Information Security in System Outsourcing

Tero Viiru, Kajaani Polytechnic,
Faculty of Technology,
FIN-87100 Kajaani, Finland.
E-mail: Tero.Viiru@kao.fi

Jussipekka Leiwo, Monash University,
Faculty of Computing and Information Technology,
MacMahons Road, Frackston, VIC 3199,
Australia.
Email:Jussipekka.Leiwo@fcit.monash.edu.
au

Abstract

Outsourcing agreement is a document to specify the relationship between outsourcing partners; service provider who offers the outsourcing service and client whose system is to be outsourced. A major success factor of the outsourcing is clear and comprehensive specification of duties and responsibilities regarding to information security. As the outsourcing agreement is juridically binding, service provider is responsible for acting accordingly. Therefore, the agreement is where security Measures should be agreed upon. As there is no clear understanding of contents of an adequate security specification in outsourcing agreement, this paper identifies the critical components and studies the issue of how to set requirements for outsourcing service providers and control enforcement of these requirements.

Keywords: Information security requirements, information systems outsourcing, information system agreements

1. Introduction

Information system outsourcing has usually been studied and justified from the financial point of view. This is a logical approach, since the major motivation behind outsourcing is usually reduction of operational cost of the system and gaining of special skills into the organization (Lacity and Hirschheim 1993). In general, outsourcing is a well understood area of information systems research (Barua 1995), but there is a special need for the consideration of information security in outsourcing. As the importance of information security as a quality

www.manaraa.com

factor of an information system is widely acknowledged, and outsourcing in generally emerging, maintenance of an adequate level of security becomes a major success factor in outsourcing. As security always increases the cost of operation, opportunity for outsourcing service provider to save by reducing security may become tempting.

Traditionally, only non-strategic systems have been outsourced. This is, anyhow, changing (Rao, Kichan and Chaudhury 1996; Hirschheim and Lacity 1997), and therefore the traditional assumption of guideline-based approach towards security (Kajava and Viiru 1996) is no longer appropriate. Typically, information security methods have evolved from checklist-based methods to the risk analysis and evaluation criteria methods (Baskerville 1993, Backhouse and Dhillon 1996). Current checklist-based approaches (Kajava and Viiru 1996) are adequate when outsourcing noncritical systems, but when the importance of outsourced systems increases, more convincing provision of security of service providers is required. This leads to the specification of the major research question within this paper: Identification of factors that have an impact on information security in outsourcing and how requirements can be formulated to cover those factors. Once this is clarified, a method can be established to provide assurance that outsourced system satisfies these requirements.

The fundamental trade off in information security is between provision of security and cost of operation. In general, higher security, higher cost. Compromising security of client's system may reduce operational cost of service provider, and the cost effectiveness of the system may increase on the short run. On the long run, on the other hand, there is a great threat of losses due to violations of security exceeding the benefit gained by reduced security. Therefore, the need for security should not be underestimated and reductions in protection justified by reduced operational cost.

The fundamental information security objective for an outsourced system is maintenance the security as it was when systems were operated internally. Anyhow, as the client looses direct control of the system, there may be a need to increase the standard. As the outsourcing agreement is the main method for setting requirements and responsibilities for client,

www.manaraa.com

there is a clear need to identify the topics that affect the comprehensiveness of security specification in the agreement.

Outsourcing contract is a part of the information security policy of both client and service provider. Requirements for outsourcing can be specified as guidelines, risk analysis, evaluation criteria or information security model. The fundamental problem is to how to guarantee to the effectiveness of security mechanisms in outsourcing. Guidelines are the lowest and formal security models are the highest, though most limited from scope, level of assurance to the comprehensive of information security. The specificy and accuracy of security is risen from guidelines to evaluation criteria. Outsourcing security policy is based on results of risk and cost analysis before outsourcing. Outsourcing contract is a key element for information security policy in outsourcing.

From the three views towards outsourcing: juridical, administrative and technical (Douglass 1993), we shall adopt the administrative point of view. Information security requirement shall be specified very broadly to be any mechanism or procedure that client must implement to maintain or improve satisfactory level of information security on operations. Implementation mechanisms of requirements shall not be studied within this paper but the focus shall be on identification rather than detailed analysis of enforcement of requirements. The focus shall be on two first phases of outsourcing: preparation and specification of an agreement. The issues studied within this paper do not influence signing of the agreement. As the major reasons for outsourcing are usually cost reduction and gaining of skilled personnel, most of the research is focused on cost benefit analysis (Wang 1995). As these issues are well understood, there is no need to study them within this paper.

This paper starts with the identification and definition of key concepts and surveying the role of outsourcing agreement in business processes. The results are presented in section 2. Once the concepts are clarified, section 3 provides with a brief analysis of new threats that outsourced systems must face compared to traditional non-outsourced systems. Once threats have been identified, we shall provide a method to provide assurance from the enforcement of security threats in section 4. Finally,

www.manaraa.com

conclusions and ideas for further research shall be presented in section 5.

2. Outsourcing Agreement and Business Processes

Information systems outsourcing means partial or total transfer of the operational responsibility of an internal information system to an external supplier (Lacity and Hirschheim 1993, Richmond 1993). The main difference between outsourcing and subcontracting is the transferring of internal operational responsibility of information system to an external supplier in outsourcing, but in subcontracting there is nothing transferred outside to the organization but external services are bought in. The second important difference is the transfer of responsibility. In outsourcing the responsibility of operations is transferred outside the organization, when in subcontracting the responsibility of operations still remains in-house and subcontractor offers only the needed services, but it has not operational responsibility for information system. Outsourcing involves two parties service provider and client. Service provider is the instance offering outsourcing service to a client willing to fully or partially outsource its information services.

Outsourcing is based on outsourcing agreement that is a document specifying information processing services that shall be outsourced, and setting requirement to the external party regarding maintenance and improvement of these services. Once requirements are established, parties must agree upon acceptable cost of these services. The more detailed the agreement, the more detailed cost analysis can be carried out. As both parties are attempting to maximize their benefit of outsourcing, the agreement is a crucial document to provide mutual satisfaction on conditions. This is, that the contractor makes profitable business and the outsourcing organization gains expected savings in operational costs (Lacity and Hirschheim 1993).

To provide this satisfaction, the agreement should clearly specify rights, responsibilities and commitments of both parties. Outsourcing contract is the most important document and starting point to the outsourcing. Participants should also identify and assess information security threats related to outsourcing. Outsourcing contract belongs to the responsibility of top managers of organization, but the help of different experts should be used

www.manaraa.com

at this stage (Douglass 1993). At the highest level, top management is required to identify the strategic value of different systems, and to decide which systems must be outsourced, and to specify high level requirements for the agreement, that shall be further refined within the agreement process (Alpar and Saharia 1995).

The outsourcing contract can be made in stages (Richmond 1993) so that in designing stage of outsourcing contract the client represents the cost estimates of outsourcing. The client can accept or reject the draft. If client accepts the draft then client defines the needed investment. When investing planning is finished, the client calculates the final cost of outsourcing. The client either accepts or rejects referred offer. If client accepts the offer the system shall be outsourced.

An essential quality factor in the outsourcing agreement is comprehensiveness. Comprehensiveness refers to the inclusion of all relevant issues into the agreement. External specialists can be used to specify measures and metrics to control specifications of outsourced subsystems. It is also essential to include potential alterations, additions and sanctions with the developing of business actions (Lacity and Hirschheim 1993). To prepare into potential problems, it is imperative that responsibilities and rights of different parties regarding compensations and corrective actions are clearly specified and understood by both parties. Therefore, the agreement should explicitly specify all security requirements that service provider is expected to meet in implementation and operation of the system in an unambiguous manner.

Outsourcing organization should not restrict the business of client, but the businesses in which the client is involved affects to the information security of client. The expectations of the adequate level of information security may be different in client and service provider. A fundamental question becomes, how conflicts of different expectations can be solved. Organizational information security model may become a feasible solution. The guideline-based solutions may not be flexible and expressive enough to solve these problems. Recent trend in the management of information security is specification of extensive checklists, such as British Code of Practice (1996) and German IT Security Evaluation Manual (1996). These documents can act as guidelines to the security

www.manaraa.com

in many non-critical systems but need to be supported by more advanced methods when critical systems are concerned (Von Solms 1997).

Different systems must also be separated from each other as specified in the outsourcing agreement. Business functions can be flexible, but the level of information security must be stable or get improved when business situations change. The fundamental problem of this kind of situation is provision of assurance of the satisfactory level of information security. Thus the minimum standard for information security and requirements must be maintained.

In the agreement stage of contract issues such as how exactly contract confines, what matters should put in the contract and what is the reporting procedure of client must be considered. Outsourcing contract must define exactly its subject area, prevented threats and acceptable mechanisms against them (Richmond 1993). The question of acceptable protection measures is a critical success factor of the management of information security. As development of security enforcement mechanisms are an extremely complicated task it is essential that those responsible for information security clearly state which security enforcement mechanisms are to be used. As a general principle, publicity analyzed algorithms and implementations that have gone through public investigation and analysis by security professionals should be favored and proprietary and less understood measures avoided.

In the outsourcing agreement, information security requirements can be stated at three levels: first there is guideline-based approach, second there is risk analysis and third there is evaluation criteria approach towards information security. As the level of information security rises from first level to third level, also cost increases. Therefore, it is essential for client to consider the expected security level of systems to be outsourced.

3. Security Threats in Outsourcing

Maintenance of adequate level of security is a fundamental problem in outsourcing since the outsourcing organization loses the direct control of information system and thus it cannot affect directly to the functioning of information system (Wong 1993). Because the responsibility of enforcement of information security is transferred to the service provider,

www.manaraa.com

the adequate level of information security must clear out in the outsourcing agreement.

The fundamental cause of new information security threats in outsourcing is the potential conflict of interests of outsourcing parties. As both parties are attempting to gain financial benefit, their interests may be in conflict and this may open the system to new threats. The level of information security may not be adequate, if the client cannot demand specific and required actions to be made for the maintaining of information security. As security increases operational cost, but reduce losses on the long run, reduction of operational costs by compromising security may be a tempting option. This is due to the fundamental property of information security. Benefit of security always comes from prevention of losses, not from increasing income.

The threats against system are same as in the internal operation of systems. Basically, all new threats are introduced by different interpretation of requirements set in the outsourcing agreement and the different environment and personnel. The fundamental problem is that has the client all the needed information and methods to maintain the information security. Is there any new and unknown vulnerability in the outsourced information system that must be taken into consideration? If the whole information system is outsourced, with the former personnel, rooms, softwares and hardware then the situation remains the same, but the employer is only changed. Then the threats of outsourcing can be quite easily noticed and predicted. There is also a theoretic possibility of external operators being untrustworthy, but that shall not be considered a major issue within this paper. We do agree that personnel security is an important facet of information security, but the focus of this paper shall be on threats that can be reduced by proper specification of the agreement.

The fundamental new information security threat in outsourcing is leakage of information from outsourced systems to competitors by new channels existing due to the transfer of operations to the client. For example, a failure in file system or improper destruction of printed material by service provider may lead to an unauthorized disclosure of business critical information to other businesses. When information system is not functioning properly

www.manaraa.com

or there has been some other problems, such as intrusion, then client can fail report to the operations of information system and client can hope to solve problems before anybody notices them. Especially when there is a threat that client may lose the outsourcing partnership for the problems or client has to pay too high sanctions to the client and client has financial problems. It is very important to notice that the dependency of client is very high and this can be very fatal when problems occur and thus the problems must be eliminated beforehand and this is a one key point to the management of information security in outsourcing.

4. Security Process in Outsourcing

To provide first requirements and later assurance of the enforcement of these requirements, a contractor provides assurance of the security enforcement. A method for this shall be introduced within this section. We shall identify each step and analyze essential ones in detail. The following steps must be considered:

STEP 1. The organization considering outsourcing specifies their security requirements. At this phase, the organization reviews their information security analysis to update and refine requirements when the system is outsourced. Depending on the level of assurance expected, different levels of formalism are required. Typically, managerial responsibilities and pervasive security requirements can only be represented as high level statements, but technical, specific information security requirements can be represented and analyzed using tools and methods of different levels of formalism.

Tools for representing technical security requirements are various. Several formal languages and notations have been developed for expressing requirements. Early access control models, such as BLP-model for confidentiality (Bell and LaPadula 1975) provided with means to specify mandatory access control requirements as tuples (s, o, r) interpreted intuitively as subject s having exactly r right to access object o. This notation was quickly proven to be inadequate, and formal, more flexible languages such as (Woo and Lam 1992) and (Jajodia et al. 1997) were proposed for coding security requirements. Access

www.manaraa.com

control requirements have also been successfully represented using Requirement Engineering (RE) approach (Dubois and Wu 1996) and Z notation (Boswell 1995). Additional coding mechanism include logic based on the theory of normative positions (Jones and Sergot 1992), security logics based on knowledge, permission and obligation (Glasgow et al 1992), specific notation for protection of associations (Leiwo and Zheng 1997) and enhanced system modeling notations such as security enhanced DFD diagrams (Baskerville 1988). Additionally, formal notations of, for example, (Kabasele-Tenday 1997) can code descriptions of threats. There are several alternatives for coding security requirements, and the selection should be made based on specific needs of protection of each system.

STEP 2. Contractor reviews the requirements. This is basically delivery of a report of security requirement analysis to the contractor for review. As the business of contractor is based on volume, requirements may need to be modified to meet the operational requirements of the contractor. Similarly to the specification of client's security requirements, different levels of formalism can be suggested.

STEP 3. Depending on the suggested changes by contractor, client either accepts or rejects the proposal. In case the proposal is rejected, then the client must return to step 1 and either to modify requirements or to find another contractor.

STEP 4. In case of accepted suggestions, the next step is that the contract is agreed upon, and the system implemented according to agreed security specifications. How this is implemented is not as stated in section 1 - within the scope of this paper.

STEP 5. Contractor provides assurance of the security enforcement. The last step of the outsourcing process is where contractor provides client with the assurance that the system enforces required security features. The level of detail required for the provision of assurance must be stated in the outsourcing agreement, and depends on the level of required security. Depending on the level of formalism required, different security logics as listed before

المنارة للاستشارات
www.manaraa.com

can be used. A suitable approach towards provision of assurance is according to the European Information Technology Security Evaluation Criteria (ITSEC 1992) where different levels of assurance can be required:

A) State: The contractor provides evidence that security mechanisms are implement to enforce required security features.

B) Describe: The contractor provides evidence that security mechanisms are implemented and a justification of them enforcing required security features.

C) Explain: The contractor provides evidence that security mechanisms are implemented and provides a detailed analysis of their capability to provide with expected security.

The problem is that the client and client must first agree the security methods and after that client must be capable to prove that security methods are functioning and effective, or some other trustworthy instance may do that. The proving of this capability in a trustworthy way is not simple task, and it is always hard to clarify the 'right threats'. So client can use a generally accepted, scientific proved, model for this, or some generally known and accepted security system. Evaluations are always evaluations, so the are not exact fact. A formal model that is proved effective in science and practice is a one suitable way to approach information security in outsourcing. However, it is important to notice that outsourcing can be operated in stages, and then different matters can be agreed and checked in each stage. It is important to agree a common goal for information security and agree the suitable methods for archiving this common goal.

5. Conclusion and Future Work

As a conclusion of this paper can be stated that contracting of outsourcing must be done in care. All the contracting matters are equally important, especially savings, costs and information security. The outsourcing contract can be made in stages and this is suitable for information security. There must be different mechanisms to prove the effective of security mechanisms, for example as in ITSEC. It is very important to make sure that the client can

www.manaraa.com

provide the needed service and maintain required level of information security. The costs and risks of outsourcing must be evaluated before outsourcing and different plans and policies are formulated. It is very important to make sure that security requirements are as clear as possible and the both sides of outsourcing can understand and agreed them. In the outsourcing agreement there must be written the minimum requirements for the information security and suitable security methods. The responsibilities and rights of the outsourcing parties should be clearly agreed upon in the outsourcing agreement. It is imperative that accepted information security policies in outsourcing and recovery and strategic plans have been established. The actions of insourcing and changing of the outsourcing partner must be planned too. The education and inform of personnel in information security matters is important and must be regular. All the information security matters must be defined clearly in contract and understood. It is important to make sure that you are dealing with trustworthy and best possible service provider that you can have afford, the money is the keyword in outsourcing and information security. The more money you spent on security the less money you spent in business, but the security is not bad investment on the long run.

One fundamental security threat in outsourcing is the potential conflict of interest of outsourcing parties. Threats in outsourcing are basically same as in internal information system and all new threats are introduced by different interpretation of requirements in the outsourcing agreement. A one threat in outsourcing is the leak of information from outsourced system. In outsourcing the important security method is controlling and monitoring of service provider. It is important to plan, control and agree the actions of client and service provider. For the controlling and agreeing of information security in outsourcing there can use ITSEC or CC-model. It can be stated that there is three different level of security, from lowest to highest, guidelines, and risk analysis and evaluation criteria, including information security models. If client and service provider can use methods of some formal model for managing information security, then information security is defined accuracy.

A one interesting question for future work is the management of information security in outsourcing. How different contracts and plans

www.manaraa.com

affect to the management of information security? Can plans for the management of information security is worked all at once or in stages? How outsourcing can be understood, a one huge process or a staged process? These are the fundamental questions for the management of information security in outsourcing.

References

Alpar, P. & Saharia, A. N., (1995): Outsourcing Information System Functions: An Organization Economics Perspective. Journal of Organizational Computing, 5(3), 197-217.

Backhouse, J. & Dhillon, G (1996): Structures of responsibility and security of information systems. European journal of information systems 5(1), 2-9.

Barua, A. & Richmond, W. B. (1995): Introduction to the Special Issue on Economics of Information Systems. Journal of Organizational Computing, 5(3), 195-196.

Baskerville, R. (1988): Designing Information Systems Security. John Wiley & Sons.

Baskerville, R. (1993): Information Systems Security Design Methods: Implications for Systems Development. ACM Computing Surveys, Vol. 25, Num. 4, 375-414.

Bell, D. E. & LaPadula, L. J. (1975): Secure Computer Systems: Mathematical Foundations and Model. MITRE Corporation Technical reports M74-244. Bedford, MA, USA.

Boswell, A. (1995). Specification and alidation of a Security Policy Model. IEEE Transactions on Software Engineering, Vol. 21, Num. 2, 63-68.

Code of Practice for Information Security Management (1995), British Standards Institute Standard BS 7799, UK, 1995.

Douglass, D. P. (ed.) (1993): New Wrinkles in Outsourcing, I/S Analyzer, September 1993, Vol. 31, Num. 9, 1-17.

Dubois, E. & Wu, S. A. (1996): Framework for dealing with and Specifying Security Requirements in Information Systems. Proceedings of the IFIP TC11 12th International Conference on Information Systems Security (IFIP/Sec'96). Samoa,

المنارة للاستشارات

www.manaraa.com

Greece.

Glasgow, J., MacEwen, G. Panangaden, P. (1992): A Logic for Reasoning about Security. ACM Transactions on Computer Systems, Vol. 10, Num. 3, pp. 226-264.

Hirschheim, R. & Lacity, M. C. (1997): Information System Outsourcing and Insourcing: Lessons and Experiences. Proceedings of the 1997 Pacific Asia Conference on Information Systems. Brisbane, QLD, Australia.

IT Baseline Protection Manual (1996), BSI, Germany, 1996.

Information Technology Security Evaluation Criteria (ITSEC). (1992): Provisional Harmonized Criteria, version 1.2. Commission of the European Communities COM (92), 298 final. Brussels, Belgium, September 1992.

Jajodia, S., Samarati, P. & Subrahmanian, V.S. (1997). A Logical Language for Expressing Authorizations. IEEE Symposium on Security and Privacy.

Jones, A.J.I. & Sergot, M. (1992): Formal Specification of Security Requirements using the THeory of Normative Positions. Computer Security - ESORICS'92. Springer-Verlag LNCS 648.

Kabasele-Tenday, J. -M. (1997): Specifying Security in Composite Systems. Proceedings of the 1997 Information Security Workshop. Ishikawa, Japan.

Kajava, J. & Viiru, T. (1996): Delineation of Responsibilities regarding Information Security during an Outsourcing Process from then Client's Point of View. Twelfth International Conference on Information Security, Sec '96/WG 11.1, Information Security Management in a Distributed Environment, Pythagorean, Samos, Greece, 20. May 1996.

Lacity, M. C. & Hirschheim, R. (1993): Information Systems Outsourcing. John Wiley & Sons, Guilford, Surrey.

Leiwo, J. Zheng, Y. (1997). A Framework for the Management of Information Security. Proceedings of the 1997 Information

www.manaraa.com

Security Workshop. Ishikawa, Japan.

Oltman, J. R. (1990): 21st Century Outsourcing. Computerworld, April 16.

Rao, R., Kichan, N. & Chaudhury, A. (Guest editors)(1996): Information Systems Outsourcing. Special Issue in Communications of the ACM, Vol. 39, Num. 7, 27-54.

Richmond, W. B. & Seidman, A. (1993): Software Development Outsourcing Contract: Structure and Business Value. Journal of Management Information Systems, summer 1993, Vol. 10, No. 1, 57 72.

Schneier, B. (1996), Applied Cryptography, 2nd edition. John Wiley & Sons, New York.

Von Solms, R. Can Security Baseline Replace Risk Analysis In Proceedings of the IFIP TC11 13th International Conference on Information Systems Security. Copenhagen, Denmark, 1997.

Wang, E. T. G. & Barron, T. (1995): The Decision to Outsource IS Processing Under Internal Information Asymmetry and Conflicting Objectives. Journal of Organizational Computing, 5(3), 219-253.

Wong, K. (1993): Outsourcing IT-Safeguarding Your Legal Interests, Purchasing & Supply Management, December, 30-33.

Woo, T.Y.C. & Lam, S.S. (1992): Authorization in Distributed Systems: A Formal Approach. Proceedings of 1992 IEEE Symposium on Research in Security and Privacy.

www.manaraa.com