Contributions to IT Security in Outsourcing

NORBERT NEIDENBACH, EDWIN WOLF and GEORGE SAVII
Department for Mechatronics
"Politehnica" University of Timisoara
Bul. Mihai Viteazul 1, Timisoara 300222
ROMANIA
http://www.mec.upt.ro/~gsavii

Abstract: - In order to lower the costs many companies choose for the translocation of business processes within outsourcing. The present article highlights the most important inherent security aspects and proposes some measures for their implementation. It presents the risks related to outsourced IT security, the integration of outsourced IT security in the business processes and control means within an outsourced IT security.

Key-Words: - Outsourcing, IT security, Managed Security Services, ITIL, MDS

1 Introduction

During the past years the demand for IT (Information Technology) security has been continuously growing given the more complex applications as well as the inherent risks. At the very same time the business processes are depending more than ever on an efficient IT. Regarding this very need for action, the IT decision-makers must also take into consideration some aspects of IT security related to the question "make or buy".

1 Partial outsourcing

The partial outsourcing (outsourcing of individual IT security parts/functions) centers on IT security cost reduction and control. By translocating some parts of IT security, one can reach greater efficiency and transparency. Moreover the performance as well as some functions of the IT security can be monitored by means of a contractual warranty system.

By means of partial outsourcing the IT security personnel-related costs can be avoided (that would involve the so-called "around the clock monitoring, respectively a lot of answers")

The very access to expert knowledge as well as to the up-to-date technology can be guaranteed without personnel growth, as the IT security service provider is very competent and experienced in this field based on its central processes.

Due to the IT security outsourcing the outsourcing service provider can concentrate more on the central processes of its own company.

All these advantages are possible by using a Managed Security Service Provider (MSSP) [1, 2]. Within Managed Security Services (MSS) one can initially mention the firewall and Intrusion Prevention Technology operation as well as various antivirus measures [3, 4, 5].

A Managed Security Service Provider is specialized in standard Managed Security Services (MSS). The service performance, the quality, the service availability as well as the support are controlled in the so-called Service Level Agreement (SLA) which has been previously agreed upon [6].

The services imply activities which go from the sheer client system monitoring to service operation as well as to service outsourcing towards dedicated-systems (one system per client) or towards shared-systems (one system for more clients). On the European market, the MSSP is in the initial stage; nevertheless it never seized to make its presence felt on the American market.

The synergy, the saving potential and the efficiency are the results of the rapid response to new challenges by means of a professional analysis, by data cumulating methods as well as the results of the access to expert knowledge.

The purpose of outsourcing should harmonize with the general strategy of the company as well as with the aims, the established Return of Investment (ROI) and with the Total Cost of Outsourcing [5].

2.1 Risks of IT-security outsourcing

The introduction and the implementation of MSSP may have as a result failure of IT security functions [7, 8].

A major risk is represented by the fact that one company entrusts the IT infrastructure protection to another company and thus depends on an outsourced service provider. In this way expert knowledge and competence are lost in the process and cannot be recovered again.

The company providing the outsourcing services has a considerable insight in the company security system.

A risk assessment is therefore a foundation of each and every outsourcing.

At the very beginning of the outsourcing the responsibilities, the contact persons, the processes, information chains as well as technical and organizational connections must be harmonized, defined and documented [9].

The Information Technology Infrastructure Library (ITIL) is a framework of best practice approaches intended to facilitate the delivery of high quality IT services [10, 11]. ITIL outlines an extensive set of management procedures that are intended to support businesses in achieving both quality and value, in a financial sense, in IT operations. These procedures are supplier independent and have been developed to provide guidance across the breadth of IT infrastructure, development, and operations.

In order to avoid risks, all the ITIL processes, especially those processes in relation with the service-support must be observed. Furthermore there are response and maintenance intervals, monitoring, reporting which must be established.

An in-depth analysis of the reported security problems has led to the conclusion that one also must define the way of handling the demand as well as the way of harmonizing the knowledge transfer between the outsourcing provider and the internal IT.

Moreover one must also take into consideration the following issues as well as the SLA contractual provisions:

- certification of MSSP according to a recognized security standard (BS 7799 / ISO 17799) respectively pursues the recognized security standards)
- existence of security measures for data protection with regard to privacy, integrity and availability
- security directives as part of the contract
- existence of a data security and data archiving concept
- existence of a Business Continuity Management (of an emergency plan and aftercare measures)
- verifying the MSSP capacities and resources in order to observe all the contractual capacities
- contractual regulations regarding contractual penalties
- existence of a recovery plan in case of the premature contract dissolution
- MSSP references
- verifying the possibility of an MSSP audit by means of the internal IT
- verifying the security demand as well as the personnel training.

2.2 Security measures

By means of IT security functions outsourcing the costs and the internal capacities can be saved by the outsourcing provider and in this way one can achieve a greater quality and a better control.

In this respect one must also asses the risks and the internal expenses regarding the control of the MSSP and of the necessary in-house processes. It is therefore of utmost importance to include the results of the above assessment in the decision.

Higher costs as well as outsourcing inefficiency are the result of neglecting of these aspects.

In case of a contract negotiation one must:

- observe the security measures
- observe the service providing and SLA provisions
- observe the agreement upon regular auditing reports
- take into consideration the risk minimizing measures

3 Total outsourcing (Full Service Outsourcing)

In most cases one may choose the outsourcing of the whole IT security as a consequence of the outsourcing of the operative IT and this should be distinguished from the outsourcing of individual IT security functions.

All the operative activities of the IT security are indicated below and the outsourcing provider is limited to:

- the strategic orientation within the field of IT security
- the service provider control
- to the definition of the security demand on the basis of the business processes
- to the monitoring of the legal requirements observation (e.g. the person in charge with data security or revision)

In this respect one must also take into consideration the internal expenses as well as the tasks resources and the functions within the general IT outsourcing costs.

3.1 Risks

A total IT outsourcing and implicitly the IT security to a MSSP is known to present both risks and advantages [7, 8].

The outsourcing provider must assume the IT risk to a greater extent in its capacity of a decision-maker regarding IT assisted processes, although it cannot directly influence the application of the IT security requirements. The outsourcing provider is obliged to observe all the legal requirements. The outsourcing provider is also responsible for the financial prejudices due to the IT unavailability or due to the privacy or integrity loss.

It is thus of utmost importance to create a universal security management in collaboration with the IT provider and to establish this contractually in the SLAs. Under these circumstances the feasibility of such a security management is also very important. The risks presented by IT outsourcing can be reduced by means of evaluation and efficiency which also guarantees a strong bond between the outsourcing provider and the client.

3.2 Managed Security Services Process (MSS) in case of the client (outsourcing provider)

The Managed Security Services (MSS) are based on the security requirements of the business processes, on the general conditions of the IT strategy as well as on the risk management (among others general security directives) and legal prescriptions.

For the organizational application of the above mentioned requirements, there must be some persons in charge with service and/or application on behalf of the outsourcing provider, who are the bridge between business processes and IT service providers.

The identification of business process requirements regarding the availability, the privacy and the integrity is to be carried out by means of a risk assessment which must be in conformity with the general risk management of the client.

The purpose of the risk management is the grouping in classes as well as the documenting of the requirements and of the business process prejudice potential regarding the IT. In this respect one can use the classification of the general security standards in order to achieve consistency and objectivity:

- Public information (the information is available and its publication does not bring any prejudices)
- private information (internal company information, which should not become available to third parties)
- secret information (information with increased security requirements, its disclosure to third parties would bring a noteworthy prejudice to the company)
- top secret information (only authorized personnel of the company has access to it; a disclosure to third parties would bring a major prejudice to the company.

Fig.1 presents an example of the risk classes' representation of an IT service, based on the risk assessment (risk classes could also be assessed by means of the potential amount of damage).

The IT service classification in risk classes and a risk potential assessment of the business processes can occur by means of IT service client consultation.

The IT security is not a goal in itself, but a real measure for risk minimization.

After evaluating the contractual risk assessment results, the requirements as well as the measures or risk minimization must be contractually regulated together with the IT service provider within SLA.

Of utmost importance is the risk and expenses analysis by means of which the measures for risk minimization with regard to the expenses can be assessed.

The expenses inherent to the security measures must be assessed in relation to the prejudices in case of a security event.

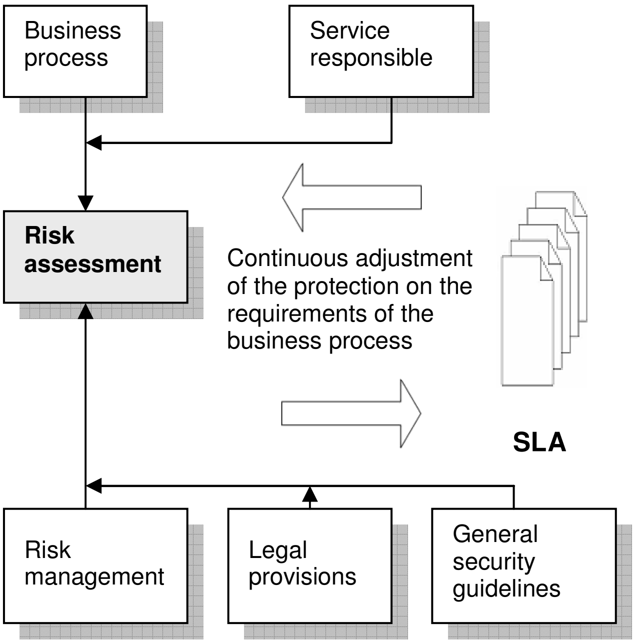
Business process
Service responsible
Risk assessment
Continuous adjustment of the protection on the requirements of the business process
SLA
Risk management
Legal provisions
General security guidelines

Fig.1 Risk analysis of business process

In order to categorize the security demand of an IT service one can refer to standardized security classes within SLA. The security classes can be based on recognized security standards, such as ISO 17799 in order to be objective and measurable. Because of the continuous changes in the demand within the business processes a regular monitoring as well as an eventual classification alteration can be carried out. The importance of the IT services can vary and the end goal should be a reliable and accurate security level by means of which an efficient and cost-effective security management can be achieved.

The established measures are to be implemented for the particular security class with the help of guidelines and process descriptions that can be applied to individual systems. In order to verify the measures implementation a client reporting form (for the revision and the as well as for the data security in charge personnel) must be drawn up. By automating the here above reporting the expenses are reduced and the relevance is ensured. The security issues are thus transparently rendered and can also be efficiently highlighted.

3.3 IT security control, security auditing

Besides the SLA inherent reporting, various auditing and control functions must be implemented in order to achieve an active control, traceability as well as transparency of security measures.

The auditing object is represented by the following verifications:

- verification of the functionality of the security management as a whole,
- security verification of various business processes
- verification of security classes measures implementation in various fields of the IT service providers

All these verifications must be carried out by continuously observing the contractually recognized security standards.

4 Conclusion

The analysis of the IT outsourcing processes and markets allowed the highlighting of the most important inherent security aspects related to IT outsourcing and to propose some measures for their implementation. As important aspects, the risks related to outsourced IT security, the integration of outsourced IT security in the business processes and control means within an outsourced IT security were presented and analysed.

With regard to the total IT outsourcing to an IT-Service Provider, the universal and unitary process starting with the risk evaluation and up to the risk reduction measures becomes more and more important. In this way possible process gaps can be avoided, losses can be minimized and the IT security can be economically and efficiently operated.

By means of reports, KPIs (Key Performance Indicators) and regular auditing, the IT security performance can be fully controlled even if this occurs within an outsourcing project. Moreover the risks can be held at bay.

References:

[1] *Managed Security for the Small and Medium-Sized Business – The Benefits of Out-Tasking Security Services to a Qualified Service Provider*, White Paper, Cisco Systems, Inc., 2007.

[2] Y.S. Choi, D.I. Seo, An analysis of ISP’s role as managed security service providers (MSSPs), *The 7th International Conference on Advanced Communication Technology*, ICACT 2005, Volume 1, 21-23 Feb. 2005, pp. 624 - 626.

[3] *Managed Security Services for Small, Midsize, and Enterprise Organizations*, *Overview*, Cisco Systems, Inc., 2004.

[4] J. Allen, D. Gabbard, C. May, Outsourcing Managed Security Services, *CERT,* 2003.

[5] J.L. Ott, Managed Security Services, *Information System Security*, Vol 10, No 4, September/October 2001.

[6] K. Brittain, R. Matlus, Road Map for IT Service-Level Management. *Gartner Article Top View*, 28 January 2002.

[7] M. Alner, The Effects of Outsourcing on Information Security. *Information Systems Security,* Auerbach Publications, CRC Press LLC, May/June 2001.

[8] L. Phifer, Outsourcing Security Needs to a Managed Security Service Provider. *SearchSecurity.com*, November 8, 2000.

[9] J, Pescatore, Choosing a Managed Security Services Provider. *Gartner Research Note*, 31 August 2001.

[10] E.A. Van Schaik, *A Management system for the Information Business,* Red Swan Publishing, 2006

[11] van Bon, J.(Editor), *The guide to IT service management*, Addison Wesley, 2002