rise, international labor rates will continue to be competitive in the foreseeable future. McKinsey Consulting estimates that by 2010, the U.S. IT industry will save \$390 billion through offshore outsourcing of software development. [1]

### 3.0 Security Risks

Firms looking to outsource application development and maintenance initiatives to offshore providers need to consider all the associated geopolitical and technical risks before endeavoring in this global economy. Unfortunately, many companies looking to

farm out their development work only think about the dollar savings and can lose focus of everything else, including the security implications.

According to Gartner, information security concerns around global sourcing will gradually take center stage alongside public concern over job losses. Analysts say that as offshore outsourcing evolves to increasingly complex global projects involving core competencies, the cost and exposure of inadequate attention to security will increase significantly. [6] Most business leaders agree with this analysis. In a recent poll by CSO Online, 85% of the respondents agreed that offshore outsourcing of code development can constitute a significant security risk. [7]

The security risks are widespread and complex as they involve economic, geopolitical, national, and organizational factors. Trade embargos, constant changes in U.S. policy towards other countries, cultural compatibility, differences in legal systems, reliability of technical infrastructure, and economic stability all contribute to the volatility and complexity of the global outsourcing environment. National security issues and terrorist threats of late have only compounded the issues. According to Rich Mogull, research director for information security and risk at Gartner Inc. in Stamford, Connecticut, "The security risks offshore generally aren't any different than the security risk you face onshore; [however] the distance and different laws and government philosophies can create more risk." [8]

As U.S. companies consider outsourcing critical IT services, including software development, to countries such as India, Pakistan, Russia and China, they need to do a sanity check in light of recent changes in the global security environment. Recent trends show the countries the software industry trusts the least with binary code are the places where source-code development is being sent. Of particular concern is the work that is being sent to China. While not yet a major provider of outsourcing services, China has a significant economic espionage program that targets U.S. technology. Also of concern are countries in Southeast Asia, particularly Malaysia and Indonesia, where terrorist networks are known to exist. [9]

IT organizations evaluating the offshore outsourcing model should question whether vendors have sufficiently robust security practices and if vendors can meet the security requirements they have internally. While most IT organizations find offshore vendor security practices impressive, the risk of security breaks or intellectual property protection is inherently raised when working in international business.

## 4.0 Risks Related to Intellectual Property (IP)

Although low-value projects may have been the initial target for outsourcing, American firms are now outsourcing initiatives that often involve “keys to the kingdom” such as core technologies or state-of-the-art research and development projects. These are the projects that must be protected at all costs. [10] IP related security issues are actually amplified in the offshore development model because the points of failure increase dramatically, and control over those points frequently rests outside the security policies

of the home country firm. IP risks can include patents, corporate trade secrets, pirated or unlicensed software, copyrights, or even 3<sup>rd</sup> party IP violations. [11]

There are several recent cases where IP rights of US firms were violated by engineers working for offshore outsourcing companies. The first known case occurred in August, 2002: “Nenette Day walked into the Ashoka, one of the city's best hotels, for a meeting with Shekhar Verma. Verma had been fired from his job at Geometric Software Solutions Ltd. (GSSL), an outsourcer based in Bombay. He claimed to have the source code for SolidWorks Plus's 3-D computer-aided design package, which GSSL was debugging. Verma had contacted a number of SolidWorks' competitors and offered to sell them the source code. The arrest led to the first prosecutorial filing for outsourcing-related intellectual property (IP) theft in India, in a case that may come to trial before year's end. Verma might well win his case. Because the source code didn't belong to GSSL, technically, Verma didn't steal from an Indian company. Thus India's laws don't necessarily apply.” [12]

Other noted cases include Legato Systems alleging that eight of its former employees in India took some of its intellectual property with them when they went to a competitor. Another instance involved a U.S. company that outsourced product design to an Indian firm, which successfully completed the project and turned around and used the code to create a version for the Indian market. [12]

IP risk is a unique risk in offshore development, primarily because of the cultural differences. Offshore development projects involve managing multicultural teams across international and cultural borders and different cultures have different value systems.

[11] For instance, standards of privacy are often looser in India because it's a close-knit society where, for instance, reading someone else's e-mail wouldn't be considered much of an intrusion. This more relaxed attitude toward privacy and intellectual property could have serious consequences when it comes to protecting corporate assets. Most companies understand that there are security issues with offshoring, but the real issues are cultural and in compliance and regulation. [13]

It is even possible for offshore developers to inadvertently introduce open-source code into customer applications and put the customer at risk of non-compliance with US IP laws. It's not that Indian, Chinese or other programmers based outside the U.S. have malicious undermining of intellectual property in mind; it's just that it's so easy to do inadvertently. Oftentimes, developers just find “freeware” components on the Web and drop them into their code. Unfortunately, inserting open-source code could conflict with the customer's licensing plans, especially if the end product is intended to be proprietary.

[14]

Typically, offshore vendors work via the Internet off their clients' systems, applications and data, which all are housed on the customer's own site or secure network. IP risks can be introduced as outsourced staff is given access to systems within the customer's network. Many companies give outsourcers VPN access to development systems for

system maintenance, coding and testing. Although a company may be accustomed to provided network access to domestic vendors, offshoring cast the practice in a new light by opening the door to into the soft center of the intranet to low-paid, relatively high-skilled, unknown workers. [15]

The risk's introduced by opening the networks to offshore vendors are increased as most offshore vendors do a poor job of protecting their own networks. Hackers may find it easy to first break into an offshore firm's network, and then pose as a developer or tester to access the customer's network and systems. It is very difficult to manage or influence the strength of the offshore vendor's infrastructure.

Most of the largest outsourcing firms have international certifications that require regular security audits. U.S. companies that use them, or that set up their own facilities in foreign lands, are probably not exposing themselves to more hacking risk than they would face here in the United States. However, many U.S. companies are turning to small and mid-sized outsourcing firms that don't have security policies in place to protect their networks and systems. [16]

Even though countries like India are trying to step up by creating and enforcing anti-hacking laws, many countries such as Bulgaria, Romania, the Philippines and China are still way behind. Russia in particular is known for its rising cyber-crime and hacker underground. Many of the well-publicized hacks involving credit card theft and other financial crimes so far have turned out to be perpetrated by Russians. [16]

## 5.0 Risks Related to Hidden Malware

Another security risk that is manifested when working with offshore vendors is related to the insertion of malicious software in the outsourced application code. Malicious software or malware is code that is specifically designed to damage or disrupt the system, such as a virus or a Trojan horse. The threat of malware is limitless as it can expose backdoors to a company's network and systems, and provide access to critical business data. Malware can also be used to destroy data or shut down systems entirely.

Most analysts agree that with more critical code being shipped overseas, companies are opening themselves up to a host of potential problems. It is very difficult to directly link the security violations with the popularity of offshoring, because it's virtually impossible to find unauthorized malware hidden deep within sophisticated, multi-tiered applications with data normalization, messaging middleware and other modules originating from software production houses in a half-dozen countries. [17] With the United States Computer Emergency Response Team (US-CERT) reporting approximately 100,000 security breaches in 2002 (a 10 fold increase from 1999), it is hard to ignore the correlation between this statistic and explosion in offshore outsourcing. [18]

India among other major offshore outsourcing countries is making a concerted effort to improve information technology security laws and capabilities, but the complexity and expense is enormous given their current environment. Based on a U.S. model of

spending 5% to 7% of the IT budget on security, and with the IT budget consuming 15% of a service company's revenue, India should be ramping up to spend \$450 to \$600 million on information security and assurance by 2008. [8]

### 6.0 Mitigation Strategies

Despite the numerous and significant security risks associated with outsourcing application development and maintenance offshore, there are many steps that US businesses can do to help mitigate these risks. According to Gartner, Caveat Emptor is the guiding principle for securing offshore IT operations. The first critical step before endeavoring in this business model is doing an investigation of potential offshore service providers and exercising due diligence and due care. Those contemplating a move offshore should have an understanding of the host country's legal climate, as well as an understanding of their security needs. [8]

US companies must understand that information security is part of the cost of doing business offshore and these costs start accumulating during initial planning. It is critical to implement a planning process that tightly integrates all security related factors. US companies are encouraged to know their security, privacy and intellectual property requirements before they start. They need to do a thorough security evaluation before signing any agreements that include regulatory compliance. [8]

The planning process should include a gap analysis that helps to determine the customer's security readiness and sets expectations for securing the offshore operation. Key areas to be reviewed are access control, network security, facilities and operations,

and applications security. Security considerations include confidentiality and service level agreements that tighten security with a veil of secrecy and contain provisions for vulnerability assessments external audits, and security process audits. [8]

Companies beginning the due diligence process can leverage a risk assessment model that Gartner has developed to help enterprises evaluate the risks of security regulations when going global for their workforces. The model that tabulates a country's risk status by taking into account such elements as the country's track record in adhering to its security provisions, the indigenous "culture" of privacy, the risk of government interception of data and limits on encryption, and protection of intellectual property. [10]

As part of the due diligence effort, US companies should look for relevant certifications. For instance, the International Information Systems Certification Consortium, which administers the industry accepted Certified Information Systems Security Professional (CISSP) exam, has over 650 Indian and Chinese CISSPs who have voluntarily registered on its Web site, from a broad mix of U.S., Indian and Chinese companies. [8]

There are specific strategies that help mitigate intellectual property related security risks. It is important to consider the offshore company history and financial stability. Firms are encouraged to use offshore service providers that have high employee retention rates, train their staff to adhere to American privacy standards and perform background checks on local staff. One way of ensuring that these steps are taken and security and regulatory compliance concerns are met is to put the onus on the outsourcing provider by writing it into the contract. The most effective approach, however, is to physically go and check the outsource centers regularly. [13]

From an IP risk perspective, companies are better off outsourcing to Indian service providers than companies from other popular offshoring countries. India has a much better cultural and legal climate for IP protection than many other nations offering offshore coding. India has a culture that generally seems to respect intellectual property, as compared with China or Russia. India is also a member of the World Trade Organization and adheres to its intellectual property add-on, Trips (Trade-Related Aspects of Intellectual Property Rights). Fortunately, several of the largest Indian outsourcing companies are incorporated in the United States and can be sued here. [12]

There are also specific mitigation strategies for addressing risks associated with hidden malware. First, companies should identify and correct security vulnerabilities before code is shipped to the offshore facility and then recheck the new code for potential "Trojan horses" before it is submitted into the build process. [18]

Companies are encouraged to leverage the File Signature Database (FSDB), which uses hash values to protect software integrity from malicious additions. The FSDB includes code module attributes such as a creation date, file name, digital hash value and other unique attributes published by each of the vendors. Companies can verify the identity and integrity of the software running on their systems by comparing it against a heterogeneous collection of "good file" information contained in the FSDB. [17]

Software traceability is another effective method for discovering software defects that expose an application to a myriad of exploits, viruses and worms. Traceability allows a given line of code or a software module to be tracked back to the developer. This method is viewed as the Holy Grail in combating hidden malware, so it is important for a

company to force the outsourced vendor to provide traceability in the application code.

[17]

A simple, but effective method for mitigating security risks when outsourcing application development offshore and providing connectivity to the home network is to only give system read access, not write privileges, to the developers and testers. Most testing activities do not require source-code access. It is also important to set up user authentication and firewall rules that constrain which IP addresses each offshore, remote user can access. Firewall rules only lock down the first hop preventing outsourced programmers to "root" development machines and install Trojan horses, corrupt production databases and cause other problems. Development hosts should be zoned off into private areas and intrusion-detection system should be implemented to scan for improper traffic. These are all cost effective network and infrastructure provisions that can be implemented to protect corporate assets when providing local network connectivity to offshore providers. [9]

As American business seek the offshore outsourcing model for their application development and maintenance initiatives it is critical that they recognize and address the aforementioned security related risks. They should leverage the numerous available tools and strategies to mitigate these risks, starting from the initial evaluation and planning process through the lifecycle management of outsourcing relationship.

References

1. Davidson, D. "Top 10 Risks of Offshore Outsourcing," *Tech Update*, [online] 1/9/2003. [http://techupdate.zdnet.com/techupdate/stories/main/Top\\_10\\_Risks\\_Of\\_fshore\\_Outourcing.html](http://techupdate.zdnet.com/techupdate/stories/main/Top_10_Risks_Of_fshore_Outourcing.html). (Accessed: 10 December 2004).
2. Pastore, M. "Who Gains from Offshore Outsourcing?", *IT Management*, [online] 12/4/2003. <http://itmanagement.earthweb.com/career/article.php/3116511>. (Accessed: 10 December 2004).
3. Martorelli, William "Indian Market Booms, But Changes Loom", *Optimize*, pp. 23-26, September 2004
4. L. Carrllo, K. Desronvi, and C.Niven "Offshore Outsourcing, Is It a Viable Approach for All Software Development Projects", *AMR Research Report*, pp.1-7, June 2002
5. Ware, L. "Weighing the Benefits of Offshore Outsourcing", *CIO Research Reports*, [online] 9/2/2003. <http://www2.cio.com/research/surveyreport.cfm?id=62>. (Accessed: 10 December 2004).
6. "Gartner Sees Security Issues on the Global Sourcing Horizon", *Tekrati*, [online] 9/21/2004. [http://www.tekrati.com/T2/Analyst\\_Research/ResearchAnnouncementsDetails.asp?Newsid=3680](http://www.tekrati.com/T2/Analyst_Research/ResearchAnnouncementsDetails.asp?Newsid=3680) (Accessed: 13 December 2004).
7. Security Check Results, *CSO Online*, [online] 2003. <http://www.csoonline.com/poll/results.cfm?poll=771> (Accessed: 13 December 2004).
8. Willoughby, M. "Offshore security: Considering the risks", *Computerworld*, [online] 9/15/2003. <http://www.computerworld.com/managementtopics/outsourcing/story/0,10801,84671,00.html>. (Accessed: 13 December 2004).
9. Verton, D. "Offshore coding work raises security concerns", *Computerworld*, [online] 5/5/2003. [http://www.computerworld.com/managementtopics/outsourcing/story/0,10801,80935,00.html?from=story\\_picks](http://www.computerworld.com/managementtopics/outsourcing/story/0,10801,80935,00.html?from=story_picks). (Accessed: 13 December 2004).
10. Keizer, G. "Security key concern in outsourcing : Gartner", *IT NEWS*, [online] 9/23/2004. <http://www.itnews.com.au/newsstory.aspx?ClaNID=16443&s=%22offshore%22+>

%22outsourcing%22+%22security%22+%22risks%22. (Accessed: 13 December 2004).

11. Bakalov, R. "Risk Management Strategies for Offshore Application and Systems Development", *Information Systems Control Journal*, Vol. 5, PP36-38, 2004.

12. Fitzgerald, M. "Big Savings, Big Risk", CSO Online, [online] 11/2003. <http://www.csoonline.com/read/110103/outsourcing.html>. (Accessed: 13 December 2004).

13. Pruitt, S. "When outsourcing, don't forget security, experts say  
Companies often forget about cultural differences that may affect security", *Computerworld*, [online] 9/21/2004. <http://www.computerworld.com/managementtopics/outsourcing/story/0,10801,96074,00.html>. (Accessed: 13 December 2004).

14. Hall, M. "Pop by Your Service Provider in the ...", *Computerworld*, [online] 9/6/2004. <http://www.computerworld.com/softwaretopics/software/story/0,10801,95697,00.html>. (Accessed: 13 December 2004).

15. Blum, D. "Weigh risks of offshore outsourcing", *Network World Fusion*, [online] 3/8/2004. <http://www.nwfusion.com/columnists/2004/0308blum.html>. (Accessed: 14 December 2004).

16. Kirby, C. "Hacking danger for outsourced records hard to gauge", *San Francisco Chronicle*, [online] 3/28/2004. <http://sfgate.com/cgi-bin/article.cgi?f=/c/a/2004/03/28/HACKING.TMP>. (Accessed: 14 December 2004).

17. Willoughby, M. "Hidden malware in offshore products raises concerns", *Computerworld*, [online] 9/15/2003. <http://www.computerworld.com/securitytopics/security/story/0,10801,84723,00.html>. (Accessed: 13 December 2004).

18. "Offshore development: Ramp up projects quicker, minimize code risks with Klocwork", *Klocwork*, [online] <http://www.klocwork.com/areas/offshoring.asp> (Accessed: 13 December 2004).