Global Information Assurance Certification Paper

Identifying and Mitigating Risks Of Information Technology Outsourcing

William T Tucek

October 7th 2002

GSEC option 1, version 1.4b

ABSTRACT

Outsourcing of goods and services is commonplace throughout the Information Technology industry for reasons that are motivated by several business factors. But what are the potential impacts to security, confidentiality and integrity of the data, not to mention the business itself?

This paper will guide the reader on methods on how to identify risks with proposed outsourced agreements - primarily with application service providers, work to reduce exposure, increase accountability and advise business decision makers of the potential consequences of the vendor selection.

Introduction to Outsourcing

Outsourcing is the use of resources external to the company or organization, which may have been previously handled internally by staff. Outsourcing of Information Technology can take shape in many forms and include a wide variety of services and support functions. Some of the most common forms of outsourcing include network hosting, source code development, and application service providers. Typically, it is support functions, which are preferential candidates for this type of business solution. Core competencies, typically should not be outsourced. [1]

Outsourcing, when executed correctly can provide many benefits to the Information Technology organization. The reasons to outsource include reduced costs, improved performance, increased business competitiveness, access to a superior knowledge base and limited in-house staff to support the business needs.

Vendors of outsourcing solutions come in a wide variety of forms and options. These can include short and long term agreements, different levels of service, everything from a basic solution to strategic alliances. Vendors also vary in location; both domestic and International opportunities exist. Due to the very nature of information technology it is possible to select a vendor worldwide thanks to high-speed networks.

With many options for an organization it is understandable why the popularity of outsourcing is strong in today's business climate. According to a recent Gartner survey from early 2002, most companies outsourcing IT services overseas will continue to do so.[2]

However with the opportunity also comes a degree of risk and uncertainty, which could potentially impact the organizations ability to function, do business or lose market share.

Some Commons Business Risks of Outsourcing

Listed below are some common business risks as a security professional you should be aware of: [3]

The Vendor Risks:

- Weak vendor staffing - Inadequate level of staffing to perform the required tasks for the contract and also the other customers.
- Weak Vendor management - The Vendor does not have experienced and adequate management to oversee your business.
- Lack of innovation and capacity planning by the vendor - Lack of technical ability and foresight to keep the product or service being utilized at an adequate competitive level.
- Methods and tools, which are primitive - The vendor simply has inadequate tools that are not up to standard with expectable levels within the industry.

The Client Risks:

- Over reliance on the vendor, or one vendor in particular
- Little or no benchmarks or defined metrics of the vendors work
- Little or poor oversight of the vendor

Potential Security Specific Risks of Outsourcing

The potential of security risk varies with each outsourcing agreement. The contract and more specifically, the statement of work, contains the finer details of the agreement where security concerns should be identified.

The biggest potential for risk and an innate factor with outsourcing, is the act of giving a third party, the outsource vendor, access to your organizations information. This information can include confidential information such as financial, medical information, records and strategic development. Along with the access, is the possibility of unwanted disclosure alteration or destruction of the information. The possible impact here to the organization is loss of reputation, competitive edge and legal risks. [4]

Arrangement specific risks: Code and program development, application Service providers and Internet service providers are Risks for vendors involved in code development and program design can include the following: [5]

- Installing trap doors within the software
- Taking system root
- Implanting malicious code

Some Risks for application service providers can include can include the following:

- Poorly coded applications: Access of data by other customers due to poor security features of the application
- Inadequate security policies
- Inability to enforce security policies
- Lack of incident response and disaster recovery plans
- Inadequate access control to data from the vendors employees [6]

In addition, risks associated with hosting centers and services that sometimes allow for remote access into the client networks by the vendor. Remote connections are usually established to handle large data transfer or remote administration. A VPN or other secure channels may be established into the clients network in order to secure data transfer. However what risk does this type of network egress between the client and vendor pose? Not to mention additional overhead to manage and monitor.

There are many examples of security issues in recent years, which had occurred during outsourcing arrangements with less than reputable vendors. In some cases, even with reliable vendors, the vendor's employees acted inappropriately in the handling of the data entrusted to them.

A F.B.I case as recently as August 25th 2002 illustrates this type of risk. In an overseas outsource venture for the purposes of debugging source code. An American company was the apparently the target of an intellectual property theft scheme when the vendors employee attempted to sell the source code to a competitor which reported it to the F.B.I. [7]

This type of case also sheds light on other potential risks, such as difficulties in dealing with different legal systems, different attititudes towards intellectual property and the ability or priority of the foreign hosts law enforcement agencies to assist in these types of issues should the risk become reality.

Identifying the Security Risks - Overview

The potential impacts to security with an outsourcing agreement depend upon the details of the arrangement. The primary question that must be asked by the security professional is; "what are threats, what is the impact of the threat and what is the frequency of the threat"? [8]

Some risks are easily identifiable, other may not be so apparent or even worse are later discovered after contractual agreements have been made. A great tool for identifying risk is to refer to the contract itself. The statement of work should give clear and conscience language of what actions is necessary and permitted by the vendor. The Service Level agreement defines the acceptable levels of the activity.

Identifying the Security Risks – Methods

For new outsourcing ventures, identifying security risks may be a bit more easily identifiable than current arrangements. This of course also depends on the level of involvement of the Security and or Risk Management department within your organization in the review of outsourcing arraignment.

There are several methods to identify the Risk involved, the outsourcing proposal review can include all or part of the following:

Site Visit: Visit the vendor's site; validate the vendor's proposal and ability to comply with the terms of the contract

Remote Security Testing: Should the vendor agree and it is included in the terms of a contract, Security testing can identify flaws quickly to the proposal. This can include application scanning, penetration testing and ethical hacking.

Vendor self-assessment: Not designed for use as the sole method in the identification of security issues, Self-assessment should be conducted in order to enhance the review process.

Identifying the Security Risks – Key areas to review with the vendor [9]

1. Security Policy and Communication:

   An important cornerstone of security is policy and communication of policy. It is pertinent that the vendor does in fact have a security policy, one that has been written and endorsed by its senior management. The security policy should address not only the policy for the service that the vendor is providing but also other aspects of the companies IT resources.

   It is also important to know if these policies have been communicated to the employees of the vendor and if so in what method and how frequently. Also how often are this polices being updated or refreshed?

   The potential impact to security due to the lack of an adequate security policy is great for you if your vendor does not have a specific policy. Security

professions should verify, if the opportunity exists that the vendor does have adequate security policies, process and procedures in place.

2. Security Administration:

Another cornerstone of security is the administration of these polices and procedures which have been established. The question is how this function being executed and to what extent. There are several factors, which need to be determined. It should be established that the vendor has an adequate number of trained staff to perform the responsibility of security administration.

Other factors include the processes for identification, authentication, access control, and authorization of requests for access and monitoring and logging of events regarding these items.

3. Vendor Personnel Practices:

Just as important as all the hardware and software involved in the safeguarding of the venture, an often-overlooked aspect of the outsourcing agreement is the vendor's personnel practices. Since people are often the weakest link in the security chain, it is important to ensure that the selected vendor has polices and procedures in place to ensure that your information will be safeguarded while it are in the trust of the vendor. The vendor should ensure that they have processes in place that their employees or contract staff is trustworthy. It is not unreasonable to ask the vendor if background checks are performed on staff.

In addition, vendors should provide examples of code of conduct statements and any vendor staff that has the potential ability to negatively impacting the organization by disclosing information and should sign non-disclosure agreements.

4. IT Operations and Business processes:

Equally important to Security and needed for a stable IT environment, a clear business process is needed in order to address changes in the environment. Depending on the type of service - application service providers, hosting providers and other service providers, reasonable assurance to ensure that adequate process exist.

Change management is an example of a type of important business process and procedure for making changes in an active environment. The vendor should ensure that changes made to production applications are not performed without careful review. This also can include process for the notification of the end users or customers if warranted. Change management is also important to security when investigating security incidences.

Other important operations processes can include the oversight and approval process of changes to firewall rules, which may have to be changed to accommodate application or customer needs. Diligence should be made to ensure that the vendor if hosting an application provides process around the management of firewall rules.

5. Physical Security:

It is often said in the security industry that without physical security there is no security. Although a vendor may claim that there computer hardware is housed in state of the art controlled hosting environments, it would be advisable to verify the vendors claims. If the potential exists to visit the vendor's facility where the computing environment is located it would be wise to request a visit to inspect the facility. Some items, which should be considered during the evaluation, are: access control, segregation of equipment – cages and vaults in larger collocation facilities and surveillance cameras.

Other considerations when reviewing the site can include plans for Disaster Recovery, typically a facility should offer environmental controls, which can include: Temperature and humidity controls, redundant Power supplies, leak detection and a review of redundant telephone connections.

6. Operating System Security:

A concrete foundation of the application or service that the outsource vendor is offering is more than likely residing on an operating system of some kind. The vendor should have substantiated practices for securing these platforms, which are documented and adhered by. As a customer of the vendor, what you would not want to experience is a vulnerability, which allows the attacker to gain access to your organizations data. Items, which you would want to verify with the vendor, are: Documented procedures for operating system builds and methods to verify the operating systems adhere to the guidelines should exist.

7. Application or Service Security:

For customers of an application service provider, the security features of the application should be of importance since this is more than likely the most accessible part of the application. Some areas of concern and suggestions for review would include the following areas: Authentication methods, Access control, Data Integrity and Security Administration.

Authentication methods: Good security controls, which should be available, include: encrypted password features, password expirations, strength, inactivity timeouts and unsuccessful logins parameters.

Access control: Some features should be included in the application are: file and directory level access. Definition of roles or groups for accounts should be clear.

Data Integrity: These features help ensure the reliability of the data, these include verification that input matches the correct criteria, timeout values for input and exception reports for data which is attempted outside of the acceptable levels.

Security Administration: These consist of the procedures that are used to maintain access to the data such as the authoring of approvals and re certification of users. These processes should be well documented, other items that would be included are logging of access to the application and security auditing of access.

8. Network and hosting Security:

Network security is an integral part of protecting any IT environment. Outsourcing IT duties with an application service provider is no exception. The vendor should be able to provide reasonable assurance that network security has been addressed. Some of the items, which should be verified as part of a due diligence, include the existence of the vendors understanding of their own environment by requesting a copy of the logical network. Other areas include verification of number and placement of firewalls, including the rulsets and allowable protocols. Intrusion detections systems, if available should be verified for administration methods such as how logs are reviewed and alerts investigated and responded to. Finally, does the architecture support a reasonable security in its design by implementing multiple tiers to limit unauthorized access?

9. Disaster Recovery and Business continuity:

Just as your organization should have adequate disaster recovery procedures in place for valued IT systems, so should the vendor providing services to your organization. These plans should ensure an adequate plan and recovery times. Some issues to verify with the vendor are: Verification that a recovery plans exists for the services being purchased, availability of an offsite location to recover applications, finally verification that the plan been tested and results documented.

10. Audit and reviews – Internal and 3rd Party:

Finally, as a customer it is of value to know if the vendor which your organization is currently doing or considering doing business with has a structured audit program. These can include both internal and external audits and reviews. This is important because as a customer, verification of controls and security measures marketed by the vendor should have a level of credibility that controls exist. A third party review or Audit typically gives a less biased view.

Examples of external reviews with can include SAS70 type II and an ISO 17799 type, which are performed by third party. Internal audit reviews, performed by the vendor's staff should not be considered equal to the external review, as internal pressures may possibly sway the review results. This is not to say that the vendors audit staff does not provide value, but as a customer the audit results, if even available may prove to be less objective than that of a third party. The bottom line is the buyers beware, a vendor that does not or have an audit program should be carefully considered.

Mitigating Security Risks:

Many of the risks with an outsourcing arrangement may be apparent to security professionals, but not necessarily the dealmakers within the organization who are seeking to obtain the services of a vendor. There are several steps that can be taken to mitigate these risks, however keep in mind that it is important to understand the role of security within your own organization first. If your organization does not consider security an important area within its organization, then arguments concerning security risk may go unheard. Hopefully, this will not be the case and your organization will understands the value and benefits of information security.

Some of the methods of mitigating security risk, which should be considered, are suggested below.

Involvement in IT projects and outsourcing:

Internal communications and participation of security in IT is an important first step of understanding how the technology environment may be changing. If your organization involves Information security staff in the process of vendor selection, preferably prior to any final agreements, then the ability to improve security can be more easily made.

In addition to security other departments should be involved as well during the selection process such as legal, business and technical units to achieve a cross relational view of the outsourcing engagement.

Choosing the right vendor:

In addition to being involved another way to mitigate security risk is to offering to review the vendor when the organization is in the selection phase, this can be in the form of a due diligence. From a business perspective it is important to understand how a security risk could outweigh the benefits of outsourcing. Security staff should be able to translate the technical risks into an impact analysis or risk factor for the management of the organization in order to better understand the current or proposed outsource arraignment

Clear and concise Legal definitions:

The contract with the vendor should be clear as to services being provided. The statement of work should include security needs of the arraignment and the service level agreement should define the expectable levels of security. For example thresholds for notification of suspected attacks at the vendors site impacting the organizations data. The ability to perform further reviews such as audits should be included in outsourcing arraignment agreement also for periodic reviews.[10]

Oversight and Management:

Both Short term (transition) and long term management of the vendor should be detailed within the organization. This includes clearly defined roles, responsibilities, oversight and reporting (metrics) of the vendor's performance to management. Periodic reviews should be conducted of the vendor's performance including impacts on security or business recovery.

Contingency plan:

Simply put, have an escape route should the vendor not be able to fulfill its obligations. It is advisable to create and document plans for an unplanned exit from the vendor. Careful consideration to securing and recovering data should be thought out. Also recreation of the environment including security features should be well documented.

Conclusion

During the course of this paper we have learned of the benefits of Outsourcing and the potential for some very real risks, which can have direct impact to Information security. Organizations who are actively or planning to partake in outsourcing should examine closely methods to identify risk and if possible, mitigate those risks.

References

[1] Hughes Software Systems, Outsourcing, a Decision of Trust, 04/2002
http://www.hssworld.com/whitepapers/whitepaper_pdf/Outsourcing_trust.pdf

[2] Gartner Research, Press Release 09/09/2002
http://www4.gartner.com/5_about/press_releases/2002_09/pr20020909a.jsp

[3] Navisource Consulting, Outsourcing Primer, 09/24/2002
http://www.navcon.net/Outsourcing%20Primer.pdf

[4] Federal Reserve Bank of New York, Outsourcing Financial Services Activities, 10/1999
http://www.ny.frb.org/bankinfo/circular/outsource.pdf

[5] Bruck & Associates, Year 2000 Computer Remediation: Assessing Risk Levels in Foreign Outsourcing, 2001
http://www.bruck-inc.com/security/news/newsfiles/y2krem.htm

[6] Jerboa Inc., Ten Things to Ask you ASP, 2001
http://www.jerboa.com/whitepapers/tenthings.pdf

[7] F.B.I. New Era of Cybercrime Cooperation, 08/2002
http://www.fbi.gov/page2/bosind.htm

[8] The SANS Institute, Security Essentials, Risk Management and Auditing, 2000

[9] CERT® Security Improvement Modules, 06/2002
http://www.cert.org/security-improvement/

[10] Baker Robbins Company, Articulating a Litigation Outsourcing Strategy, 10/1998
http://www.brco.com/articles_details.asp?id=4