Global Information Assurance Certification Paper

How to improve security by contracting security outsourcing

Maria Jose Caballero Molina

GSEC V1.4.b option 1

17 Nov 2003

Abstract

There is an increasing number of articles and internet forums against outsourcing security and contracting Managed Security Services. In this type of articles and forums, outsourcing providers professionals are presented as a security threat to their customers.(An extreme example of this can be seen at Cio.com Forum (6)). The aim of this paper is to show customers the possible advantages of contracting outsourcing, not only in traditional areas but also in security, from the point of view of a worker at a outsourcing services provider. Security workers at outsourcers are IT security professionals and the only difference with other security colleagues is that “our” machines are providing services to our customers’ enterprises instead (really besides) to our own enterprise.

From model indicated at SANS Security Essentials (1), we will see how Operations Security Program, Defence in-depth and Security Policies can be improved due to a collaborative relationship between customer and outsourcer. All depends on how customer faces outsourcing, signed contract and rely on outsourcer.

Table of Contents

Introduction

Nowadays, there are many customers who are afraid of contracting security outsourcing and other customers who having outsourced their I/T Services have preferred to keep all or part of the security responsibility on their own and are experiencing security problems.
At the same time, several studies from prestigious firms like Gartner or Datamonitor present outsourcing security as a good solution to actual security weakness at enterprises, mainly at SMB's. (2, Wearden;3,Jacques;4,Brietling)

We should then ask ourselves, which are reasons that block security outsourcing and share security management with an experienced security outsourcer.

According to several authors (and my own experience) lack of trust on outsourcer is the main reason meanwhile fear to lose control over both core data and technology protecting core data, is the second.

> Two fundamental problems are routinely perceived to stand in the way of successful contractual relationships. The first is trust … The problem of trust arises because, to the extent that the objectives of the contracting parties differ, the fear of opportunistic behaviour or down-right non-cooperation may seem justified. It may also appear sufficiently risky to make in-house provision the only safe option.
> The second problem is control. When a contractor undertakes an activity which is part of the purchasing organization's value chain, control over the human and physical resources rests with the provider and not with the purchaser. Control over performance can be exercised through the provisions of the contract, monitoring, and levying of penalties, but that generally precludes having direct access to, and influence over, the contractor's resources. It is this latter aspect that creates concerns over potential loss of control: many client organizations, particularly in the public sector, believe that unless they have direct control over the inputs required for the production, they have little if any control over the outputs. (5, Dombenger)

I would add other related reason to the previous ones, the physical presence of workers. Traditionally, security or administrative people were sitting close to management, they could be consulted quickly in case of an incident or a doubt and their implication could be watched directly. Customer is then afraid of outsourcer not being involved at security incidents and not considering them as their own problems. Moreover, if customer does not have outsourcer workers near, he can feel outsourcer is not enough involved. But this factor should not be taken in to account by customers as actually physical presence is changing inclusive internally at theirs enterprises. Technology advances have caused a revolution in other discipline, Facility Management, whose outsourcing is increasing too. Everyday there are more technical staffs who work separated from different buildings to enterprises management and even they are working at their own houses. The important fact is working as a "virtual" team with common objectives using technologic advances and without enterprises frontiers :

> "In essence, the technology can now be attached to the individual and not just to a physical place. This dramatically changes the dynamics of how offices are structured...
> Teamwork is not limited to the corporate office. Today's technology is also making great strides in bringing geographically dispersed people together for collaborative work. The growth in electronically mediated team environments is seen in desktop video conferencing, electronic whiteboards, corporate 'chat rooms', etc. The facilities group needs to structure the office with areas where these types of facilities can be shared, where electronic whiteboards can be rolled into a team space and where larger communal monitors can be used to facilitate these high-tech meetings." (7, Reuvid & Hinks)

So, it is really a problem of delegation capability. Customers prefer not to delegate other enterprise their security problems and their security management, which implies not contracting security outsourcing at all or contracting incomplete security outsourcing.
On the contrary, if customer delegates on outsourcer and outsourcer gains customer's trust, we will have a good basis for a future win-to-win relationship between customer and outsourcer where security is the big winner. We could see this as the necessary trust among people at any life field where we treat with professionals, your doctor, your car repairer, ...

Scope

Customer and Security Outsourcer should join themselves to build on mutual agreement a proper common Operations Security Program which manages security during whole life of contract considering :

- Directive Operations Controls, being Security Policy and Procedures the base.
- Preventive Operations Controls, including main types of Defence- In-Depth protection which strengthen access controls at all information systems layers.
- Detective Operations Controls, as more known threats mitigation methods for internet
- Corrective and Recovery Operations Controls, for example Disaster Recovery Plans from Business Continuity Plans

This paper will go trough this Operations Security Program to show how an alliance between customer and outsourcer can improve level of security for customer.

Directive Operations Controls

Directive Controls is the key to build a common Operations Security Program between customer and outsourcer. Common objective should be to create a Corporate Program Policy, so many Security-Specific Policies as necessary to cover all security spectrum for the customer and associated Security Standards, Guidelines and Procedures to implement this directive controls into the rest of more "practice" controls (preventive, detective, corrective and recovery controls).

Here, we can find several types of situations : small customers without security policies, big customers with many written policies not transformed to "practice" controls, customers who do not communicate their policies because they consider them as something private. At all these cases, security outsourcer can improve situation because a good security outsourcer cannot work without security policy and for it, must know customer needs at security field :

- For customers without security policies, outsourcer helps them to think for first time which security policies really wish and can collaborate showing its own policies as a well experienced reference.

- For customers with non-implemented security policies, outsourcer helps them to transform these policies into security procedures which can be really implemented to systems and workings methods.
- For customers with "private" policies, outsourcer helps them to open their minds by building a common policy which uses elements from both policies : customer and outsourcer ones. This will imply a better security policy as it will be result of the best of two worlds.

Unfortunately, there will always be customers not providing any information to outsourcer. This conducts to security outsourcer facing security alone at these customers and very probably to mutual no satisfaction at security results. Outsourcer will be aware that security commitments could not be enough and customer will not be able to value outsourcer efforts because these commitments can not coincide with their actual security objectives.

Program Policy. First Policy and Joint Verification

To design a first Program Policy, a Joint Verification team composed by customer and outsourcer people with security skills is fundamental. Customer provides their security policies and their security problems and outsourcer provides its experience at security policies and solving security problems. The more knowledge from customer's security is acquired by security outsourcer, the better outsourcing security service will be.
So, customer attitude is the main driver for success. A "honest" customer will provide real information and will avoid to hide security problems. It is better to indicate "I have this policy but it is not being executed" and build together security policies and procedures to find difficulties at service time that can conduct to service disruptions and no satisfaction because customer procedures cannot be really executed.
First step to solve security problems is to admit them, as at any other life field. Sometimes, customer feels he is being audited or even interrogated by security outsourcer and he prefers to trick the supposed "opponent".
Joint Verification is a project to give service to customer and ensure a good transition to security service. An example of Joint Verification, even though treated partially, can be seen at another GSEC work (15,Martinez).

Program Policy. Changes

Technology evolves and our way of thinking also does. So, Security policy must be reviewed and modified accordingly. An annual review agreement between customer and outsourcer reserves space and resources to :

- examine possible on-going security problems and think how to correct them through policy changes,
- security areas not adequately examined at previous security policy reviews. For example, at first policy building time, there may be many other attention foci because all outsourcing service is being designed and all security areas are difficult to be managed at same depth.
- new business areas with new security requirements

Program Policy. Legal requirements

Program policy should include local legal requirements about data privacy and any regulatory normative associated to customer business. However, this aspect of security seems to have been forgotten by customers if you see the following internet poll. Although, 82 % enterprises have reviewed their policies, only 33% of them recognize to have reviewed new security legislation and regulations :

Have you reviewed the effectiveness of your information security policies in the past 12 months? (8, CSO online.com polls**)**


yes **(82%)**


no **(18%)**

Does your company have a designated process (or person) to review new security legislation and regulations? (9, CSO online.com polls**)**


yes **(33%)**


no **(46%)**


not sure **(21%)**

Mainly at European countries, there are severe laws specifically conducted to protect personnel data privacy. In fact, European Union (EU)has approved creation of the European Network and Information Security Agency and stricter measures to protect data privacy are expected. (13, COMM(2001)298Final)

So, a security outsourcer acting as a technological partner can be the best solution to implement legal measures. Outsourcer can share experiences among all their customers with same legal necessities and even expensive solutions could be shared between several small customers. Security policies and regulatory normative annual reviews ensure policy effectiveness and law awareness. In case of legal requirement changes, new projects should be developed jointly. For, it, a real technologic partner should be considered that has capability to execute new technological projects, not only execute an on-going project without modifications.

In fact, EU, at its Actions Plan “eEurope 2005 : An information society for all”, considers technology deployment associated to secure data and communications as a factor for EU progress as its objective is “to stimulate secure services, applications and content base on a widely available broadband infrastructure” (14, COMM(2002)263 Final)

Program Policy. Functions and Obligations of Personal

Many customers arriving to an outsourcing contract do not have any policy about functions or obligations of personal or do not have any disciplinary process in case of abuse performed by an employee. This, joined to the fact that most of security incidents are committed by internal staff, predispose enterprises to have security attacks, not to be aware of them and not to punish them. It is endorsed with this internet poll where only 17% of enterprises admit to have security policies with sanctions :

Is your company's information security policy armed with sanctions (i.e., specific repercussions for specific breaches)? (10, CSO online.com polls**)**


yes **(17%)**


yes, but not enforced **(17%)**


no **(33%)**


not sure **(33%)**

For these customers, outsourcing is an arm to ensure that possible incidents caused by technical people, which is now contracted by outsourcer, are rightly penalized. These incidents could have two ways of penalties : economical and administrative.

- First, economical, because there is an contractual relationship between customer and security outsourcer and security incident consequences as service unavailability are economical penalizable. And this aspect can only be covered by an outsourcing contract.
- Second, administrative, by outsourcer security policies. A good security outsourcer will have a security policy with personal guidelines for Functions and Obligations, Business Conduct Guidelines, Non-Disclosure Agreements and Disciplinary Processes in case of severe non-compliances. Outsourcer should have them by honesty but it is also part of its business if really wishes to remain at market.

At this way, outsourcer staff will know their obligations and job loss consequence if they are not complied with as it can suppose a big loss for their enterprise :

- economical by outsourcing contract penalties,
- economical by outsourcing contract lost,
- prestigious by outsourcing contract lost,
- prestigious by outsourcing contract lost publishing.

This awareness is really other security skill to be learned at enterprises with a big role at security and, hence, a dependency of security management way for growing at market.

Besides, if security incidents happen at a customer privacy area, non-disclosure agreements included in the contract between both customer and security outsourcers would work.

An important aspect is that if both customer and outsourcer have Functions and Obligations of Personal, its compatibility should be studied at Joint Verification.

Program Policy. Administrative tasks

To delegate outsourcer security skills contracting is really a headache less for customer because customer doesn't have to be worried about neither skills nor salaries.

To be effective and give a good quality security service, outsourcer should have a qualified staff to manage security. It does not mean people with high level of knowledge at security systems who can "hack" systems but people with real security skills to manage security and manage it honestly. Part of this staff recruitment is responsibility of Security Outsourcer Human Resources Departments but other external companies can help. Certified entities as GIAC or CISSP are trying to ensure this type of skills among conditions demanded to their candidates for their certifications. So, an outsourcer with this type of personal is an assurance for both the customer and the outsourcer.

About own security professionals, their salaries and their career will improve at an security outsourcing company. Security outsourcer can pay market salaries because he can share them among several customers and services and can offer a more attractive professional career as everyday there will be new challenges for any of his customers. This argument is endorsed in articles as "The Case for Outsourcing Security" at computer.org internet publishing (19, Schneier).

Specific-Security Policies

Besides general policy, normally designed by high level management, it is necessary to have lower level policies for the main security aspects. Now, we can see some examples of specific-security policies and outsourcing contribution to them :

Physical Access Security Policy

At this so important security field, we can find several typical outsourcing scenaries :

- Customers delegating all physical security at outsourcer
- Customers owning all physical security at their own buildings

At first case, it is physical security policy from security outsourcer to be implemented.
At second case, it is customer security policy which is implemented but it should be agreed to outsourcer by several reasons :

- continuous access need to customer installations from outsourcer staff to work
- outsourcer responsibility over systems availability and logical security do not let obviate physical controls at customer buildings
- contributions to improve customer policy with best practices of physical security at outsourcer policy

In favour of a full physical security outsourcing I would indicate :

- Buildings access control. It is easier for a big security outsourcer to have buildings with the most sophisticated access controls as they can be expensive, mainly for small customers. By sharing buildings to other customers, a better physical access control can be possible.
- Buildings safety. For the same reason, it is easier for a big outsourcer to have a safety and modern building with less risks, problems detection systems and tested evacuation procedures.
- Restricted access areas. Each restricted access area is prepared to hold systems for a particular customer. Protection measures for restricted access areas are designed and repeated for each customer ensuring effectiveness and privacy at the same time.
- Physical access controls : Latest authentication devices as smart cards or biometrics devices identifying staff accessing rooms where machines are hold are out of scope of small customers.

All these advantages let customers concentrate themselves on their business without having to think about technical people and systems safety or physical access controls.

Logical Access Control Security Policy

This policy should take into account the following principles indicated by SANS (1) and related to logical access controls : Data owner, Data custodian, Separation of duties, Least privilege.

- Data and userid ownership : Indispensable to a customer-outsourcer relationship as each part should be responsible for their data and users. An outsourcing contract forces to separate data files from operating system files and to seek for a owner per each data file inside customer organization.
- Data custodian : At an outsourcing contract, normally, custodian responsibility of removable media containing data is transferred to security outsourcer together with physical security. It is a good point to make an inventory of this kind of information, be aware of information at these media, to make a cleaning-up and assign owners. Regular reviews of inventory ensure protection of this information.
- Separation of duties : By concept, outsourcing is splitting security responsibilities. At a full outsourcing, meanwhile customer is responsible of business data privacy basically, outsourcer is responsible to manage the environment where these business data are stored and accessible.
- Least privilege : By considering outsourcing as an starting point, a profiles reviews based on least privilege can be done at the beginning of service. There will be business profiles for customer and technical profiles for outsourcers, all of them with least privilege necessary to do job.

User Administration Security Policy

This policy would be focused on administrative tasks related to Access Management : Account Administration, Maintenance, Revocation, Accountability and Monitoring as indicated by SANS (1).

- Account Administration. At this task, professionalism is gained with outsourcing as many customers are doing access management without procedures or with no secure procedures. Outsourcing of account administration lets this discipline is carried out with secure procedures and separation of duties. Customer is aware of internal approval workflows to get a new userid or a new access and outsourcer manage customer requirements once they have been approved rightly. Besides, outsourcer must authenticate always authorized people from customer to receive user requirements and to distribute confidential information as passwords in a secure way. There are less risk of social engineering as there are 2 enterprises involved at process.
- Maintenance. Userid ownership lets both customer and outsourcer review theirs users regularly.
- Revocation. Both customer and outsourcer must compromise themselves to have a good Human Resources process which communicates employees leaving companies in order to delete any associated individual userids. As a result of maintenance, errors at this process could be resolved periodically.
- Accountability. Again, this is other success factor for security outsourcing.It is necessary to use individual userids with associated ownership and to active systems audits to know who caused a security incident and, at this way, get accountability. This can determinate, sometimes an economical penalty, as we have seen previously. But sometimes, it is not possible to do determinate technical jobs with individual users as the case of “root” administrative userid at Unix-like systems. This problem is mentioned as a security outsourcing stopper but even though can not be solved at operating system (except for Z/OS Unix Services which interrelate to RACF to solve this problem) or security product (sudo (25) or Tivoli Access manager for Operating Systems (21) help some but are not complete), it could be solved with a solution which controls accountable use of this type of userids, as described at other GSEC work (15, Martinez).
- Monitoring. It is basic to get accountability, to be aware of what happens at systems and investigate incidents. And over all, it is the best tool to show outsourcer honesty at his job. So, a good outsourcer will always wish audit is active.

Information Classification Policy

Some customers believe an information classification policy is only incumbent upon themselves and they do not like talk this theme to security outsourcer, as if communicating how they classify data was communicating data itself to outsourcer.
This is, again, an error, as each classification level will have different protection requirements and treatments which outsourcer should know to proceed rightly.
Customer CIO failures in communicating requirements to outsourcer, can lead to non-fulfilment of customer data owners expectations.
Even, it can have legal consequences as some type of data require determinate security protection by data privacy laws.
So, this policy should be designed by both customer and outsourcer. This is the best method to ensure all company and legal requirements are done by all levels of information classifications.

Backup and Recovery Data Policy

This policy is closely related to Information Classification Policy. Normally, each level of classification will have a different backup policy.
Also, recovery data cannot be done at any way. Data owner is the only person who can authorize a recovery for certain data and it can have legal impact for personnel data. So, communication flows between customer and outsourcer should be established through this policy. Again,

outsourcing works as a separation of duties assurance : data owner approves and outsourcer executes.

Disaster Recovery Plan

Disaster Recovery Plan could be considered other security policy. Some outsourcing contracts do not include this plan to reduce price. It is an error because this money is well paid. It is the assurance to restore your systems in case of disaster. Outsourcer can help to build a Disaster Recovery Plan using customer requirements and real experience on this matter. Even, there are cases where customers have arrived to outsourcing after a Disaster Recovery Plan did not work properly and an outsourcer had helped to recover as many data as possible.
Besides, an external company helps to reduce typical mistakes around Disaster Recovery Plan. .

- DRP Testing : Because DRP design will be managed as a project, DRP only will take into production by outsourcer when it is enough tested.
- DRP procedure and roles : DRP procedure will be part of DRP plan, it is not only how backup data to be restored but how restore these data using involved people and technical.
- Alternative building : For an outsourcer it is easier to have an alternative building where to store backup data and restore systems. It can be really expensive for one customer but it is possible to share it between several outsourcing customers.
- Lack of Security Controls : If security is also contracted at outsourcing, security controls at restoration time will be taken into account at DRP design.
- DRP updates : A regular review to verify plan effectiveness included at contract will help DRP works continuously.

As you can deduce from following internet poll, DRP updates and testing are not being done by customers, normally :

Has your organization rehearsed its business continuity plan? (11, CSO online.com polls**)**

(32%)	No, we don't have one.
(27%)	We've never rehearsed it.
(14%)	We've rehearsed it once.
(27%)	We rehearse it or parts of it regularly.

Preventive Controls

Preventive Controls could be summarized at having proper tools and procedures to implement directive controls and provide defense-in-depth.

- Tools, because a big amount of machines should be managed centrally to avoid errors and to have a real control over machines and
- Procedures, because a good outsourcer only will execute tasks under procedures which indicate among other things how to use tools.

Examples of procedures or tools which an outsourcer could provide or improve are the following ones :

Centralized account administration

Customer can take benefit of an existing centralized account administration tool which ensures principles from account administration policy minimizing human errors and ensuring a bigger time for service. Tools like Tivoli Identity Manager (20) or BMC Control-SA (22) let :

- Requirements management
- Approvals management
- Involved people authentication
- User profiles definition
- Automatic provision
- 24x7 self-service for passwords reset
- Human Resources database connection
- User regular reviews

It is cheaper and faster that if the customer himself would have to develop this type of solution. Yet customer would have to work with outsourcer to adapt this tool to his requirements.

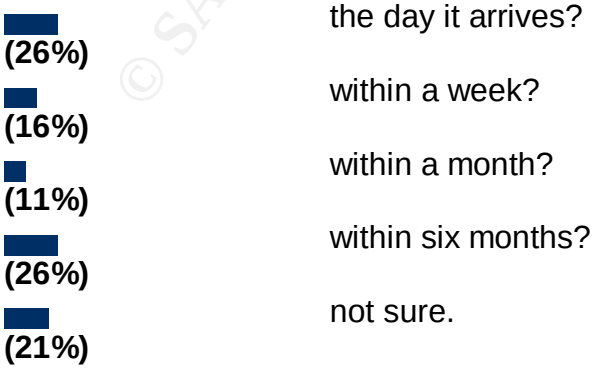
Production checklist.

Outsourcer administrative staff must work with production checklists to configure a new machine according to customer policies which would include system settings as password policy, user basic and profile definitions or system files protection. This very valuable tool to ensure right security at servers can be improved with experience of outsourcer at doing this type of skeletons and adapting them to customer requirements.
Regular reviews for productions checklists after security policy reviews or weakness detection are necessary to keep production checklist rightly updated.

Vulnerability Patches Fix Process

I see vulnerability patches fix process, together to antivirus update, as the preventive control by excellence to provide defence-in-depth.
This process' objective is having machines updated to the latest level of security patches. For it, first step is to be aware of new security patches as soon as they are available, second one is to plan patches fix at all impacted systems and last one is fix patches, really.
This process' quality can be substantially improved with an outsourcer as this process fails normally at many enterprises, as can also be seen from this poll from internet :

Does your organization apply software vulnerability patches.... (12)



Main advantage of outsourcing this service is that the customer can forget having dozens of suscriptions to different services to cover all platforms and products installed at machines and having to interpret their communications. It is outsourcer which does it. Other major advantage is that the low-detailed follow-up of fixes planning is performed by outsourcer.

Antivirus signatures updates Process

Similar to patches process, this process ensures signature files of antivirus software are updated. A security console to review status of updated and alert generation for problems help to improve this process and it is used by outsourcer to control all managed machines.

Detective Controls

These controls will help to detect both intents of bypassing preventive access controls implemented according to security policy and own security policy weakness.
Some of these controls, like IDS, could be considered also as preventive as let you know an unauthorized access very early and can be programmed to avoid it or send an alert.

Auditing

The simplest detective tool is to activate audit registration at systems. It should be imperative for a good security outsourcer as it allows to investigate responsibilities in case of a security incident. Once more again, outsourcer can improve auditing by having centralized logs servers with audit records for all systems. Outsourcer must have this type of solution to be able to study any incident or doubt which can happen at any of the so many machines managed by outsourcer.

System Health Checking

Thus is the way a good security outsourcer has to measure effectivenes to implement preventive controls based on customer policy. So, this service should be contracted. On the contrary, both customer and outsourcer would be working blind.
Tools like Symantec Enterprise Security Manager (23) or ISS System Scanner (24) could be used for this purpose with a central server collecting information from all connected agents.

Managed Security Services

Sometimes, the unique security area which is externalized are detective controls and are known as Managed Security Services.
Managed Security Services can be dealt by external people but it is always needed to collaborate with administrative people to discard false positives and understand vulnerabilities indicated by automatic tools. So, security outsourcer providing administrative security is basic to understand these type of reports and use them rightly and, hence, at least, second level support should be contracted to security outsourcer.
Skills for executing this type of services are very reputed at market and it is difficult a customer can hold these skills ((19, Schneier).

Among these controls we can find :

- Network-based intrusion detection
- Host-based intrusion detection
- Network Vulnerability Scanner

These type of services have become essential, mainly if customer servers are connected to internet. It is really a help in case of a security incident.

Corrective and Recovery Controls

Security Issues Management

All corrective actions resulting from a detective tool should be managed as security issues as they are really weakness. For each one of them, a corrective plan must exist and Outsourcer should present regularly security issues status to customer.

Incident Handling Process

Some security issues become security incidents and they must be managed and corrected rightly. At this case it is not valid outsourcer solves incident by himself and presents a report to customer. Here, both customer and outsourcer should work closely. For it, from outsourcing beginning, this process, roles and responsibilities and communications between customer and outsourcer must be clarified and written. Both parts should have 24x7 way of communication to handle incident together. Outsourcer can improve this process due to incident security experience and skills.

Disaster Recovery Plan

In case of a real disaster, Disaster Recovery Plan is other important procedure which must be carried out together with customer like security incident process. In fact, a real disaster could be considered as the worst security incident, really. To get success on it, it is very important Disaster Recovery Plan have been designed, tested and updated rightly.

Risk Analysis

Risk analysis should be considered at all stages of outsourcing contract. We have seen it at Joint Verification but it should be carried out with any security issue and security procedure at an on-going service.

Security Plan

All risks found at joint verification analysis and all changes to carry out at security management could be joint to build a security plan leadered by a Security Advisor.
When Security is understood as an strategic area at an enterprise, a Global Security Plan with associated resources should be considered. At this way, enterprise has an outsourcer resource thinking at its security as objective.

Conclusion

So, It's possible to outsource security and have a good quality service. The key is :

- To contract outsourcer with well provided security policies including Personal Functions and Obligations.
- To contract outsourcer with honesty behaviour in front of law
- To contract outsourcer with good security knowledge and awareness
- To contract outsourcer who can contribute as a technologic partner
- To contract outsourcer good at procedures and tools
- To contract outsourcer good at transitions
- To contract a full security outsourcing

- To review security requirements regularly and

- … to trust outsourcer and work jointly with him.

Please, take into account that some of these conditions are not included at basic portfolio from outsourcers companies. So, it is basic to know which security services are included at contract.

An example of a satisfied customer who was initially afraid of losing quality at security can be seen at (18, Steiner)

My acknowledgements to those colleagues already GSEC certified who have written papers about outsourcing even though it has been from a different point of view (15, 16, 17).

References

- (1) Cole, Eric & Fossen, Jason & Northcutt, Stephen & Pomeranz, Hal, Security Essentials with CISSP CBK Versión 2.1, February 2003, capther II. Defense In-Depth & Capther IV. Secure Comunications,
- (2) Wearden, Graeme, "Few Takers for Security Outsourcing", ZDNet UK, April 11, 2003, http://news.zdnet.co.uk/internet/security/0,39020375,2133349,00.htm (17-11-2003)
- (3) Jacques, Robert,"Don't limit offshore outsourcing security", vnunet.com, 19-09-2003, http://www.vnunet.com/News/1143741 (17-11-2003)
- (4) Breitling, Jay,"European MSSP Market to Grow to $4.4B by 2006", Security Wire Digest, 25-02,2002, http://infosecuritymag.techtarget.com/2002/feb/digest25.shtml (17-11-2003),
- (5) Domberger , Simon, The Contracting Organization: A Strategic Guide to Outsourcing, Oxford University Press © 1998, Chapter 7. Control and Flexibility
- (6) Cio.com Forum, http://comment.cio.com/comments/12651.html (17-11-2003)
- (7) Reuvid, Jonathan & Hinks, John, Managing Business Support Services: Strategies for Outsourcing and Facilities Management, Kogan Page © 2001, Chapter 2 - The Identification of Core Business Processes and Their HR and IT Implications,
- (8) CSO online.com polls, "Security Checks Results for Security Policy Reviews", (08/19/03 - 08/26/03), http://www.csoonline.com/poll/results.cfm?poll=1659 (17-11-2003)
- (9) CSO online.com polls, "Security Checks Results for laws reviews", (07/15/03 - 07/23/03), http://www.csoonline.com/poll/results.cfm?poll=1568 (17-11-2003)
- (10), CSO online.com polls, "Security Checks Results for Sanctions", (11/11/03 - 11/15/03) http://www.csoonline.com/poll/results.cfm?poll=1931 (17-11-2003)
- (11) CSO online.com polls, "Security Checks Results for BPC", (11/26/02 - 12/03/02), http://www.csoonline.com/poll/results.cfm?poll=650 (17-11-2003)
- (12) CSO online.com polls, "Security Checks Results for software vulnerability patches", (02/11/03 - 02/18/03), http://www.csoonline.com/poll/results.cfm?poll=866, (17-11-2003)

- (13) Commission of the European Communities, “COMM(2001)298Final, Network and Information Security, Proposal for an European Policy Approach” , 6-6-2001, http://europa.eu.int/eur-lex/en/com/cnc/2001/com2001_0298en01.pdf (17-11-2003)
- (14) “COMM(2002)263 Final . eEurope2005 : An information society for all”, 28-5-2002, http://europa.eu.int/information_society/eeurope/2002/news_library/documents/eeurope2005/eeurope2005_en.pdf (17-11-2003)
- (15) Martinez, Leslie, “Retain Control Of Security (even in the wake of an IT Outsource), (ver dirección internet), February 2003, http://www.giac.org/practical/GSEC/Leslie_Martinez_GSEC.pdf, (17-11-2003)
- (16) Tiow, Bee Ling, “A Security Guide for Acquiring Outsourced Service” , 19 Aug 2003, http://www.sans.org/rr/papers/index.php?id=1241, (17-11-2003)
- (17) Faile, Jonathan, “Security Outsourcing” , 25 Aug 2001, http://www.sans.org/rr/papers/index.php?id=223, (17-11-2003)
- (18) Steiner, Paul, “Outsourcing Security”, Security Management, October 2001, http://www.securitymanagement.com/library/Security_Steiner1001.html, (17-11-2003)
- (19) Schneier, Bruce, “The Case for Outsourcing Security”, computer.org, http://www.computer.org/computer/sp/articles/sch/, (17-11-2003)
- (20) IBM Tivoli Software, Tivoli Identity Manager, http://www-3.ibm.com/software/tivoli/solutions/security/id/, (17-11-2003)
- (21) IBM Tivoli Software, Tivoli Access Manager for Operating System, http://www-3.ibm.com/software/tivoli/products/access-mgr-operating-sys/, (17-11-2003)
- (22) BMC Software, Control-SA, http://www.bmc.com/products/proddocview/0,2832,19052_19426_22855_1587,00.html, (17-11-2003)
- (23) Symantec, Symantec Enterprise Security Manager, http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=45, (17-11-2003)
- (24) ISS, ISS System Scanner, http://www.iss.net/products_services/enterprise_protection/vulnerability_assessment/scanner_system.php, (17-11-2003)
- (25) Henry-Stocker, Sandra, “Sudo, Unix System Administration”, IT World.com, 03/21/2001, http://www.itworld.com/nl/unix_sys_adm/03212001/, (17-11-2003)