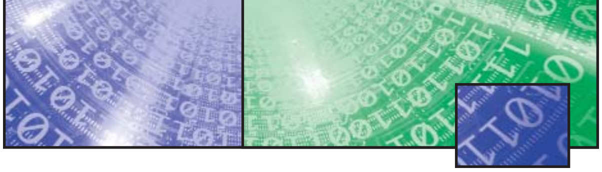
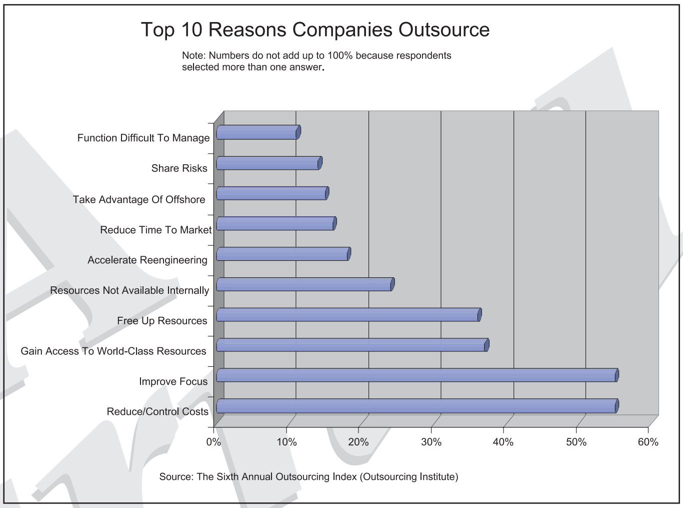


Security Risks Associated with Geosourcing

By Dr. Richard Bassett, Vincent Ierace, Ellen Murphy and Riccardo Palmerini

Introduction

Major firms today are looking for ways to reduce costs, increase efficiency and flexibility while expanding operations to provide around the clock services (see figure 1–Why companies outsource). One of the ways that organizations are attempting to achieve these goals is through the outsourcing of their information technology and service needs overseas. Overseas outsourcing, also referred to as offshoring or geosourcing, is defined as the transfer of ownership of a business process to an outside global supplier. While the expanding availability of global broadband access to the Internet has enabled organizations to outsource overseas an increasing diversity of IT services and business processes, it has introduced significant risks associated with the underlying electronic collaboration. These risks include loss of confidentiality, integrity and availability of data, applications and systems as well as issues of authentication and non-repudiation. This article will focus on an assessment of the types of risks that overseas outsourcing presents, factors that influence these risks as well as legislative and regulatory considerations when outsourcing overseas. Case studies will be presented related to three types of security breaches, in addition to controls that can be implemented to prevent and mitigate risks.

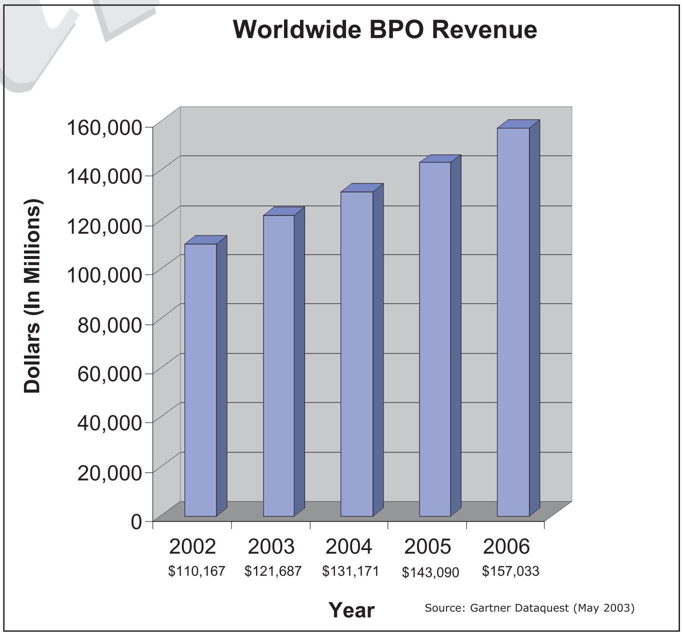


Source: The Sixth Annual Outsourcing Index (Outsourcing Institute)

Figure 1: Why Companies Outsource

Benefits

As outsourcing appears to offer competitive advantages, U.S. companies are increasingly looking to countries in the Asia/Pacific region and Eastern Europe for their outsourcing needs in areas of application development (coding, testing and maintenance), network management and helpdesk support in addition to business processes (see figure 2–Worldwide business process outsourcing revenue growth) such as call centers, claims processing, medical and legal transcription as well as various financial services. The business processes that are being outsourced have traditionally been those that, while important to an organization, do not differentiate a company from its competitors. Outsourcing of these activities allows the company to focus on their core competencies, eliminating "internal diversification". According to a study by J.P. Morgan, companies that are focused outperform their diversified counterparts by almost 20% in the marketplace[1]. Since the service being offered by the supplier is the supplier's core competency as opposed to being an overhead activity to the organization that is outsourcing, it is believed that the supplier can provide a superior, more consistent process and that the economy of scale that the supplier realizes by offering the same type of service to multiple clients, allows the supplier to provide the service at a lower cost than the organization that is outsourcing could achieve if kept in-house. Outsourcing overseas is believed to provide further advantages in terms of a readily available, educated, lower-wage labor pool and the difference in time zones supports reduced cost, multiple shift operations. A recent study by Gartner Inc. predicts that by 2004, more than 80% of U.S. companies will consider outsourcing critical IT services overseas[2].



Source: Gartner Dataquest (May 2003)

Figure 2: Worldwide Business Process Outsourcing (BPO) Revenue Growth

Risks

The growing trend to outsource increases the potential of major security breaches for firms venturing overseas since most organizations fail to fully assess or mitigate the unique and increased risks associated with different environmental, legal and geopolitical systems.

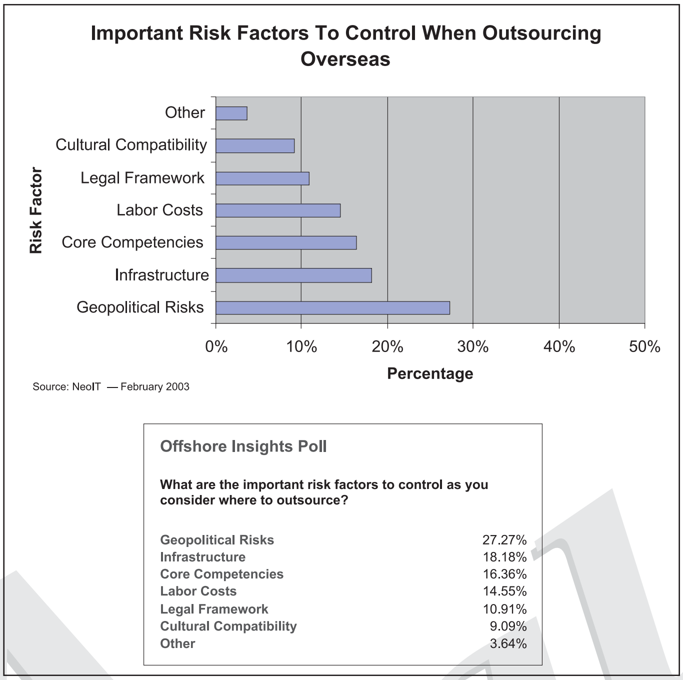
Technical and Operational Risks

There are significant technical and operational risks involved with overseas outsourcing. Of the significant risks associated with offshore outsourcing, risks related to confidentiality, which is the unauthorized access, disclosure or interception of data are greatly increased since information sent across major continents must travel through various networks of unknown security statuses. Additionally, the nature of outsourcing transfers control of access to proprietary systems and confidential information at the overseas location to the outsourcing vendor, presenting additional risk. The ease of outsourcing due to the Internet combined with the fact that the vendor is an autonomous organization to the company outsourcing, increases the threats to confidentiality as well as to the integrity of data and applications since opportunities to fabricate or modify data during transmission or when stored in a database are more likely to be exploited. The introduction of malicious code to applications further presents a risk to integrity. David McCurdy, a former congressman from Oklahoma and executive director of the Internet Security Alliance believes that the risk from offshore outsourcing was "the most serious of the industry-based issues that this country faces[3]."

Systems and applications are at risk of being infected with malicious code from Trojan horses, viruses, sleeper bugs (time or logic bombs) and trap doors. These threats can result in information leaks, unauthorized access and unavailability or destruction of data, applications and systems. Denial of Service (DOS) attacks, deletion of applications and data, theft or destruction of hardware are potential availability risks a firm may incur when outsourcing offshore. These risks have proven to have merit as "there have been a number of cases where software was found with intentionally planted back doors," according to Shawn Hernan, team leader for vulnerability handling at the CERT Coordination Center at Carnegie Mellon University. "Most of these were for providing support, although no such support option was given to commercial customers[2]." While experts agree that it is virtually impossible to find unauthorized malware hidden deep within a sophisticated multi-layered application with data normalization, messaging middleware and other modules originating from labs in a half-dozen countries[2].

Geopolitical Risks

Geographic factors, infrastructure maturity, political stability, legal disparity and differing government philosophies can influence risk. In a survey taken by NeoIT, provider of offshore advisory and management services, the highest-ranking risk factors to control when considering where to outsource were geopolitical risks followed by infrastructure risks (see figure 3—Important Risk Factors)[5]. Forrester Research estimates of the 3.3 million American IT jobs moving offshore by 2015 (see figure 4 – What business areas are outsourcing jobs overseas), 70% will move to India, 20% to the Philippines and 10% to China[3].



Offshore Insights Poll

What are the important risk factors to control as you consider where to outsource?

Geopolitical Risks	27.27%
Infrastructure	18.18%
Core Competencies	16.36%
Labor Costs	14.55%
Legal Framework	10.91%
Cultural Compatibility	9.09%
Other	3.64%

Figure 3: Important Risk Factors

Infrastructure and Environmental Risks

Outsourcing creates a significant dependency on the availability and consistency of electrical power and bandwidth for both voice and data communications. Extended, sporadic system failures, short, recurring outages and slow response times during peak hours will impact availability of systems and data as well as productivity[6]. Additionally, a geographic location's remoteness and vulnerability to natural disaster such as floods or earthquakes also pose considerable risk to business continuity at that location. Although the overseas IT services sector has not seen a substantial disruption of operations resulting from a catastrophic event, it not difficult to apply the impact that a similar event to that of the earthquake in Kobe, Japan which devastated the infrastructure and had global impact on the production of chip manufacturing, might have on the availability of outsourced IT services being delivered from concentrated areas such as Bangalore or Hyderabad, India.

Political Risks

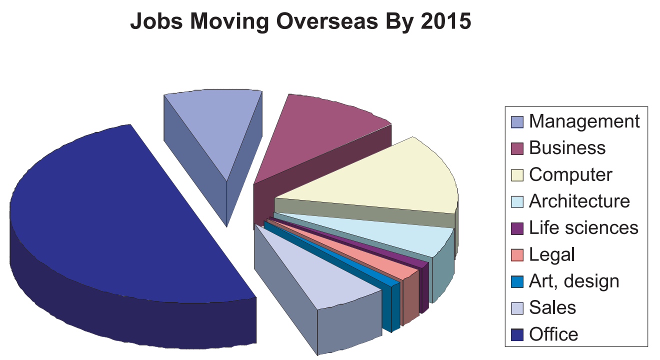
Political climate influences risk from a number of sources. The Philippines, India and Russia have political instability or military tension in at least some regions. Aon Trade Credit, underwriter of political risk insurance, rates India, China and Russia as moderate risk and classifies the Philippines as medium-high and Pakistan as a high-risk area, when considering political and economic risk factors[7] while in Southeast Asia, Malaysia and Indonesia are known to have terrorist networks operating from within their borders[2]. For organizations looking to outsource overseas, consideration must be given to the potential of a change in government and its affects on outsourcing vendor's operations and that country's economic policies, incidence and attitude towards corruption, likelihood of labor unrest, latent level of anti-U.S. sentiment within that country and personnel security risks of U.S. visitors. In Hyderabad, India, a city within the state of Andhra Pradesh with a high concentration of offshore development and call centers, a security risk exists. Maoist rebels belonging to the People's War Group (PWG), with the goal of creating a communist state, have waged a three-decade insurgency against "anti-poor" government policies. In October 2003, rebels were identified as responsible for the assassination attempt on Chief Minister N. Chandrababu Naidu, wounding him and IT Minister Gopalakrishna Reddy[8], a champion of globalization and exportation of IT services. Events such as the unexpected change in foreign government may have an unforeseen impact on business continuity and the geopolitical climate within a country. For example, in India, where Forrester Research is predicting 70% of outsourced jobs will relocate to, uncertainty about the influence that communist parties will have as a result of recent elections was blamed for the greatest one day market plunge of the Bombay Stock Exchange, the Sensex as well as the Nifty Index of the National Stock Exchange. This uncertainty is due to concerns that the incoming Congress party may slow privatization of state-run companies and reverse market-friendly policies.

Espionage

Risks from government sponsored and industrial espionage are greater when outsourcing overseas. The Industrial Espionage Act of 1996, which made it a criminal offense to steal trade secrets, does not apply to non-U.S. citizens acting outside of U.S. borders[4]. Independent multinational groups are working to address issues related to security of software development; however India and China have not committed to the Common Criteria process for testing software to check for common vulnerabilities in order to assign a security profile[9] while China has been identified as having an economic espionage program that targets U.S. technology[2]. Adding to the risk is the susceptibility to industrial espionage being greater in poor countries that often lack laws to protect foreign companies and rarely enforce the laws that may exist[4]. As a result, it is important to be aware that foreign governments and international competitors may target your outsourcing vendors overseas in order to obtain information about your organization and customers since these acts would be outside the jurisdiction of the U.S. courts.

Intellectual Property Theft

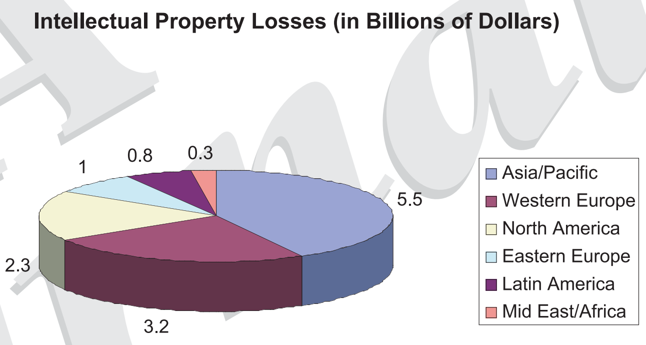
Intellectual property laws and respect for intellectual property rights differs overseas (see figure 5—The cost of Intellectual Property Theft (June 2003)). It is common perspective that China, a member of the World Trade Organization (WTO), regards intellectual property as communal property, especially that of foreigners. The WTO's charter has an add-on, Trade Related Aspects of Intellectual Rights (TRIPS). However, even if a country is a member and adheres to TRIPS, enforcement is at a low level and if a country's culture does not respect property, courts are unlikely to enforce these laws[4]. Piracy rates (see figure 6—Piracy rates (2001 – 2002)) are also an indication of the risk level associated with intellectual property. China, Indonesia, Pakistan, India and the Philippines rank within the top 25 violators where China ranks second with a 92% software piracy rate and of these countries only Pakistan has decreased its piracy rate from 2001 to 2002[10]. The International Intellectual Property Alliance (IIPA) has recommended that China remain subject to Section 306 Monitoring as a result of the apparent unwillingness of the Chinese government to take the actions necessary to reduce piracy rates[11]. While a country's past record regarding respect for property rights also factors into risk. In 1977, the IT industry was nationalized by the Indian government, which forced multinational companies, including IBM, to withdraw from India[12]. IP theft overseas is a risk when using outsourcing vendors as well as when operating overseas. Legato Systems, developer of storage software, has alleged that eight former engineers in India took intellectual property with them when they went to work for a competitor. Bobby Young, Vice President and chief solutions officer of Legato speaking as a private individual, believes that it is better to bring skilled individuals from overseas to the U.S. rather than have them work in their home countries. Young stated that, "if you want to keep your intellectual property protected, keep it somewhere they have laws to protect it.[21]"



Source: Forrester Research, Inc. November 2002

Office	1,659,310	**Architecture**	184,347
Computer	472,632	**Legal**	76,642
Business	348,028	**Life sciences**	36,770
Management	288,281	**Art, design**	29,564
Sales	226,564	**Total**	**3,322,138**

Figure 4: What Business Areas Are Outsourcing Jobs Overseas



Region	Loss (In Billions)	Percentage
Asia/Pacific		
Western Europe		
North America		
Eastern Europe		
Latin America		
Mid East/Africa		
Total		

Figure 5: The Cost of Intellectual Property Theft

Hackers, Organized Crime Agents and Cyberterrorism

Concern is growing about abuse by hackers, organized crime agents and cyber terrorists in nations like Pakistan, the Philippines and Russia[3]. Organized criminal activities include copying of data to be exploited by an international identity theft ring while hackers may use or sell stolen credit card data. Cyber terrorists can disrupt a business's activities by infiltrating their systems; holding data hostage and demanding ransom to recover customer account databases or they may embed sleeper code (logic bombs, embedded viruses or worms) to target essential services such as SCADA, NYSE, hospitals, banks or the U.S. air traffic control system. These concerns are not limited to external sources, as insider fraud made possible by the outsourcing of help desk functions and network management, allows for the resetting of passwords, which can result in the disruption of access to servers or databases, fabrication or modification of data or use of the data for fraudulent activities[13]. Other countries like the U.S., are debating the security risks associated with overseas outsourcing. In response to the apparent illegal taking of sensitive financial information and credit card details from a British financial institution that had an overseas call center operation, a National Outsourcing Association (NOA) spokesman in Britain asserted, that there are some things that should not be sent overseas because "if you are using people in a low wage area, organized crime can afford to pay a lifetime's wages for data.[22]"

Legislative and Regulatory Considerations

Beyond the risk of direct losses caused by failure to meet security goals, an organization may be subject to penalties resulting from non-compliance with U.S. legislation and regulations applicable to financial, healthcare, pharmaceutical and defense industries (see figure 7—Legislative and Regulatory Compliance). Akiba Stern, Partner in NYC Office of Global Law and Consulting Firm, Shaw Pittman cautions that "the companies themselves know a lot about the regulations in their industries but the people who are doing the outsourcing don't[14]." Individual privacy legislation such as Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley (GLBA), California SB 1386 and the Notification of Risk of Personal Data Act (NORPA), still under senate consideration, include requirements for organizations to safeguard confidential data. While sections of Sarbanes-Oxley legislation, focusing on corporate conduct, specifically address security risks in regard to confidentiality, integrity and availability of financial and other critical information. Export regulations, International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR), both prohibit the release of data related to munitions or commercial products with potential military applications to anyone not a U.S. citizen or permanent resident alien[14]. Since, it is more difficult when outsourcing to control the flow of information and the safeguards used to protect it, compliance is at risk of being compromised. Additionally, an outsourced to vendor may be reluctant to be forthcoming about a breach or understand what constitutes a breach. The failure of timely disclosure or delayed rectification of the underlying cause has the potential of resulting in increased penalties and significant negative publicity for an organization.

Case Studies

The risks that are presented to information security when outsourcing overseas have been exploited and are apparent in current news. Three recent cases deal with intellectual property theft, threat of disclosure of sensitive, client data and compromise of control to vital source code.

25 Countries With the Highest Software Piracy Rates

Country	2001	2002
Vietnam	94%	95%
China	**92%**	**92%**
Other CIS	88%	90%
Indonesia	**88%**	**89%**
Russia	**87%**	**89%**
Ukraine	86%	89%
Pakistan	**83%**	**80%**
Nicaragua	78%	77%
Thailand	77%	77%
Bahrain	77%	76%
Qatar	78%	76%
Bolivia	77%	74%
Lebanon	79%	74%
Kuwait	76%	73%
Paraguay	72%	71%
India	**70%**	**70%**
Oman	77%	70%
Romania	75%	70%
Zimbabwe	68%	70%
Other Asia/Pacific	70%	69%
Bulgaria	75%	68%
El Salvador	73%	68%
Malaysia	70%	68%
Philippines	**63%**	**68%**
Nigeria	71%	67%

Source: Eighth Annual BSA Global Software Piracy Study — June 2003

Figure 6: Piracy Rates (2001 - 2002)

The first case deals with intellectual property theft against SolidWorks, who had outsourced the debugging of software code. Shekhar Verma, a former employee of Geometric Software Solutions Ltd. (GSSL), an outsourcer that is based in Mumbai (Bombay), India, claimed that he had the source code for SolidWorks Plus's 3-D computer-aided design package and contacted competitors of SolidWorks via e-mail to try to sell the code. The e-mail ultimately reached Nenette Day who arranged a meeting with Shekhar Verma. Day examined the source code and upon confirmation that it was the actual SolidWorks software code, they negotiated a price of $200,000 (reported to be valued at between $70 and $90 million). When the deal was concluded, the India Central Bureau of Investigation (CBI) arrested Verma. Day, a special agent for the Federal Bureau of Investigation's Boston's Cyber-crime division who had been contacted by SolidWorks after a competitor alerted them to the situation, was working undercover with the CBI[3]. However, since stealing trade secrets wasn't a crime under Indian law at the time, Verma had to be charged with simple theft. While Verma's attorneys claimed that SolidWorks did not have a case against him since he was not their employee[17].

The second case has to do with the risk of the disclosure of client, sensitive data and lack of control over confidential information. This case is of significant importance due to the enactment of HIPAA legislation. A Pakistani medical transcriber that was transcribing audio tapes of patient information belonging to the University of California at San Francisco Medical Center contacted the medical center threatening to post the records on the Internet. Lubna Baloch claimed that she was owed money from the person who subcontracted her. The medical center, which has a practice of not using offshore services, had originally outsourced the work to Transcription Stat, a company, in Sausalito, CA to do the work. Transcription Stat then outsourced the work to Sonya Newburn in Florida who then proceeded to outsource to Texan subcontractor, Tom Spires of Tutranscribe who ultimately hired Lubna Baloch in Pakistan. The audio recordings were sent to Pakistan, without the medical center's knowledge via the Internet with unknown safeguards. The medical center, after obtaining a retraction from Baloch on her threat, settled the dispute and no records were disclosed. In the end, the University of California at San Francisco Medical Center had no control over who was working with the patient data or how it was handled[20].

Additional cases continue to be documented. However, no case has had more widespread potential impact or media coverage than that of the recent posting of Microsoft Windows 2000/NT source code on the Internet.

The source of the leak, yet to be confirmed, appears to have originated from an outside organization that uses the code to enhance graphics for a CAD/CAM (Computer Aided Design/Computer Aided Modeling) application. Beyond the direct damage that Microsoft may experience, the availability of the source code presents significant threats to countless systems that use these versions of Microsoft Windows from those who will attempt to exploit the vulnerabilities that are now identifiable through the release of the source code.

Controlling and Mitigating Risk

Although the risks of offshore outsourcing are evident, there are controls (see figure 8—Controls) that can be put into practice to mitigate these risks. A risk assessment should be completed prior to entering into an outsourcing agreement and necessary controls identified. These controls should be written into contracts and must be clearly defined, including accountability for implementation and monitoring as to their effectiveness.

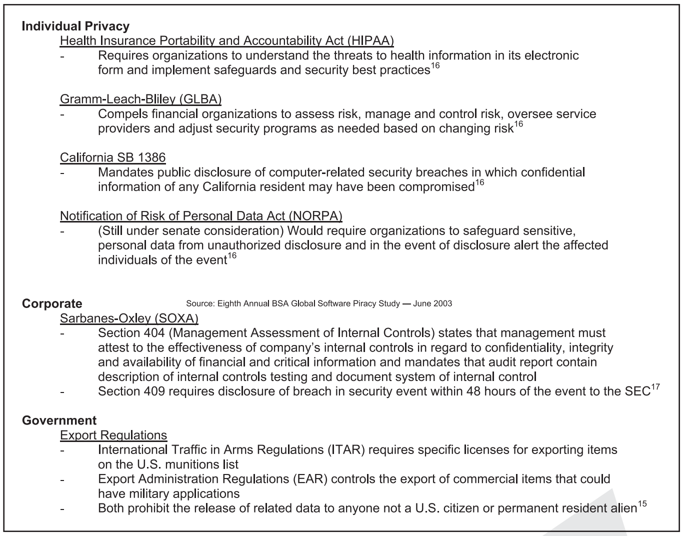
One control that should always be implemented is thorough checks of the physical security of the outsourcing site. It is necessary to control access to key systems and make sure that facilities have procedures so there is an audit trail of when people are at the site. It is recommended that an independent third party or non-offshore employees perform physical security audits of the offshore site to make sure that the security policy and systems are being enforced and properly maintained[18].

Controls should be implemented to ensure that all, important source code and confidential data are protected by a secure network incorporating strong encryption and authentication such as passwords and mandatory access controls systems. This will reduce the risk of unauthorized access to confidential data and systems while ensuring that data and applications will not become widely available in the country that is being outsourcing to or anywhere else. Offshore programmers should only have access to test data and not data that are sensitive or vital to a company's operations in order to prevent risk from disclosure of data[18]. Business process outsourcing, since by the nature of the service provided mandates that actual production data be used, requires additional safeguards and monitoring be implemented such as disabling of system drives, restriction on Internet and e-mail access as well as policies that control what is brought into a work area and is allowed to be removed.

It is important to make sure that there is a very good understanding of the legal system of the country where outsourcing will occur, supported by enforcement and international cooperation. Intellectual property agreements should be written into outsourcing contracts to clarify ownership. It is important to insist that outsourcing vendor has very strict human resources selection process while ensuring that the vendor, its employees and contractors are not currently and will not in the future be working for a competitor by obtaining non-disclosure, non-compete and confidentiality agreements from the outsourcing vendor and mandating that the vendor obtain them from its employees and contractors. Contracts should clearly define the outsourcing company's accountability for the actions of all their employees.

It is pertinent that a company outsourcing application development maintains backups of up-to-date source code at its non-offshore site. This will ensure that if an infrastructure failure or any other disaster happens offshore, loss of source code will not occur[18]. For business process outsourcing, as part of any outsourcing agreement, there should be a documented and tested disaster recovery and business continuity plan.

Knowledge transfer of all legislation and regulations that are industry specific is imperative. A legislative analyst may also be used to ensure legislative and regulatory compliance in operations and during software development.



Individual Privacy

Health Insurance Portability and Accountability Act (HIPAA)
- Requires organizations to understand the threats to health information in its electronic form and implement safeguards and security best practices[16]

Gramm-Leach-Bliley (GLBA)
- Compels financial organizations to assess risk, manage and control risk, oversee service providers and adjust security programs as needed based on changing risk[16]

California SB 1386
- Mandates public disclosure of computer-related security breaches in which confidential information of any California resident may have been compromised[16]

Notification of Risk of Personal Data Act (NORPA)
- (Still under senate consideration) Would require organizations to safeguard sensitive, personal data from unauthorized disclosure and in the event of disclosure alert the affected individuals of the event[16]

Corporate

Source: Eighth Annual BSA Global Software Piracy Study — June 2003

Sarbanes-Oxley (SOXA)
- Section 404 (Management Assessment of Internal Controls) states that management must attest to the effectiveness of company's internal controls in regard to confidentiality, integrity and availability of financial and critical information and mandates that audit report contain description of internal controls testing and document system of internal control
- Section 409 requires disclosure of breach in security event within 48 hours of the event to the SEC[17]

Government

Export Regulations
- International Traffic in Arms Regulations (ITAR) requires specific licenses for exporting items on the U.S. munitions list
- Export Administration Regulations (EAR) controls the export of commercial items that could have military applications
- Both prohibit the release of related data to anyone not a U.S. citizen or permanent resident alien[15]

Figure 7: Legislative and Regulatory Compliance

1.	*Clearly Defined Contracts*
2.	*Physical Security*
3.	*Secure Information Infrastructure*
4.	*Information Safeguards*
5.	*Confidentiality Agreements*
6.	*Intellectual Property Agreements*
7.	*Personnel Policies*
8.	*Backup Procedures*
9.	*Disaster Recovery/Business Continuity Plans*
10.	*Knowledge Transfer*
11.	*Audits*

Figure 8: Controls

Conclusion

Although increased and unique information security risks are present when outsourcing overseas and these risks have been exploited, it is unlikely that the trend to outsource offshore will subside any time soon based on Forrester Research 's estimate that 3.3 million American jobs will move offshore by 2015[5]. With research firm IDC predicting that 23% of IT services will be delivered from offshore centers by 2007 as compared to only 5% in 2003[19], organizations must integrate risk assessment and implementation of controls into outsourcing agreements in order to prevent the types risks that have been discussed. This is essential since the competitive advantage of a firm's decision to outsource overseas will dramatically decline when malicious acts are performed by individuals or groups who are seeking to profit or to potentially ruin a firm's reputation while jeopardizing its ability to exist. Add to this the undeniable reality that in today's world, military might has been replaced by economic power where the means to destroy economic power is through the targeting of a nation's businesses. As a result, U.S. businesses may find themselves more vulnerable when they outsource abroad.

Ultimately, organizations must stay aware that "when you outsource work, you also outsource control.[3]"

[1] Drisdale, Jr., John K. "Outsourcing Rewards and Risks." Available at: http://www.texasbusiness.com

[2] Verton, Dan. "Offshore Coding Work Raises Security Concerns." Computerworld (May 5, 2003) Available at: http://www.computerworld.com/managementtopics/outsourcing/story/0,10801,80935,00.html

[3] Schwartz, John. "Experts See Vulnerability as Outsiders Code Software." New York Times (January 6, 2003)

[4] Fitzgerald, Michael. "Big Savings, Big Risk." CSO Magazine (November 2003)

[5] Offshore Insights February Opinion Poll. Accessed on January 28, 2004. Available at http://www.neoit.com/asp/Editorialcomments-Feb-03.asp

[6] Funk, John, Sloan, David, partners; and Zaret, Scott, associate Day, Jones. "Beware the Dangers of Outsourcing." Bank Systems & Technology (April 7, 2003)

[7] Aon Political Risk Services - Political and Economical Risk Map (2004) Available at http://www.aon.com/us/politicalrisk

[8] Choudhury, Savitri. "Indian Police Turn Up Heat on Maoist Rebels as They Probe Assassination Bid." Agence France-Presse (AFP) (October 2, 2003)

[9] Willoughby, Mark. "Hidden Malware in Offshore Products Raises Concerns." Computerworld (September 15, 2003) Available at: http://www.computerworld.com/securitytopics/security/story/0%2C10801%2C84723%2C00.html

[10] Eighth Annual BSA Global Software Piracy Study (June 2003). Available at http://global.bsa.org/globalstudy/2003_GSPS.pdf

[11] International Intellectual Property Alliance 2003 Special 301 Report. Available at http://www.iipa.com/rbc/2003/2003SPEC301PRC.pdf

[12] Willoughby, Mark. "Offshore Security: Considering the Risks." Computerworld (September 15, 2003) Available at: http://www.computerworld.com/managementtopics/outsourcing/story/0,10801,84671,00.html

[13] Smith, Gordon. "IT Outsourcing: Placing Our Nation at Risk." Available at http://www.indyisaca.org/newsltr/2003/new0310/09-2003.pdf

[14] Overby, Stephanie. "How To Safeguard Your Data in a Dangerous World." CIO Magazine (January 15, 2004)

[15] Security Compliance. Available at: http://www.threatfocus.com/security_laws.php

[16] Thurman, Mathias. "Stepping Up to Sarbanes-Oxley." Computerworld (January 26, 2004) 32

[17] Garfinkel, Simson. "Information without Borders." CSO Magazine (January 2004)

[18] Fitzgerald, Michael. "Nine Steps That Can Help Protect Your Intellectual Property." CSO Magazine (November 2003)

[19] Metz, Cade. "Tech Support Coming Home?" PC Magazine (February 17, 2004)

[20] Lazarus, David. " A Tough Lesson on Medical Privacy Pakistani Transcriber Threatens UCSF Over Back Pay." San Francisco Chronicle (October 22, 2003)

[21] Withers, Stephen. "Outsourcing Overseas." Technology & Business Magazine (February 3, 2003)

[22] Warren, Pete. "India Call Centre Staff Bribed." Evening Standard (February 10, 2004)