Delta Technology Handbook Series:

Security and IP Risks When Outsourcing

Abstract: *Independent Software Vendors and Application Service Providers have become increasingly pressured by external market conditions when developing an offshore sourcing strategy, yet few properly understand and mitigate the associated security and intellectual property risks.*

By

Delta Technology & Management Services Pvt. Ltd

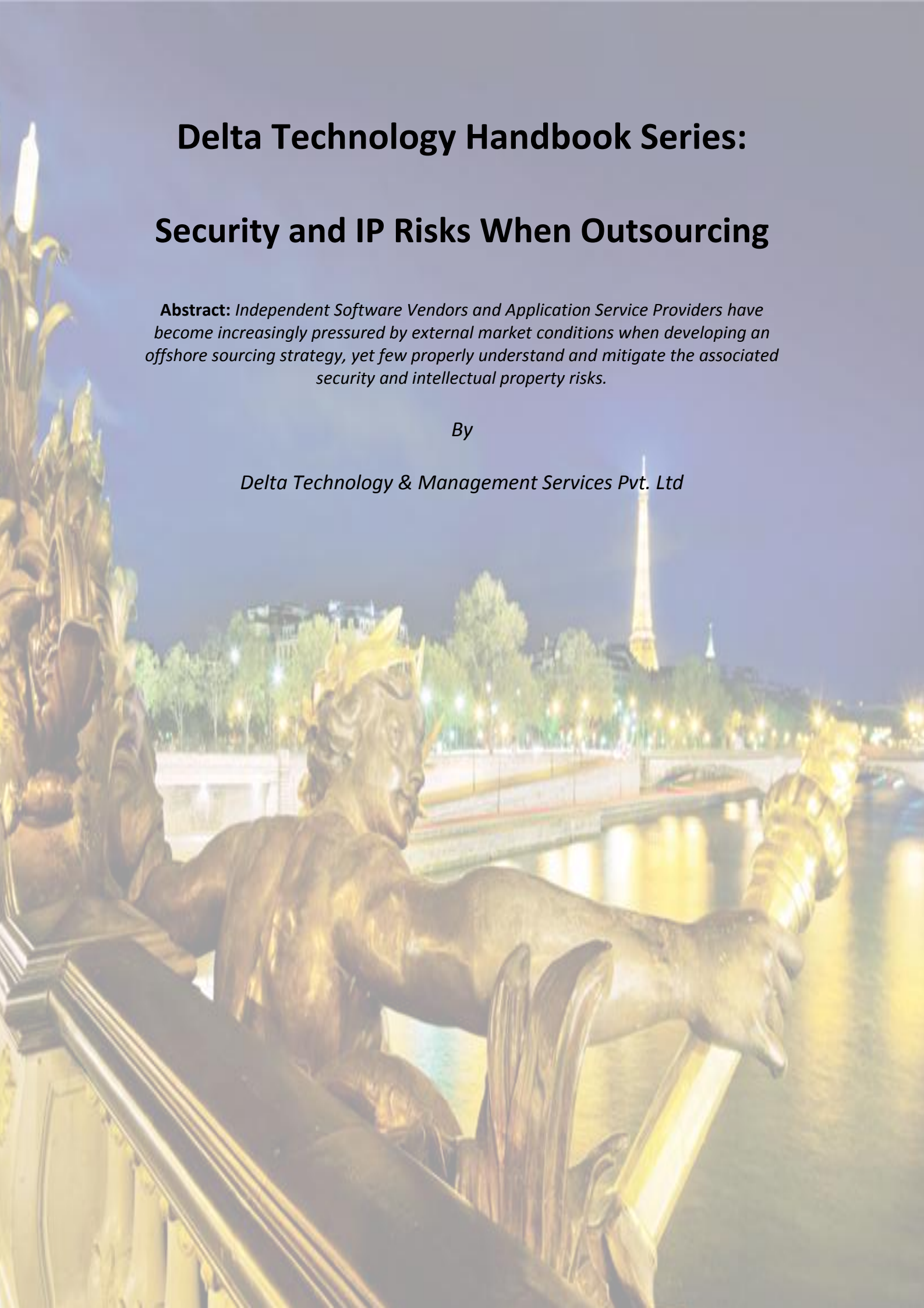


Table of Contents

1. Executive Summary

The success of Independent Software Vendors (ISVs) and Application Service Providers (ASPs) is dependent on their ability to:

- Bring innovate products and services to the market faster than their competitors;
- Supplement their development teams with the specialist skills and knowledge base that's needed to make things happen
- Re -balance their development priorities in order to accelerate revenue generation.

However, management and investors are under pressure to lower total cost of ownership and increase shareholder value. In addition, due to the standardization of software engineering processes, pricing pressure, margin compression and increased enterprise customer expectations (total cost of ownership and return on IT investment), software companies are faced with the task of developing increasingly complex products with limited and decreasing time frames.

Today, Independent Software Vendors and Application Service Providers are valued mostly for their intellectual property (IP) and in fact for many, their IP is much more valuable than any physical asset they hold.

Software companies derive more than 80% of their market value from intangible, digital assets and intellectual property. Yet, despite the advanced measures currently used by security conscious software companies, often they have no way of knowing if (and indeed when) intellectual property leaves their corporate networks.

The internet has destroyed everyone's ability of controlling information flow and this 'security perimeter' approach is no longer enough to guard against this leakage of intellectual property and other security violations. This is worrying because insiders are responsible for more than 80 % of all corporate security breaches today. Former Attorney General John Ashcroft estimated in October 2006 that intellectual property theft costs U.S. companies about $275 billion a year. Plus, the majority of intellectual property thefts occur through electronic media.

This is why it's vital for software companies who outsource their software development, maintenance and quality assurance, to assess how they can lessen the potential risks before they arise, as well as during and after the outsourcing relationship.

Other security factors to consider are that offshore development companies may carry risks because most vendors work for more than one client. Also, the physical security of the development center where the distributed team is located should be

given utmost importance when it comes to protecting intellectual property.

So with all these security issues to consider, what steps does a typical software company take in order to reduce the risk of security breaches and ensure the safety of their intellectual property?

This white paper discusses where the security and intellectual property risks and vulnerabilities exist in the distributed software development environments. It also addresses critical business issues where qualified risk management techniques can help to mitigate those identified risks, along with team collaboration tools, a verification and audit process resulting in greater visibility of the software development process and improved security. All of which will go towards reducing the risk of IP abuse and theft.

2. The Challenges Facing Independent Software Vendors and Application Service Providers

According to research carried out by McKinsey, in 2005 only 4–8% of large, offshore software engineering markets worldwide were associated with packaged software R&D - with most of that growth occurring in the last four to five years.

Increasingly, global outsourcing is becoming a viable option as the operational barriers and challenges normally associated with global outsourcing are gradually removed. Vendors are viewing outsourcing as a way to remain cost competitive. As a result, regardless of size and maturity, offshore outsourcing is becoming a pragmatic option for many different reasons and more and more, are hiring external vendors for their product development work.

This increasing reliance on IT outsourcing raises serious concerns about the theft of intellectual property as well as the very integrity of the source code being produced. Ironically, it's the countries with a history of intellectual property theft and those that ISVs and ASPs trust the least with their binary code are the places where software code development is being sent. And what is even more of a concern is that many of these countries have known terrorist networks and there is no way to ascertain the security risk of the workers used to produce software components for mission critical applications.

Currently, companies have inadequate safeguards or policies in place to deter or punish "insider" programmers who abuse the trust and privileges granted to them by intentionally harming source code. This threat to the source code has never been greater but the current level of awareness and priority given to this threat by organizations has not been given the seriousness it deserves. It should be a main

concern for companies today to expand security measures and this can be done by simply addressing system operational weaknesses and identifying where the vulnerabilities are when developing software.

From the points discussed, it is clear that security is a major concern when it comes to outsourcing.

Below are some practical steps that ISVs and ASPs can follow to protect their Intellectual Property and reduce risks while outsourcing software development offshore.

3. The Definition of Computer Security

Computer security is about protecting information against unauthorized access, modification, or destruction. It deals with the prevention and detection of illicit acts by users.

However, this definition implies an understanding of the value of the information to be safe guarded in order to develop protective measures.

In fact, strong measures can only be created from an understanding of how they can be compromised and they usually fall into the following categories:

- Confidentiality: Preventing unauthorized disclosure;
- Integrity: Preventing erroneous or malicious modifications;
- Availability: Preventing unauthorized withholding of information and resources.

The object of computer security is to protect valuable and sensitive organizational information from attacks while making it readily available to authorized users. Whilst the information revolution opened new avenues for IT, it also opened new possibilities for crime.

A rough classification of protective measures in computer security is as follows:

1. Prevention: Measures to prevent illicit damage, change or theft of information;

2. Detection: Measures to detect the who, when, and how of an information attack;

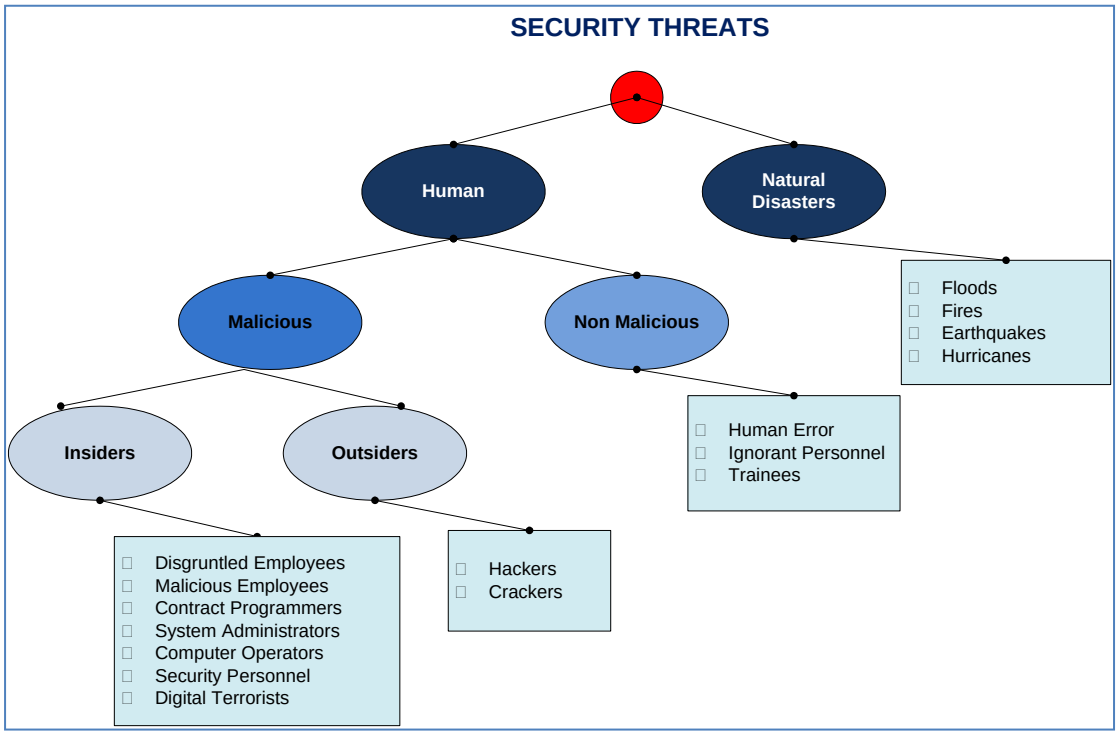
3. Reaction: Measures to allow recovery of original information;

4. Authentication: Verification of user identity;

5. Authorization: Validation of authorized access to sensitive systems.

4. The Nature of Security Threats

The diagram is a schematic of the types of security threats that exist.



5. Security within Business Categories

While planning, designing, executing and evaluating offshore outsourcing initiatives, software companies should consider the following attributes and business categories of security that cover both the internal and external environment:

- Intellectual Property Rights;
- Network Security;
- Physical Security;
- Information Protection;
- Personnel Security;
- Customer Privacy;
- Disaster Recovery;
- Business Continuity.

5.1. Intellectual Property Rights

This is one of the most critical concerns in an off-shoring scenario and to ensure any security measures put in place are effective, the facilities, assets, services, and personnel all have to be considered.

The four legally defined categories of intellectual property are:

1. **Patents**
When software organizations register their inventions with the government. This process can take more than a year until applicants gain the legal right to exclude anyone else from manufacturing or marketing it. Patents cover tangible things. They can also be registered in foreign countries, to help keep international competitors from finding out what your company is doing. Once you hold a patent, others can apply to license your product. Patents last for 20 years.

2. **Trademarks**
A trademark is a name, phrase, sound, or symbol used in association with services or products. It often connects a brand with a level of quality on which companies build a reputation. Trademark protection lasts for ten years after registration and, like patents, can be renewed. But trademarks don't have to be registered. If a company creates a symbol or name it wishes to use exclusively, it can simply attach the TM symbol. This effectively marks the territory and gives the company room to prosecute if other companies attempt to use the same symbol for their own purposes.

3. **Copyrights**
Copyright laws protect written or artistic expressions fixed in a tangible medium - novels, poems, songs, or movies. A copyright protects the expression of an idea, but not the idea itself. The owner of a copyrighted work has the right to reproduce it, to make derivative works from it (such as a movie based on a book), or to sell, perform, or display the work to the public. Businesses don't need to register their material to hold a copyright, but registration is a prerequisite if they decide to sue for copyright infringement. A copyright lasts for the life of the author plus another 50 years.

4. **Trade secrets.**
Formula, pattern, device, or compilation of data that grants the user an advantage over competitors is a trade secret. It is covered by state, rather than federal, law. To protect the secret, a business should prove that it adds value to the company - that it is, in fact, a secret - and that appropriate measures have been taken within the company to safeguard the secret, such as restricting knowledge to a select handful of executives. Coca-Cola, for example, has managed to keep its formula under wraps for more than 117 years.

IP protection can be achieved by using the following security controls, but companies also need to work with a local legal representative to ensure total protection.

- **Agreements** - should be structured through different levels of security confidentiality agreements both at organization and individual level.

- **Country Laws** - different government laws pertaining to IP, piracy, and copyright should be addressed. Companies should carefully evaluate the country's track record and compare the laws on the books with the actual implementation and enforcement of those laws.

- **Physical Security** - See the Physical Security section

- **Legal Compliance** - companies should structure the contract so the offshore supplier is liable for any breach of confidence.

- **Compliance with Security Standards** - companies need to ensure the compliance of the supplier organization with accepted
- International Security Standards like BS7799, ISO 17799, Safe Harbor, CoBIT etc.

- **Employee Contract** - companies should also specify in the contract that (supplier) employees cannot work for a competitor for a fixed duration after leaving the present company. They cannot divulge confidential data to competitors, press, or make other non approved disclosures.

- **Security Management Training** - the supplier should have a process in place for periodic Information Protection training for all offshore employees.

Contractual Security

When going offshore, there are several concerns that arise with regard to the legal considerations that cannot be avoided. Trade secrets are also a major concern to software companies, as competitors can easily embezzle them.

Hence, tight security measures should be employed in software development projects especially while going offshore. The following procedure explains in detail the measures to be taken to ensure that the offshore vendor provides enough contractual security.

Legal Bindings

The vendor should sign at least two agreements for the purpose of securing intellectual property.

1. Non-Disclosure Agreement;
2. Consulting Agreement.

Non-Disclosure Agreement

- NDA is an agreement stating the terms of confidentiality, which should be signed by the vendor at the time of discussing the project feasibilities;

- The offshore vendor should sign a Non-Disclosure Agreement (NDA) to assure confidentiality of information even before signing the contract;

- Companies should ensure that the NDA provided by the vendor states what exactly the vendor means by confidential;

- The NDA should clearly express how the vendor will ensure the confidentiality of your information. For example, the NDA should state one or more of the following points in the agreement to ensure confidentiality:

- Shall not remove any proprietary or other legends or restrictive notices contained or included in any confidential information provided by Company;

- Shall not copy any confidential information;

- Shall not disclose any confidential information to a third party without the prior written consent of the Company hereto;

- Agrees to keep secure and maintain the confidential information of Company in a manner no less protective than that used to maintain the confidentiality of Recipient's own confidential information, but in any event not less than a reasonable degree of care; and agrees to use the confidential information only for the purpose of this agreement.

- All employees of an offshore vendor should also sign a similar NDA with their company when they join. This also ensures that any customer data is confidential. Thus proprietary information stays with the best possible IP protection methods.

Consulting Agreement

- The offshore vendor should sign a consulting agreement at the time of entering into a partnership. This agreement should cover all IP-related issues;

- The contract should capture and secure all prices, costs, and other business benefits sought;

- The contract agreement should also state the definition of confidential information and what it includes. For example, confidential information can include any one or more of the following:

- Proprietary computer software, programs, applications, and processes, including documentation, trademarks, or service marks;

- In-house personnel, financial, marketing, and other business information, and manner and method of conducting business;

- Strategic, operational, and other business plans and forecasts;

- Information provided by/regarding in-house employees, customers, vendors, and other contractors;

- The ownership right for the software that is developed by the offshore vendor should remain your property and the offshore vendor should not own any right for the intellectual property of the development work;

- The vendor should agree that any and all work produced that becomes copyrighted, or that may be the subject of an application for copyright protection, will be considered a work made for hire;

- Contractual relationships should include provisions for inflation, taxation, and changes in corporate structure. Finally, the companies need to plan for the end of outsourcing/vendor relationships.

Enforceability of agreements

Although intellectual property and commercial law are practiced throughout the world, software companies should seek relationships with U.S. entities that have real U.S. assets. Companies should consider provisions for alternative dispute resolution such as arbitration and mediation as well.

Trade secrets

Trade secrets are kept as secrets through the law of confidentiality. Software companies should ensure that all those who are given access to their confidential data at the offshore location understand the conditions of confidentiality and are bound by them.

5.2. Network Security

The majority of the violations in Intellectual property rights occur through electronic media. Most vendors work for more than one client and thus the offshore development center cannot be expected to be a dedicated facility for a particular client alone.

Also, the offshore development center (ODC) is usually connected to the client's systems through International private leased line circuit (IPLC) or a virtual private network (VPN) through the Internet. It is very important that the functioning of networks at the offshore location is closely examined to ensure that the network links are secure and less vulnerable to access by unscrupulous personnel.

A good infrastructure is the basic requirement for successful execution of the project. It addresses the responsibilities of suppliers for establishing, maintaining, implementing, administering and interpreting organization-wide network security policies, standards, guidelines and procedures.

- **Dedicated Infrastructure** - suppliers should use customer-dedicated racks for housing servers, routers, switches, and firewall products;

- **Network Security** - the supplier system administrator will be responsible for performing network security risk assessments, preparing network security action plans, evaluating network security products and performing other activities necessary to assure a secure network environment;

- **Network Device Security** - a high-level of security for network devices is necessary to prevent unauthorized access. The following steps can be undertaken to ensure network security at the vendor's premises.

Security for Network links

- The vendor's network should be protected by a firewall and only authorized IPs should be allowed to access the systems at the ODC after proper verification and authentication;

- The user name and password used to access the systems at the ODC should be changed periodically to avoid hacking;

- The ODC's servers should be monitored periodically for any form of unauthorized access.

Security and access to customer's proprietary data

- It is preferable that the vendor follows a formal procedure for requesting access to the network. The request should be originated by the Project Manager stating the users who are allowed to access the network;

- The system administrator should ensure that the security guidelines stipulated by the client are ensured at all times;

- The vendor should have secure methods for information transfer between the ODC and the client/onsite team;

- When data transmission is done over the Internet, it is a must to ensure that data is encrypted and sent through a VPN tunnel.

Code Security

- Important information such as source code should be well protected with passwords and access codes and should be made available only to the members working on that project;

- Proper version control procedures should be deployed to keep track of the changes done in the code;

- The code should be backed up using an appropriate media and erased from development, test and deployment servers after completion of the project;

- Backed-up data should be kept in a secure access area in the ODC as well as in a well-defined offsite storage area to protect from natural disasters.

5.3. Physical Security

Physical security of the development center is of the utmost importance when it comes to protecting intellectual property. Determining the flow of information into, through and out of a vendor's company should be considered. Protection against the physical threats that can jeopardize the infrastructure assets of vendors should also be considered.

These are some typical best practices to ensure physical security:

Access Control - access control ensures only authorized personnel enter client-servicing areas. Round-the-clock security presence with:

- Photo ID cards;
- Access controlled by swipe-card system with different levels of access. Biometric access if necessary. 24/7 operations require a higher degree of security measures. Any employee, who forgets to carry the ID card, has to sign in at the reception desk and wait for a supervisor to identify and escort him/her inside;
- Entry/exit tracking system should monitor movement on each floor and each individual room;
- All visitors should register at the Security Office, sign and obtain a temporary ID badge. Their movement within the facility should be restricted and an authorized company employee should escort them;
- Critical facilities are secured with electronic lock devices;
- All important/confidential information is kept secure in lockable file storage systems.

Limited Access - employee access is restricted to their areas of work.

Access by other supplier personnel is denied to the client's floor - isolated from the supplier LAN.

Dedicated Facility/Work Area - physical security of facilities is managed through dedicated floors. If this is not required, then logical isolation is sufficient to prevent inappropriate and unauthenticated access.

Camera Surveillance - round-the-clock surveillance to monitor any breach of security

Movement Restriction - no printouts, photocopies, computer media, or computing devices are allowed to enter or leave the floor. All housekeeping staff will clean the floor under the direct supervision of a Supervisor for the shift.

Separate Meeting Rooms - provision for separate meeting rooms to facilitate interaction with team members, vendors and other external personnel.

Recreation Facilities - separate recreation area.

Fire Safety - fire alarms, electronic-grade fire-fighting equipment, emergency measures. Fire drills, regular upkeep of fire equipment and fire insurance policies should not be taken for granted in offshore supplier agreements.

The following steps can be undertaken to ensure physical security at vendor's premises:

Work area security

- Round-the-clock security should be provided for the work premises;
- It is a must for a company to know and monitor the physical movements of its employees. Ideally, surveillance cameras should be used for this purpose;
- Entry to the development premises should be restricted with the help of access cards. It is recommended that technology using fingerprint or facial recognition, in combination with access cards, are deployed;
- Developers belonging to different projects should be grouped into different bays/cabins;
- It would be nice to have a separate, locked work area for customer's team.

Procedures for storing and protecting printed project materials and files

- All the printed materials and files should be catalogued and stored in a location protected by lock-and-key system;
- Every employee should be provided with a cabinet where all details/paperwork related to the project can be stored. It should be ensured that the employees lock their cabinets for safekeeping before they leave their workplace;
- The Project Manager should be responsible for storing and locking all the materials after their usage and accessibility should be given only to the authorized personnel. She/he should also ensure that the place is protected from fire, rodents, insects, etc.

Authorization levels or mechanisms to control access to customer's development tools and proprietary information

- The Project Manager should authorize only a select few members of the project for accessing development tools and other proprietary information;
- Other members should not be authorized to have access to complete information about the project/engagement. In case of any information requirement, they should approach the authorized team member who will provide the needed information.

5.4. Information Protection

Offshore supplier organizations generally use different information protection methods for different clients based on the business needs of the engagement. An Information Protection Agreement is a “must have” and should cover the basic areas mentioned below in detail.

Vulnerability Assessment - is the analysis of information assets within an organization to determine their sensitivity to outages. This includes identifying technical and non-technical weaknesses that may impact the secure environment.

Technical Criticalities - use of IPS / IDS scanner tools to identify and document the technical weakness of the IT systems.

Non-Technical Weaknesses - interview custodians of information assets for non-technical and process weaknesses and document the same.

Data Access - in order to protect important and confidential data, information should be exchanged strictly on a need-to-know basis. Monitor and restrict access to source data. All workstations should have disabled CD and floppy drives to disallow any wrongful data transfer. All team managers and associates should have secure workspaces including secure lockers.

Note: In general, personnel/customer/sensitive data should not reside in the offshore location. However, for faster execution of work, a working copy with specific information can be made available to offshore employees. Information Protection can still be ensured through various means such as encrypting the data, creating "test" data with all the sensitive fields randomized or deleted, etc.

Data Audits - perform data security audits and report test results. Several types of audits common in offshoring exist, including periodic audits, surveillance audits, penetration testing, etc. Clients can hire an independent local third party to audit and certify compliance.

Data Security - appropriate access control procedures should be established, which include logging individual access/actions. Use of firewalls is critical for segmenting and protecting information and limiting access.

5.5. Personnel Security

Companies currently have inadequate safeguards in place to deter “insider” programmers who abuse the trust and privileges granted to them, from intentionally harming source code with almost total impunity. The threat to the source code has

never been greater - the current level of awareness by organizations is not commensurate to that threat. It is the critical priority for companies today to expand security measures from simply addressing system operational weaknesses to include unprotected software developmental vulnerabilities.

Personnel security addresses the potential risk from current and past employees and factors to mitigate the risk. Diligence in this area is as appropriate as in onshore engagements. Government rules and regulations in different geographies also play a major role.

For example: The level of detail allowed under US law while conducting background checks is significantly different from that of Indian, Philippine, or Russian laws. What could be considered a breach of personal privacy in one country could be viewed more tolerantly elsewhere.

Background Checks - companies should conduct detailed background checks for all employees working with sensitive information based on client requests. Some best practices include:

- **Routine Checks**: Verification of educational qualifications and reference checks of fresh candidates by HR;

- **Reference Checks**: For all the employees with prior experience, reference checks with previous employers;

- **Integrity Checks**: An external intelligence agency is employed to do a thorough background integrity check for those employees who would be handling sensitive data. The parameters for these types of checks could include family background, personal character, social status, and criminal records;

- **Special Checks**: Specific checks like drug screening are carried out in accordance with the client's criteria and business needs.

Non-Disclosure/Confidentiality Agreements should be mandatory for all employees to sign in a standard format.

Hardware Limitations - suppliers do not have access to the CD drives or master application. Read, write, use, and modify access can be granted according to the specific function of the employee/team.

Internet Usage - access to the Internet is locked to the specific applications the employee uses. Some kind of Internet monitor tool/mechanism can also be used.

Usage of Mobile Commuting- restricted usage. Not allowed in the actual work area.

Housekeeping - all housekeeping staff are required to work only under the supervision of the Shift Manager/Supervisor.

5.6. Customer Privacy

In the course of conducting business, companies collect and process personally identifiable information of their clients, suppliers, business partners, shareholders, employees and other persons. This is commonly known as Personal Data and Information and can be used directly or indirectly to identify a living individual.

When the Personal Data and Information includes sensitive categories of information, such as information that reveals racial or political opinions, ethnic origin, religious beliefs, trade union membership, health or sexual orientation. This type of information is categorized as Sensitive Personal Data and Information.

Maintaining the integrity and confidentiality of Personal Data and Information, and handling it correctly is important. The privacy policy/agreement should be in place between client and service provider and should describe how the outsourcer and its employees should handle Personal Data and Information.

5.7. Disaster Recovery

Backups - tape backups should be taken at pre-specified schedules as specified in the company security guidelines or per the need of the client.

The backups could be full backups at specific periods or daily incremental backups. Routinely, it is a combination of the two.

The backup tapes have a unique number for easy identification.

The tapes are stored as archives in off-site locations as part of disaster recovery plans.

Note: It is important to have scheduled backups not only for data residing within the organization but also for data that is being carried around. For example: Data residing within laptops of various key people in the organization

Data Recovery - provision of adequate tools to recover data quickly.

Non-storage of production code/data in an offshore location - all sensitive data

should reside on a dedicated server at the client site. However, all project management records, quality tracking documents, project related documents, source code, dummy development/working environment, should reside on the local server at the offshore facility and should have a backup and recovery policy. Periodic testing and verification of the test results ensures compliance.

Disposal of sensitive data - sensitive data should be disposed of using a shredder on a daily basis.

5.8. Business Continuity

Before building a Disaster Recovery and Business Continuity Plan, companies should perform an objective risk assessment to identify business-critical applications and/or processes. Once potential risks are defined assigning accountability is crucial. Determine 'what is the expected degree of assurance' and 'what level of backup is required' as these points will decide the required number of resources and associated costs. Ensure implementation of the policy by a combination of preventive measures and technical controls.

The Disaster Recovery and Business Continuity Plan should cover these areas:

Risk assessment - identify the areas of offshore risk.
Keep in mind that some risks are geography-specific. The recent SARS epidemic in Singapore, Hong Kong, and China is an example of this type of risk. Other examples include: civil disorders, outbreak of war, breakdown of public services (basic amenities like water, electricity, and roads/access) are a few. A key component of the assessment is to determine the maximum allowable downtime.

Restoration process - outline, in the event of a disaster, how quickly the services can be restored. Identify the minimum and maximum time schedule for restoration of basic services versus full services.

Testing of Back-up Systems - regular testing of back up arrangements should be organized to ensure they meet the requirements of the Business Continuity Plans.

Audits - develop an audit calendar to verify the accuracy of data and process restoration.

On-going monitoring - indicate a schedule for plan reviews (quarterly, bi-annual, annually). Plan to also monitor compliance and preparedness through mock disaster recovery drills. Be sure to reform the plan as needs change.

Managing the alternate site - identify levels of disaster and plan for backup sites. Include one alternate site for low-level disaster and another secondary site for a

higher level of contingency.

Key resources - planning for movement of key resources/personnel is crucial. One best practice is to have two sets of equally prepared teams located in two different geographical areas to dilute the risk.

Post Disaster Communication - outline a communication plan that includes who to contact and the plan of action in the event of an emergency. This plan should also include details for any external communication.

6. Role of a Security Organization (SO)

Even with the adoption of a strong information protection policy, network security architecture and a good disaster recovery and business continuity plan, it is prudent to use third party assessments to ensure that the policies and processes are being used correctly.

To ensure compliance, it is suggested that two assessors should be appointed ie an offshore assessor who can perform periodic audits and carry out ongoing monitoring and one based locally who performs the role of the Security Organization .

The primary objective of a Security Organization is to ensure a secure work environment. Whether the offshore presence is with a third-party or an expatriate from the client organization, responsibilities should include:

- Conduct 'Information Risk Assessments' on prospective supplier organizations;
- Develop, monitor, and review information protection and security policies;
- Ensure compliance;
- Monitor security risks and threats;
- Determine responsibilities of key individuals;
- Approve and support the implementation of Information Security Management System and information security initiatives;
- Review security incidents through reports presented by the SO covering status of security implementation, update on threats, results of security reviews, audits etc;

- Security coordination within company and with external regulatory authorities

7. Best Practices

Before signing the contract

- It is preferred that companies inspect in person the physical premises where the software is to be developed. This is an opportunity to check the security firewalls of your vendor's buildings and work area, the organization culture, the functioning of their networks, etc;

- It is preferable that companies interview the team members who will work on your project. This will help you to judge the level of reliability on the employees;

- Companies should also check the offshore development company's employee retention rate and also if the outsourcee is working with any competing organizations. If such is the case, companies should ensure that the teams working on their competitors' projects do not have access to their project information;

- Any method of information transfer such as e-mails, fax, electronic file exchange, instant messenger, on-line meetings, paper documentation etc, should have their parameters for usage defined;

- All activities that will have to accompany the end/termination of the contract should be defined while negotiating the contract terms and conditions. This includes the retrieval of any methods and procedures, documents, source and executable code, company proprietary security or development standards, code libraries, and data stored offsite;

- Contracts should be set up such that the offshore company takes responsibility for the actions of its employees;

- Companies should ensure that any project-related work is not subcontracted without approval. This will help in protecting a sensitive application or data within the application;

- Companies should ensure that the vendor agrees not to use any of the company's confidential information for purposes like sales, marketing, or demo without prior approval.

After signing the contract

- Companies should ensure that only data related to the performance and reliability of the system is transmitted over the Internet. Information from the database should not be disturbed during any part of the project;

- Companies should make sure that the system experts make modifications to the system only after obtaining prior permission;

- Exchange of passwords and other critical information should be made secure by encrypting them;

- Companies should ensure that the data used during testing does not expose the real information of the customers;

- Unwanted data should be destroyed;

- Companies should ensure that the vendor will report any change in the project team;

- Companies should ensure that an original copy of the source code is maintained.

8. References

1. “Computer Security,” Dieter Gollman, 2005, 1999
2. Why Software is So Bad, and What To Do About It, MIT Technology Review, June 2002
3. “Department of Defence Trusted Computer System Evaluation Criteria,” (Orange Book) NCSC, 1983
4. “Security Threats.” www.microsoft.comtechnet/security
5. The Business Risk of Offshore Outsourcing Jag Dalal Neil Hirshman, Doug Dickey,
6. “Process Maturity Profiles of The Software Industry,” Software Engineering Institute, August 2000
7. “No silver Bullets: Essence and Accidents of Software Engineering,” Frank P. Brooks, 1987
8. 47% of the H1B visa quota went to foreign computer programmers, U.S. Labor Department, 1998
9. Cochran, S., “The Rising Cost of Software Complexity”, Dr. Dobb’s Journal, April 2001, pg. S14.
10. United Nations Commission on Crime and Criminal Justice Survey 1998
11. Computer Security Institute/FBI Computer Crime & Security Survey, 1998