2007

A Conceptual model for Security Outsourcing

K. Samarasinghe
Deakin University

M. Warren
Deakin University

G. Pye
Deakin University

DOI: 10.4225/75/57b54ed4b8760
Originally published in the Proceedings of 5th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, December 4th 2007

A Conceptual model for Security Outsourcing

K.Samarasinghe, M.Warren and G.Pye,
School of Information Systems,
Faculty of Business and Law,
Deakin University,
Burwood, Victoria, Australia, 3217
mwarren@deakin.edu.au

Abstract
This research analyses the current literature on IT security outsourcing and the organisational attitudes towards this approach to determine the applicability of outsourcing IT security in a commercial environment. A conceptual model is developed as the main goal of research which provides guidance in the process of outsourcing IT security functions to a third-party security service provider. The research conducted has established a complete process for outsourcing IT security.

Keywords

Security Outsourcing and Modelling.

INTRODUCTION

Businesses and organisations value the consumer information stored in their information systems as it defines the needs of their customers and how they carry out their business. Even though these interconnected Information Systems (IS) have proven to be greatly useful in the domain of worldwide business, it had also left these IS's exposed to a variety of security threats which have evolved at the same pace as the innovations of Information Systems. This had opened up a whole new playground for malicious attackers giving them unauthorized access to valuable information easily (Ketler and Willems, 1999).
Outsourcing is the process of hiring a third party service provider to carry out a non-core business process of an organisation. This allows organisations to focus on their core business processes while a specialised third party takes care of their non-core business functions for a certain price (Ketler and Willems, 1999). The need for securing organisational information systems against evolving security threats is greater than ever. Attempts to facilitate this need have opened the way for outsourcing IT security functions as a manageable low cost solution (Deshpande, 2005). The paper proposes a conceptual model that could be used in making security management decisions.

WHAT IS OUTSOURCING?

Over the years, outsourcing had been defined in a few different ways. Even though most of us today instinctively think about software outsourcing when talking about outsourcing, it has its roots in other aspects of businesses such as human resources and manufacturing (Lee et al., 2003).
Oza et al. (2004) defines outsourcing as a decision taken by an organization to contract-out or sell an organization's software assets, people and/or activities to a third party supplier, who in exchange provides and manages assets and services for monetary returns over an agreed time period.
As identified by Laplante et al. (2004), IT organizations can outsource two basic types of work:

- explicit functions relevant to the operation of IT (for example software development and infrastructure);
- business operations that have direct impact on IT systems (for example, customer call centres and manufacturing).

Traditional outsourcing has focused upon business processes such as physical security, call centres or general IT processes. The next generation of outsourcing focused on specialisation areas within an organisation.

SECURITY OUTSOURCING

Security outsourcing is carried out in the form of Managed Security Services where security functions of an organisation are contracted out to Managed Security Service Providers (MSSP). Some definitions of security outsourcing are presented next.

According to Andress (2004) in managed security services, the security infrastructure of a client company is overseen or managed by a managed security service provider (MSSP).

Further more, Fenn et al. (2002) defines security outsourcing as it as the transfer of in-house IT security functions to a third party provider.

It is important to note here that security outsourcing is carried out in the form of providing a service. In general outsourcing, there is an end product (i.e. developed software) which concludes the outsourcing contract. However in contrast, security outsourcing is regarded as an ongoing management process as it provides services to the clients rather than a clearly defined end product.

Security outsourcing is an option not only for established businesses, but also for start-up organisations and those entering new lines of business. For established businesses, security outsourcing is economically driven. For start-up organisations or start-up market operations, there is the potential of time minimization by contracting an outsourcing organisation to provide those services immediately (CICA 2003).

IT Security Outsourcing Process

The main goal of the current research is to develop a conceptual model which provides decision making guidance throughout the process of IT security outsourcing. In order to achieve this, the key processes involved in the practice of IT security outsourcing must be identified. Through the analysis of the current key literature on the topic (Allen et al., 2003; Axelrod, 2004; Deshpande, 2005) and the observations of the researcher, the following five processes were identified as the critical steps involved in outsourcing IT security:

Step 1. Decide whether to outsource IT security or not;
Step 2. Select a Security Service Provider (SSP);
Step 3. Prepare a contract/ Service Level Agreement (SLA);
Step 4. Implement security outsourcing;
Step 5. Monitor Security Service Provider (SSP).

The following describes each of the five steps in turn that are critical to the outsourcing process and conceptual model:

Step 1: Decide Whether to Outsource IT Security or Not

This step encompasses the most critical decision involved in the whole security outsourcing process, which is determining whether an organisation should manage IT security in-house or to hire a third party security service provider to manage their IT security. Determining the areas of IT security which are vulnerable to security threats and carrying out a feasibility analysis by comparing costs, benefits and risks involved in security outsourcing are the key sub processes involved in this step. If outsourcing IT security is found to be feasible, the remaining steps of IT security outsourcing process are carried out. Otherwise, in-house IT security management is chosen.

Step 2: Select a Security Service Provider (SSP)

Once the feasibility of security outsourcing is established, the next logical step is to seek a viable SSP. Choosing the correct SSP is crucial for the successful implementation of security outsourcing. Even though a number of SSP selection criteria are identified throughout the literature (Allen et al., 2003; Axelrod, 2004; Deshpande, 2005), considerable thought should be given to a few critical factors. Preparing and sending out a Request for Proposal (RFP), evaluating SSP proposals against selection criteria and choosing the final SSP after a detailed analysis of short listed SSP's are the key sub processes involved in Step 2. Once a final SSP is selected, the next step involved in the process is to prepare and agree on a Service Level Agreement.

Step 3: Prepare a Service Level Agreement (SLA)

As with any kind of business relationship, contracts play a vital role in security outsourcing to establish the expectations of organisations and SSP's both. As highlighted previously, Service Level Agreements are commonly used in security outsourcing practices to ascertain the level of service quality expected from SSP's. Step 3 focuses on preparing a SLA, comparing the developed SLA with SSP's SLA and finally to evaluate and negotiate any further requirements or issues relating to the SLA.

Step 4: Implement Security Outsourcing

Once a SLA is developed and agreed on by both the organisation and the SSP, implementation of security services can be carried out. This process comprises of activities such as training, system testing, documentation etc. These activities must be carried out in a planned manner to ensure a successful and effective service implementation. Therefore, Step 4 mainly consists of identifying implementation issues, developing an implementation plan, conducting a post-implementation review and dealing with any issues identified with implementation. Upon completion of this step, the focus moves onto Step 5 which is monitoring SSP.

Step 5: Monitor Security Service Provider (SSP)

Step 5 can be considered as an ongoing process since regular monitoring of the SSP is essential to maintain service requirements and expectations established in Step 3. Regular reports and reviews on service performance prepared by the SSP must be compared against the SLA to verify that initial service level expectations are being met. Continuing with the same SSP and renewing the contract at the end of its term should solely depend on the SSP's ability to meet service levels. Therefore, Step 5 consists of the following sub processes: identifying issues with reporting requirements; evaluating service levels with essential criteria and determining the renewing or termination of SSP contract.

This framework formed the basis of the conceptual model described with the paper.

CONCEPTUAL MODEL BACKGROUND

There are numerous modelling techniques and languages available for representing complex processes and the decisions involved in them. In terms of the models used for the conceptual model, the authors focussed upon:

- flow charts;
- data flow diagrams.

The authors decided to use these modelling approaches in order to model the complexity related to outsourcing. The authors also decided not just to use a single approach but a hybrid approach containing both approaches.

Flow Charts

Chapin (1971) defines flow charts as,

"…a means of portraying, in graphic form, a sequence of specified operations performed on identified data."

Flowcharts have their origins in describing the representation of computer systems/programs and were used to communicate the operations of computer systems/ programs to people who are not familiar with computer use. Flow charts made it easy for the describer to explain the workings of such processes visually to the person who wants to learn them (Chapin, 1971).

Flowcharts are one of the earliest representation tools for physical systems and are still used very commonly to visually describe physical procedures (Hawryszkiwycz, 2001). Flowcharting technique uses a finite set of symbols to represent system components (i.e. physical hardware devices, information stores) as well as processes. When drawing flowcharts, physical system components are represented by flowchart symbols and then information flows between these components are marked according to the system (Hawryszkiwycz, 2001). The flowcharts can be used to model the logic behind the security outsourcing decisions.

Data Flow Diagrams (DFD)

As defined by Hofer et al. (1999), a data flow diagram is a graphical tool that allows analysts and users to depict the flow of data in information systems. The system that is being modelled can be either: physical; logical; manual or computer-based.

Data Flow Diagrams mainly use four kinds of symbols to represent system components which are processes, data stores, data flows and external entities. A key concept of data flow diagrams is their ability to decompose a process. A DFD for a process or a system starts off by drawing a Context Diagram. It is an overview of a system that shows the system boundaries, external entities that interact with the system, and the major information flows

interacting between the entities and the system (Hoffer et al., 1999). This context diagram is then decomposed to a Top-level DFD or Level 0 DFD. This level shows the major processes of the system along with the data flows and data stores at a high level of detail. Further, each of the processes identified in the top-level DFD can then be decomposed into more detailed DFD's (Hawryszkiwycz, 2001; Hoffer et al., 1999). The DFDs can be used to model the detail contained within any security outsourcing decisions.

CONCEPTUAL MODEL DIAGRAM MAPPING

Since the development of the conceptual model for outsourcing IT security was carried out using a hybrid modelling approach, a means for mapping between the steps of outsourcing IT security and the corresponding sections of the conceptual model. Table one lists all the steps involved in the conceptual model process of IT security outsourcing presented previously that was developed and each step is linked with a corresponding flowchart and DFD.

Steps Involved in IT security Outsourcing
1.0: Decide Whether to Outsource IT Security or Not
1.1 Risk Analysis
1.2: Determine Feasibility of In-house or Outsourced Security Management
1.2.1 Determine Costs of In-house Security Management
1.2.2 Determine Costs and Benefits of Outsourcing IT Security
1.2.3: Determine Main Risks of Outsourcing Security
1.2.4 Compare Costs, Benefits and Risks
2.0: Select a Security Service Provider
2.1: Prepare and Send Out a Request for Proposal (RFP)
2.2: Evaluate SSP Proposals
2.3: Negotiate and Clarify Any Issues or Requirements
3: Prepare and Evaluate a Service Level Agreement (SLA)
3.1: Prepare a SLA
3.2: Compare Client's SLA with Provider's SLA
3.3: Evaluate and Agree on SLA
4.0: Implement Security Outsourcing
4.1: Identify Implementation Activities
4.2: Identify Common Problems Relating to Implementation
4.3: Prepare an Implementation Plan
4.4: Carry Out Implementation According to Plan

4.5: Conduct a Post-implementation Review
4.6: Communicate Implementation Issues and Negotiate Resolutions
5.0: Monitor Security Service Provider
5.1: Analyse Regular Reviews and Reports
5.2: Identify Issues with Reporting and Modify Reporting Requirements
5.3 Verify If Terms of SLA are met
5.4: Make Necessary Changes to SLA and Notify SSP
5.5: Terminate Contract with SSP
5.6: Renew Contract with SSP and Review SLA

Table 1 – Mapping of security outsourcing steps

An example flowchart can be found in Figure 1 and an example DFD can be found in Figure 2. Each step of the model would have a corresponding flowchart and DFD.

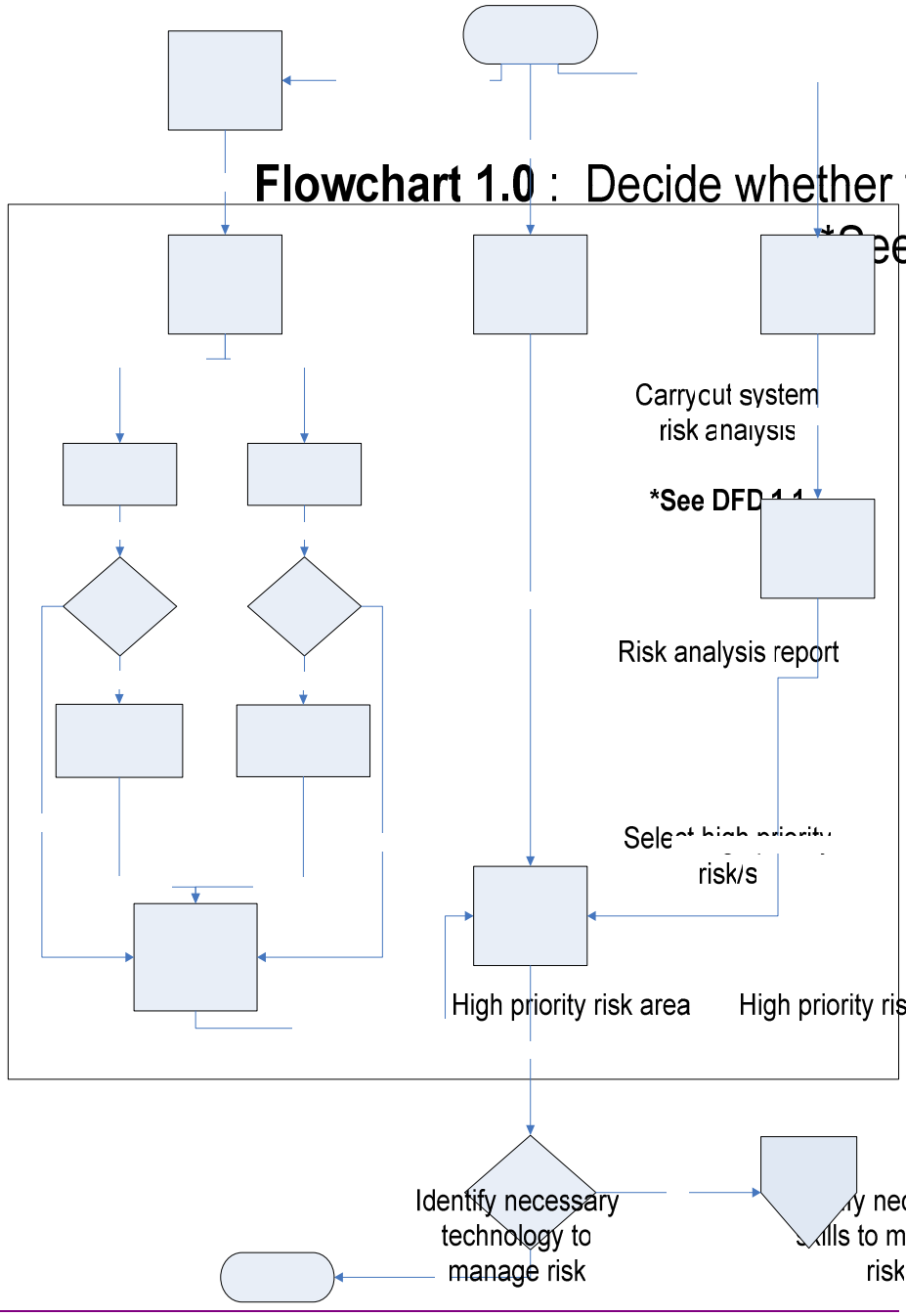

Figure 1: Example Flow Chart: Decide whether to outsource security or not

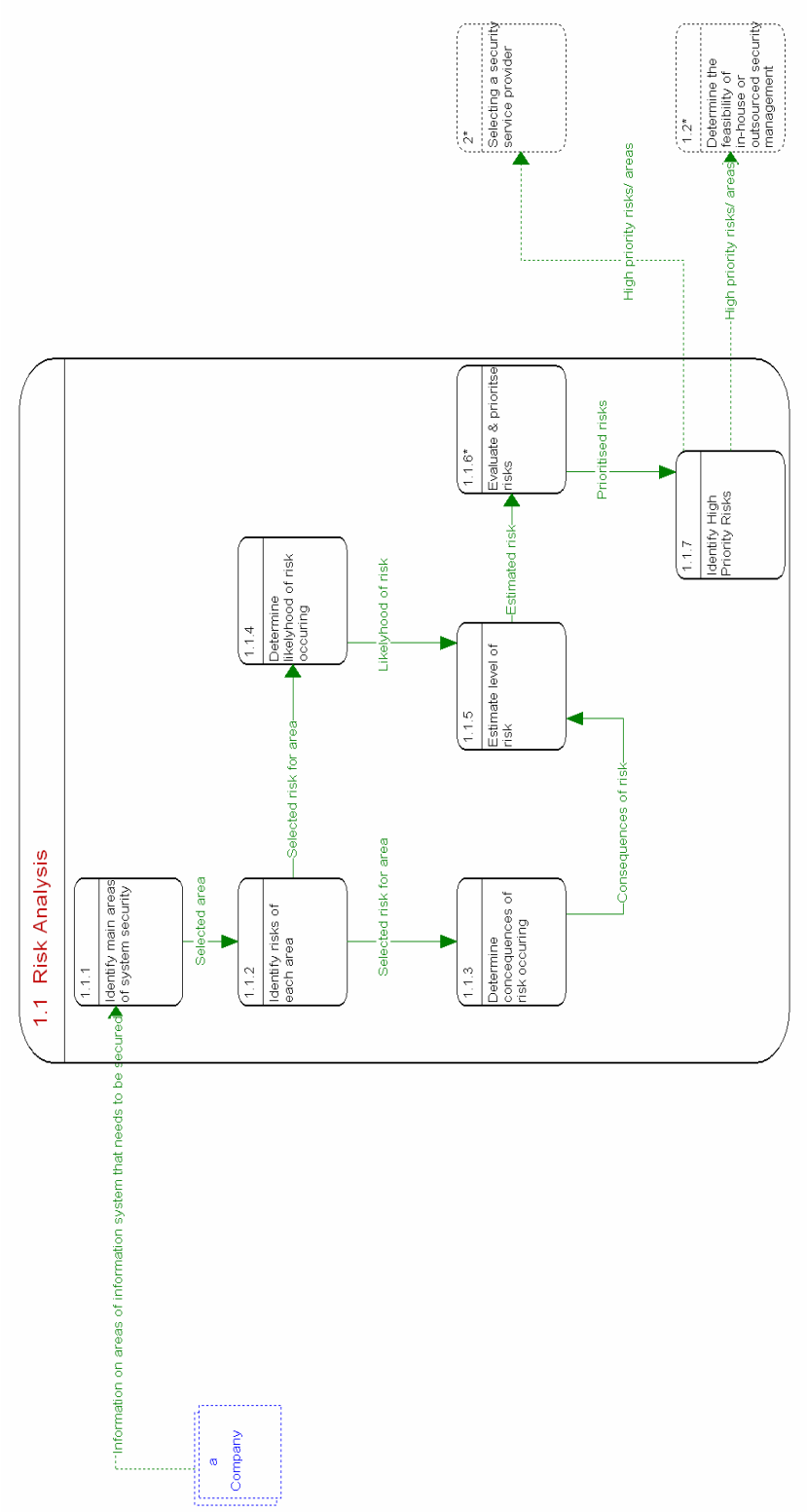

Figure 2: Example Data Flow Diagram

This section has provided a brief overview of the overall processes involved in outsourcing IT security and identified the five key steps in the process as well as describing the hybrid modelling approach.

CONCLUSION

This paper has provided a brief overview of the overall process involved in outsourcing IT security and identified five key steps. A conceptual model which guides an organisation through the process of outsourcing IT security has been presented. The paper presents the rationale and explanation of the conceptual model by dividing the key steps of security outsourcing into sub processes and explaining how the conceptual model addresses each of these sub processes in detail.

REFERENCES

Allen, J., Gabbard, D. and May, C. (2003), *Outsourcing Managed Security Services,* CERT Coordination Center.

Andress, A. (2004), *Surviving security: How to integrate people, process, technology.,* Auerbach Publications.

Axelrod, C. W. (2004), *Outsourcing Information Security,* Artech House, Norwood.

CICA (2003) Canadian Institute of Chartered Accountants, "Information technology Outsourcing", Toronto 2003, URL: http://www.cica.ca/multimedia/Download_Library/Research_Guidance/IT_Advisory_Committee/English/eIT outsourcing0204.pdf Accessed: October 4, 2004

Chapin, N. (1971), *Flowcharts,* Auerbach Publishers, USA.

Deshpande, D. (2005), *Managed security services: an emerging solution to security,* Proceedings of the 2nd annual conference on Information security curriculum development, ACM Press, Kennesaw, Georgia, pp.107-111.

Fenn, C., Shooter, R. and Allan, K. (2002), ' IT SECURITY OUTSOURCING - HOW SAFE IS YOUR IT SECURITY?' *Computer Law and Security Report,* Vol. 18, no. 2 pp.109-111.

Hawryszkiewycz, I. (1998), *Introduction to Systems Analysis and Design,* Prentice-Hall, New Delhi.

Hoffer, J. A., George, J. F. and Valacich, J. S. (1999), *Modern Systems Analysis and Design,* Addison Wesley Longman, Inc., USA.

Laplante, P. A., Costello, T., Singh, P., Bindiganavile, S. and Landon, M. (2004), 'The who, what, why, where, and when of IT outsourcing', *IT Professional,* Vol. 6, no. 1 pp.19-23.

Lee, J.-N., Huynh, M. Q., Kwok, R. C.-W. and Pi, S.-M. (2003), 'IT outsourcing evolution: past, present, and future', *Commun. ACM,* Vol. 46, no. 5 pp.84-89.

Ketler, K. and Willems, J. R. 1999, *A study of the outsourcing decision: preliminary results,* Proceedings of the 1999 ACM SIGCPR conference on Computer personnel research, ACM Press, New Orleans, Louisiana, United States, pp.182-189.

Oza, N., Hall, T., Rainer, A. and Grey, S. (2004) In *Proceedings of the 2004 ACM workshop on Interdisciplinary software engineering research,* ACM Press, Newport Beach, CA, USA, pp. 67-71.

COPYRIGHT