INFORMATION SECURITY CONCERNS TOWARDS BEST PRACTICES FOR IT OUTSOURCING PROJECTS FROM THE PERSPECTIVE OF SERVICE PROVIDER IN IRAN

NIMA PARHAM

A project report submitted in fulfillment of the
requirements for the award of the degree of
Master of Computer Science (Information Security)

Centre for Advanced Software Engineering (CASE)
Faculty of Computer Science and Information System
Universiti Teknologi Malaysia

MARCH 2009

Dedicated to my loving parents

ACKNOWLEDGEMENT

I would like to express my sincere appreciation to all those people who supported me and helped me with the writing of my master thesis.

First of all, I am extremely thankful to my supervisor, Dr. Zuraini Binti Ismail, for encouragement, intellectual support and understanding that made this research possible, and for her patience.

I am grateful to my friends, Shadi and Hamid. You have been there during the difficult times and the good times along the way. I also thank my brothers and sister, Pouya, Saman and Sanaz, for their unconditional love.

And finally, I must acknowledge my greatest cheerleaders, my loving parents. I am forever thankful to my parents, Nabi and Parvaneh, who have loved and prayed for me through every journey in my life. Father and Mother, I love you, you inspire me to go higher.

ABSTRACT

Many firms are now evaluating the possibility to outsource their IT functions in order to focus their efforts and capitals on core-competencies thus reducing costs and improving quality of their IT services. While the client's sourcing decisions and the client-service provider relationship have been investigated in literature, the service provider's perspective has rarely been studied. Since the outsourcing organization loses the direct control of information system, maintenance of adequate level of security is a fundamental problem in outsourcing. This study focus on various aspects of information security in IT outsourcing that must be addressed by Iranian service providers, but attention will be focused on importance of physical security, personnel related security issues and business continuity planning. There are several objectives for this study. This study firstly attempts to explore the IT outsourcing activities of Iranian service providers. Secondly, is to investigate the service provides' practices in terms of physical security, personnel related security issues and business continuity planning. This study further examines physical security, personnel related issues, business continuity planning and the relevancy of those factors with best practices of information security implementation. IT managers and IT executives of service provider companies are the targeted respondents. There are three phases in the design of the study. The initial phase is preliminary study where interviews are conducted. This is done to probe IT outsourcing practices in Iran from perspective of service provider. In the second phase, which is the main phase, questionnaires are distributed. Subsequently, interviews are conducted which involves purposeful sampling method. This is embarked in order to derive a more comprehensive conclusion.

ABSTRAK

Kebanyakan organisasi kini telah mengenalpasti kemungkinan mengambil perkhidmatan luar (*outsourcing*) bagi melaksanakan fungsi IT di organisasi mereka. Ini membolehkan organisasi tersebut lebih menumpukan usaha dan modal kearah perkhidmatan yang lebih utama sekaligus mengurangkan kos dan meningkatkan kualiti perkhidmatan IT di organisasi mereka. Berdasarkan penyelidikan yang dijalankan, kajian dari sudut penyedia-perkhidmatan adalah amat kurang dijalankan berbanding kajian terhadap hubungan diantara pelanggan serta penyedia-perkhidmatan. Memandangkan organisasi perkhidmatan luar tiada kawalan terus terhadap sistem maklumat, menyediakan kawalan keselamatan yang berpatutan merupakan masalah utama bagi perkhidmatan luaran. Penyelidian ini bertujuan untuk mengenalpasti aktiviti-aktiviti yang dijalankan oleh penyedia-perkhidmatan yang terdapat di Iran dan respondent utama adalah pengurus dan pegawai IT yang terdapat di organisasi tersebut. Penyelidikan ini bertujuan mengkaji beberapa perkara berkaitan keselamatan maklumat bagi perkhidmatan luar yang perlu diambil kira oleh penyedia-perkhidmatan yang terdapat di Iran. Tujuan penyelidikan ini adalah bagi mengkaji secara terperinci amalan perkhidmatan yang disediakan oleh penyedia-perkhidmatan dari segi keselamatan fizikal, keselamatan individu dan rancangan perkhidmatan yang berterusan bagi mengenalpasti amalan terbaik bagi pelaksanaan keselamatan maklumat. Terdapat tiga fasa dalam melaksanakan penyelidikan ini dimana fasa pertama adalah bertujuan untuk memahami dengan lebih mendalam masalah amalan perkhidmatan luar IT di Iran dari pandangan penyedia-perkhidmatan. Maklumat yang diperolehi adalah melalui temubual. Phasa kedua pula dijalankan secara meninjau (survey) dimana soalan-soalan akan diberikan kepada para responden terpilih di organisasi tersebut. Seterusnya, pada peringkat akhir, temubual terhadap respondent akan dijalankan bagi mendapat penyelesaian yang lebih menyeluruh.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Overview

Growth of Information Technology (IT) outsourcing has been on upward trend since 90's and still is going on. The growth of outsourcing is mainly attributed to its supposed benefits; improve strategic focus and structural change, generally hyped by IT service provider press release or publications (Linder, 2004). A report by Gartner Group (2005) indicates that worldwide spending in IT outsourcing will rise from US$193 billion in 2004 to US$260 billion in 2009.

The underlying concept of IT outsourcing is the acquisition of services and/or products, through continuous interactions between parties to the agreement; may it be temporary or designated within an agreed length of time (Hirschheim and Lacity, 2000).

IT outsourcing is a perfect opportunity for clients and service providers to achieve their business approaches. However, lack of information security aspects would impede the IT outsourcing in meeting the objectives. Failure to understand, implement and maintain comprehensive information security in IT outsourcing by service providers may put the clients exposed to threats. Hence, there is a need for look at information security in IT outsourcing from service providers perspective.

1.2 Background of the Problem

IT outsourcing has been usually 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, 1993a).

Nevertheless, a particular attention to information security in outsourcing is a need. Traditionally, only non-strategic systems have been outsourced. This is, anyhow, changing (Rao et al., 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 are adequate when outsourcing noncritical systems, but when the importance of outsourced systems increases, more convincing provision of security of service providers is required (Kajava and Viiru, 1996).

1.3 Problem Statement

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). As long as the responsibility of enforcement of information security is transferred to the service provider, the adequate level of information security must be considered by service provider. The important information security objective for an outsourced system is maintenance of the security as it was when systems were operated internally. Hence, it is very critical that organizations make sure that service providers have adequate security measures in place (Khalfan, 2004). As Levina and Ross (2003) noted, the client's outsourcing decisions and the client-service provider relationship have been examined in IT outsourcing literature. However, the service

provider's perspective has hardly been explored. According to British Standard (1999), information security implementation refers to preservation of:

- Confidentiality: ensuring that information is accessible only to those authorized to have access.
- Integrity: safeguarding the accuracy and completeness of information and processing methods.
- Availability: ensuring that authorized users have access to information and associated assets when required.

Information security covers both data security and business recovery planning (Lee, 1995). The former aims to ensure the integrity and privacy of data owned by the organization, whereas the latter aims to include measures which ensure the rapid restoration of normal business operations in case of an occurrence of IT-related problems (e.g. infection by computer virus, destruction of data, sudden outage of the IT function) (Khalfan, 2004).

In addition, personnel related security issues are the other subjects that must be considered by service providers in order to implementation of information security. Hence, a study on the information security aspects of outsourced IT projects towards best practices is timely as there is lack of empirical study, particularly in Iran. In contrast, this proposed study examines the matter from the service provider perspective.

1.4 Project Aim

The aim of this research is to identify critical information security factors and study the issue of how service providers implement the information security requirements for IT outsourcing in both technical and non-technical aspects and control enforcement of these requirements.

This study focus on various aspects of information security in IT outsourcing that must be measured by service provider, but attention will be focused on

importance of physical security, personnel related security issues and business continuity planning in IT outsourcing and duties and responsibilities of service provider to provide those factors. Specific issues related to IT outsourcing include the client/service provider relationship, types of outsourcing and factors best practices of IT outsourcing are also another objectives of this research.

1.5 Project Objectives

Questionnaire will be used as quantitative method and semi-structured interviews will be used to collect the qualitative data in order:

- To explore the IT outsourcing activities of Iranian service providers.
- To investigate the IT service providers' information security concerns in terms of physical security, personnel related security issues, business continuity planning towards best practices of information security implementation.
- To develop a framework regarding the best practices of information security implementation.
- To examine the relevancy of physical security, personnel related security issues and business continuity planning with best practices of information security implementation.

1.6 Project Scope

- The scope of this study covers information security concerns in IT outsourcing projects in Iran from the perspective of service provider.
- Sixty five Iranian private companies will be selected to participate in the investigation (all the organizations are service provider).
- Questionnaire and semi-structured interview are the methods of collecting data.

1.7 Summary

The chapter begins with an overview of the study, followed by background of the problem. Subsequently, problem statement was described and project aims and objectives were defined. The next chapter presents the review of IT outsourcing literature.

REFERENCES

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

Barthélemy, J. (2003). The seven deadly sins of outsourcing. *Academy of Management Executive*, 17(2), 87–100.

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

Benbasat, I., Goldstein, D.K., and Mead, M. (2002). *The case research strategy of information systems*. In: Myers, M. D. and Avision D. *Qualitative Research in Information Systems*. (79-100). Sage Publications.

British Standard, Part 1 (1999). Information security management.

British Standards Institute (1993). *BS 7799: Code of Practice for Information Security Management (CoP)*. London: British Standards Institute.

Canavan, S. (2003). An Information Security Policy Development Guide for Large Companies. SANS Institute.

Casale, F. (2001). IT Outsourcing: The State of the Art. The Outsourcing Institute, *IT Index*. 2001.

Ceraolo, J. P. (1996). Penetration testing through social engineering. *Information Systems Security*. 4(4).

Chen, L. and Soliman K. S. (2002). Managing IT outsourcing: a value-driven approach to outsourcing using application service providers. *Logistics Information Management*. 15(3), 180-191.

Chen, Q. and Lin, B. (1998). Global outsourcing and its managerial implications. *Human Systems Management*. 17(2), 109-114.

Ching, C., Holsapple, C. W. and Whinston, A. B. (1996). Toward IT support for coordination in network organizations. *Information & Management*. 30(4), 179-199.

Clark, T. D., Zmud, R. W. and McCray, G. E. (1995). The outsourcing of information services: transforming the nature of business in the information industry. *Journal of Information Technology*. 10, 221-237.

Clott, C. B. (2004). Perspectives on global outsourcing and the changing nature of work. *Business and Society Review*. 109(2), 153–170.

Conrath, E. J. (1999). *Structural Design for Physical Security: State of the Practice*. ASCE Publications.

Creswell, J. W. (2003). *Research design: qualitative, quantitative, and mixed methods approaches*. (2th ed.). Sage Publications.

De Looff, L. (1995). Information Systems Outsourcing Decision Making: A Framework, Organizational Theories and Case Studies. *Journal of Information Technology*, 10, 281-297.

Denning, D. E. (1999). *Information Warfare and Security*. USA: ACM Press.

Desman, M. B. (2002). *Building an IS security Awareness Program*. USA: Auerbach Publications.

Dhillon, G. and Backhouse, J. (2001). Current Directions in IS Security Research: Towards Socio-Organizational Perspectives, *Information Systems Journal*, (11), 127-153.

Dilger, K. A. (2000). Application service providers: healthy growth foreseen for an already diverse solution model. *Manufacturing Systems*. 76-8.

Doherty, N. F. (2005). Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis. *Information Resources Management Journal*. 18(2), 21-39.

Dube, L., and Pare, G. (2003). Rigor in information systems positivist case research: Current practices, trends, and recommendations. *MIS Quarterly*. 27(4), 597-636.

Fink, A. (1995). *The Survey Handbook*. SAGE Publications.

Forcht, K. A., Pierson, J.K. and Bauman, B. M. (1988). Developing awareness of computer ethics. *Proceedings of the ACM SIGCPR conference on management of information systems personnel*.

Fowler, F. J. (2002). *Survey Research Methods*. (3th ed.). Sage Publication.

Furnell, S., Sanders, P. W. and Warren, M. J. (1997). Addressing IS security training and awareness within the European healthcare community. *Proceedings of Medical Informatics Europe '97*.

Galliers, R. D. and Land, F. F. (2002). *Choosing appropriate information system research methodologies*. In: Myers, M. D. and Avison, D. *Qualitative Research in Information Systems*. (13-17). Sage Publications.

Gartner Group. (2005). Forecast: IT Outsourcing, Worldwide, 2004-2009 Update, Stamford, CT.

Gattiker, E. (2004). *The information security dictionary*. Springer Publications.

Gomzalez, R., Gasco, J. and Llopis, J. (2005). Information systems outsourcing risks: a study of large firms. *Industrial Management & Data Systems*. 105(1), 45-62.

Hackney, R. and Hancox, M. (2000). *IS/IT Outsourcing: Conceptualizing Practice and Perception, Business Information Technology Management Alternative and Adaptive Futures*, Macmilan Press.

Hanifzadeh, P., Tabatabai, M. R. and Hosseini, S. A. A. (2006). Identify the effective factors to select the appropriate form of collaboration between one company and other companies in information technology industry of Iran. Faculty member of Industrial Management, Department of Industrial Management, School of Management and Accountancy, Allameh Tabataba'ee University (ATU).

Hermann, D. B. P. (2008). *When Disaster Strikes - A Guideline to Business Continuity Awareness*. GRIN Verlag.

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

Hirschheim, R., and Lacity, M. (2000). The myths and realities of information technology in-sourcing. *Communications of the ACM*, 43(2), 99-107.

Ismail, Z., Hussin, H., Suhaimi, M. A. and Abdul Karim, N. (2005). Knowledge sharing role in IT outsourcing. *International Conference on Knowledge Management (ICKM)*. 7-9th July 2005. Putra World Trade Centre (PWTC), Kuala Lumpur, Malaysia.

I.S.O. (2001). Information technology: code of practice for information security management. London: British Standards Institution

Ismail, Z. (2007). *IT Outsourcing Practices in Malaysia: Service Quality, Partnership Quality and Collectivism towards Outsourcing Success*. Doctor Philosophy. International Islamic University Malaysia.

Jones, A., Kovacich, G. L. and Luzwick, P.G. (2002) *Global Information Warfare*. Washington: Auerbach.

Kajava, J. and 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*. 20 May 1996. Pythagorean, Samos, Greece.

Khalfan, A. M. (2004). Information security considerations in IS/IT outsourcing projects: a descriptive case study of two sectors. *International Journal of Information Management*. 24(1). February 2004, 29-42.

Koh Ser Mui, A. (2003). *Investigation of IT/IS Outsourcing in Singapore*. Master thesis. Blekinge Institute of Technology, Sweden

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

Lacity, M. C. and Hirschheim, R. (1993b). Implementing information systems outsourcing: key issues and experiences of an early adopter. *Journal of General Management*. 19(1), 17-31.

Lacity, M. C. and Willcocks, L. P. (1995). Interpreting information technology sourcing decisions from a transaction cost perspective: findings and critique. *Accounting, Management & Information Technology*. 5(3), 203-244.

Lacity, M. C. and Willcocks, L. P. (1998). An empirical investigation of information technology sourcing practices: Lessons from experience. *MIS Quarterly*. 22(3), 363–408.

Lee, M. (1995). IT Outsourcing Contracts: Practical Issues for Management. Working Paper # 95/05, Information Systems Department, City University of Hong Kong.

Levina, N. and Ross, J.W. (2003). From the Vendor's Perspective: Exploring the Value Proposition in IT Outsourcing. *MIS Quarterly*. 27(3), 331-364.

Linder, J. C. (2004). Transformational outsourcing. *MIT Sloan Management Review*.

Li, H., King G., Ross M. and Staples, G. (2000). BS7799: A Suitable Model for Information Security Management, *America's Conference on Information Systems*, Electronic Commerce track, August 10–13, Long Beach, CA, Atlanta, GA: Association for Information Systems

Loh, L. and Venkatraman, N. (1992a). Diffusion of Information Technology Outsourcing: Influence Sources and Kodak Effect. *Information Systems Research*. 3(4), 334-358.

Loh, L., and Venkatraman, N. (1992b). Determinants of information technology outsourcing: a cross-sectional analysis. *Journal of Management Information Systems*. 9 (1), 7-24.

Ma, Q. and Pearson, J. M. (2005). ISO 17799: "Best Practices" in Information Security Management. *The Communications of the Association for Information Systems*. 15(32).

Mathieson, K. (1991). Predicting user intentions: comparing the technology acceptance model with the theory of planned behavior. *Information System Research*. 3(2), 173-191.

McFarlan, F. W. and Nolan, R. L. (1995). How to manage an IT outsourcing alliance. *Sloan Management Review*.36(2), 9-23.

Minoli, D. (1995). *Analyzing Outsourcing-Reengineering Information and Communication Systems*. McGraw-Hill

Myers M. D. and Avison, D. (2002). *Qualitative research in information systems*. (1th ed.). Sage Publications.

NIST Handbook (1995). *An Introduction to Computer Security*. USA: NIST special publications.

Noroozi, F., Ayazi, F., Abbasi, Z., Khodaband, H., Ahmadi, K. and Abbasi, K. (2006). Outsourcing of IT Services and Its Affect on IT Development in Iran. *Information and Communication Technologies*. 1(24), 316-321

Peltier, T. R. (2003). Preparing for ISO 17799. *Security Management Practices*. January-February, 21-28.

Pfleeger, C. P. and Pfleeger, S. L. (2003). *Security in Computing*.(3th ed.). Prentice Hall Professional Technical Reference.

Power, M. J., Desouza, K. C. and Bonifazi, C. (2006). *The Outsourcing Handbook: How to Implement successful Outsourcing Process*. Great Britain and the United States: Kogan Page.

Purser, S. (2004). *A practical guide to managing information security*. Artech House Publications.

Rao, R., Kichan, N. and Chaudhury, A. (1996). Information Systems Outsourcing. *Special Issue in Communications of the ACM*. 39(7), 27-54.

Schut, J. H. (1990). Insurance: Lessons from Disasters. *Institutional Investor*. October. p. 297.

Sekaran, U. (2003). *Research methods for business: a skill building approach*. (4th ed.). John Wiley and Sons.

Siegel, J. G. (2006). *Accounting Handbook*. (6th ed.). Barron's Educational Publications.

Slaughter, S. and Ang, S. (1996). Employment Outsourcing in Information Systems. *Communication of the ACM*. 39(7), 47-54.

Straub, D. W. and Welke, R. J. (1998). Coping with systems risk: security planning models for management decision making. *MIS Quarterly*. 22(4), 441-464.

Trauth, E. M. (2001). *The choice of qualitative methods in IS research*. In: Trauth, E. M. *Qualitative Research in IS: Issues and Trends* (1-19). IDEA Group Publishing.

Weingart, S. H. (2000). *Physical Security Devices for Computer Subsystems: A Survey of Attacks and Defenses. Cryptographic Hardware and Embedded Systems*. (45- 68). Berlin: Springer.

Wilson, M., Zafra, D. E. D., Picher, S. I., Tressler, J. D. and Ippolito, J. B. (1998). *Information Technology Security Training Requirements: A Role- and Performance-Based Model*. Gaithersburg: NIST Special Publication.

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

Wright, S. and Boschee, K. (2004). The offshore IT provider is under fire - will the US company be next? *Employee Relations Law Journal*. 30(1), 60–64.

Udo, G. G. (2000). Using analytic hierarchy process to analyse the information technology outsourcing decision. *Industrial Management & Data Systems*. 100(9), 421-429.

Von Solms, R. (1999). Information Security Management: Why Standards are Important. *Information Management & Computer Security*. 7(1), 50-57.

Zhang, Q. and Cao, M. (2002). Business process reengineering for flexibility and innovation in manufacturing. *Industrial Management & Data Systems*. 102(3), 146-52.