

MANAGED SECURITY SERVICES INDUSTRY IN SRI LANKA

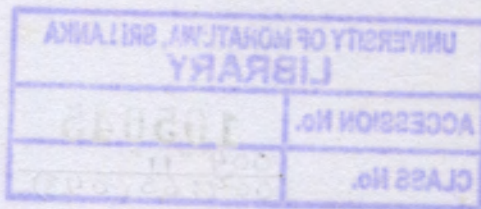
Dhammike Wishwanath Subasinghe Koralage

(08/9067)



University of Moratuwa, Sri Lanka.
Electronic Theses & Dissertations
www.lib.mrt.ac.lk

Dissertation submitted in partial fulfilment of the requirements for the degree of Master of Business Administration in Information Technology



Department of Computer Science & Engineering

University of Moratuwa
Sri Lanka

004 "11"
004:65 C0+3

February 2011

105045
(NO CD-ROM included)

University of Moratuwa



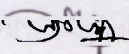
105045

105045

Declaration

I declare that this is my own work and this dissertation does not incorporate without acknowledgement any material previously submitted for a Degree or Diploma in any other University or institute of higher learning and to the best of my knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.

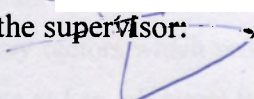
Also, I hereby grant to University of Moratuwa the non-exclusive right to reproduce and distribute my dissertation, in whole or in part in print, electronic or other medium. I retain the right to use this content in whole or part in future works (such as articles or books).

Signature: 

Date: 2011/02/05

The above candidate has carried out research for the MBA in IT Dissertation under my supervision.

UOM Verified Signature

Signature of the supervisor: 

Date: 07/02/2011

Abstract

Organizations outsource their IT security to qualified security service providers and it is commonly referred as managed security services (MSS). In contrast to the in-house approach in which organizations use their own resources to fulfil information security requirements, outsourcing of security provides many benefits as well as some risks to organizations. This research discusses the present standing of the MSS industry in Sri Lanka, in terms of several dimensions such as available services, MSS adoption, organizational perception and issues associated with the use of MSS. Furthermore, key drivers and inhibitors which affect the use of MSS in Sri Lankan organizations are also identified.

The results reveal that all of the MSS service categories are available in Sri Lanka, though the number of vendors offering MSS is somewhat limited. In terms of service offerings, Managed Firewall and Managed Policy Compliance services are the highly offered services while Security Consultancy services being the least offered service. On the other hand, Managed Email Content Filtering and Managed Firewall/VPN services are the mostly used services. Moreover, it can be seen that MSS is used by Sri Lankan organizations in general. The research has also identified that limited vendors, offering less services, unfulfilled MSS requirements and negative perception on MSS are key issues prevalent in the industry. In addition to the above findings, lack of security skills and perceived security enhancement by MSS are the key factors which promote the use of MSS while trust and hidden cost related issues are acting as key inhibitors for the use of MSS.

The entry of new vendors into the MSS industry, capitalizing on identified key drivers, strategies to deal with key inhibitors, proper identification of organizational requirements and effective marketing strategies to overcome the negative perception on MSS are recommended for MSSPs in order to develop the industry further. On the other hand, ensuring required level of security for information resources and practicing accepted risk mitigating approaches against the risk of trust and hidden cost related aspects are highly recommended for organizations. Moreover, in-depth inspection of available service offerings for a better selection of vendor is also recommended for organizations.

Key Words: MS, MSS, MSSP, Information Security, Information Security Outsourcing

Acknowledgement

This dissertation would not have been a reality without the support and cooperation from many individuals through various means. After a difficult and challenging effort, it is really a great pleasure to pay my gratitude to all of those who helped me to make this research study a success.

First and foremost, I would like to extend my sincere gratitude to my supervisor Dr. Chandana Gamage, Department of Computer Science & Engineering, University of Moratuwa, who provided continuous and invaluable guidance from the beginning to the end.

I further extend my sincere gratefulness to Prof. Kennedy Jayewardene, University of Sri Jayawardanapura, for allocating his time for me and giving invaluable guidance and opinions to fine-tune this study in the initial stages.

I also extend my sincere gratitude to Mrs. Vishaka Nanayakkara, head of the department of Computer Science & Engineering and all the other academic/non-academic staff of the department for giving their support and the guidance throughout the research.



University of Moratuwa, Sri Lanka.
Electronic Theses & Dissertations
www.lib.mrt.ac.lk

Further, my special thanks goes to my MBA batch mates, IBM colleagues and other friends who helped me a lot in order to make this effort a success.

Next, I would like to pay my sincere gratitude to all IT managers, vendors and ICT experts who allocated their time to fill the questionnaires and gave me an invaluable feedback. Without their input, this study will not be successful.

Lastly and most importantly, I would like to thank my wife Shaki, my parents and my sisters, for bearing up with me and constantly encouraging me. Without their help and encouragement, this endeavour would have been impossible.

Dhammike Wishwanath Subasinghe Koralage
MBA/IT 08/9067.

Table of Contents

Declaration.....	i
Abstract.....	ii
Acknowledgement	iii
List of Figures.....	viii
List of Tables	ix
List of Abbreviations	xi
CHAPTER 1 INTRODUCTION	1
1.1 Background and Motivation	1
1.2 Research Question	2
1.3 Research Objectives.....	3
1.4 Significance of the Study	4
1.5 Research Methodology.....	5
1.6 Nature & Form of Results.....	5
1.7 Structure of the Dissertation	6
CHAPTER 2 LITERATURE REVIEW	7
2.1 Introduction.....	7
2.2 Managed Security Services.....	8
2.3 Service Categories of MSS.....	9
2.4 Benefits of MSS.....	13
2.5 Risks Associated with MSS	16
2.6 Drivers and Inhibitors	19
2.6.1 Key drivers.....	19
2.6.2 Inhibitors	21
2.7 Service Selection for Outsourcing	22
2.8 Criterion for the Selection of an MSSP	24
2.9 MSS Adoption	25

2.10	Chapter Summary	26
CHAPTER 3	RESEARCH METHODOLOGY.....	27
3.1	Exploratory Study Approach	27
3.2	Descriptive Study Approach	32
3.2.1	Conceptual framework.....	32
3.2.1.1	Factors promoting MSS usage	33
3.2.1.2	Factors inhibiting MSS usage	34
3.2.1.3	Other factors influencing MSS usage	35
3.2.1.4	Summary of variables for data collection	37
3.2.2	Hypotheses development	39
3.2.3	Research design	42
3.2.3.1	Research instruments	42
3.2.3.2	Dimensions of variables.....	42
3.2.4	Sample design	45
3.2.4.1	Population	45
3.2.4.2	Sample size	47
3.2.5	Data collection	47
3.2.6	Methods of data analysis	49
CHAPTER 4	DATA ANALYSIS & DISCUSSION.....	50
4.1	Introduction.....	50
4.2	Reliability Analysis.....	50
4.3	Descriptive Analysis	51
4.3.1	Organizational response	52
4.3.2	MSS usage & requirements	56
4.3.2.1	MSS usage	56
4.3.2.2	Unfulfilled MSS requirements.....	58
4.3.2.3	Requirement to have SLAs & NDAs.....	59
4.3.3	Organizational perception on MSS.....	61
4.3.3.1	Limited services	61
4.3.3.2	Fulfilment of security outsourcing requirements.....	62
4.3.4	Descriptive analysis of variables	63

4.3.4.1	Level of information security skills	64
4.3.4.2	Perceived security enhancement	66
4.3.4.3	Need to focus on core business	68
4.3.4.4	Need for 24x7 support	70
4.3.4.5	Need for regulatory compliance.....	73
4.3.4.6	Trust related issues.....	75
4.3.4.7	Ownership related issues.....	77
4.3.4.8	Dependency related issues	79
4.3.4.9	Hidden cost related issues	81
4.3.4.10	MSS awareness	83
4.3.5	Analysis of MSSPs & service offerings.....	85
4.3.5.1	Form of the MSSP	85
4.3.5.2	Service offerings	86
4.3.5.3	SLA & NDA	87
4.4	Analysis of Hypotheses.....	88
4.4.1	Testing hypothesis 1	88
4.4.2	Testing hypothesis 2	89
4.4.3	Testing hypothesis 3	90
4.4.4	Testing hypothesis 4	91
4.4.5	Testing hypothesis 5	92
4.4.6	Testing hypothesis 6	92
4.4.7	Testing hypothesis 7	93
4.4.8	Testing hypothesis 8	94
4.4.9	Testing hypothesis 9	95
4.4.10	Testing of hypothesis 10	96
4.4.11	Testing hypothesis 11	98
4.4.12	Testing hypothesis 12	99
4.5	Overall Results of the Study	100
4.5.1	Available MSS	100
4.5.2	MSS usage	101
4.5.3	Organizational MSS requirements	102
4.5.3.1	Unfulfilled MSS requirements.....	102
4.5.3.2	SLA/NDA requirements	102

4.5.4	Organizational perception.....	102
4.5.5	Issues related to MSS.....	103
4.5.6	Key drivers for MSS.....	104
4.5.7	Key inhibitors for MSS.....	105
4.6	Chapter Summary.....	105
CHAPTER 5 CONCLUSIONS AND RECOMMENDATIONS.....		107
5.1	Conclusions.....	107
5.2	Recommendations.....	110
5.2.1	For MSSPs.....	110
5.2.2	For organizations.....	112
5.3	Limitations of the Study.....	113
5.4	Future Research Directions.....	114
References.....		116
Appendix A.....		119
A.1	Questionnaire for Organizations.....	119
A.2	Questionnaire for MSSPs.....	128
A.3	Pre-survey Questionnaire for Organizations.....	132
A.4	Pre-survey Questionnaire for MSSPs.....	137

List of Figures

Figure 2.1: MSS adoption by service category	25
Figure 3.1: Conceptual framework for inferential analysis	35
Figure 4.1: Industry/sector wise distribution of responses	52
Figure 4.2: Industry/sector wise distribution of responses with normal curve	53
Figure 4.3: Industry/sector wise distribution of responses in a pie-chart	54
Figure 4.4: Distribution of employee head count of the organizations responded	55
Figure 4.5: Distribution of designation category of respondents.....	56
Figure 4.6: MSS adoption in terms of number of services used	57
Figure 4.7: MSS adoption by service category	58
Figure 4.8: Unfulfilled MSS requirement	59
Figure 4.9: Histogram of level of information security skills.....	66
Figure 4.10: Histogram of perceived security enhancement	68
Figure 4.11: Histogram of need to focus on core business	70
Figure 4.12: Histogram of need for 24x7 support.....	72
Figure 4.13: Histogram of need for regulatory compliance.....	74
Figure 4.14: Histogram of trust related issues	76
Figure 4.15: Histogram of ownership related issues.....	78
Figure 4.16: Histogram of dependency related issues	80
Figure 4.17: Histogram of hidden cost related issues	82
Figure 4.18: Histogram of MSS awareness	84
Figure 4.19: Form of the MSSP	85
Figure 4.20: Number of vendors offering each MSS.....	86

List of Tables

Table 2.1: List of managed security services,.....	12
Table 3.1: Operational definition of variables	37
Table 3.2: Variables and dimensions	43
Table 3.3: Population, confidence level, confidence interval and sample size.....	48
Table 4.1: Case processing summary for the entire data set.....	50
Table 4.2: Reliability statistics for the entire data set.....	51
Table 4.3: Reliability statistics for individual variables	51
Table 4.4: One-sample statistics of SLA/NDA requirement	60
Table 4.5: One-Sample test of SLA/NDA requirement.....	60
Table 4.6: One-sample statistics of perception on limited service offerings.....	61
Table 4.7: One-sample test of perception on limited service offerings	61
Table 4.8: One-sample statistics of perception on possibility to fulfil security outsourcing requirements.....	62
Table 4.9: One-sample test of perception on possibility to fulfil security outsourcing requirements.....	63
Table 4.10: Descriptive statistics of level of information security skills.....	64
Table 4.11: Frequency analysis of level of information security skills	65
Table 4.12: Descriptive statistics of perceived security enhancement	67
Table 4.13: Frequency analysis of perceived security enhancement.....	67
Table 4.14: Descriptive statistics of need to focus on core business	69
Table 4.15: Frequency analysis of the need to focus on core business.....	69
Table 4.16: Descriptive statistics of need for 24x7 support.....	71
Table 4.17: Frequency analysis of need for 24x7 support	71

Table 4.18: Descriptive statistics of need for regulatory compliance.....	73
Table 4.19: Frequency analysis of need for regulatory compliance	74
Table 4.20: Descriptive statistics of trust related issues	75
Table 4.21: Frequency analysis of trust related issues.....	76
Table 4.22: Descriptive analysis of ownership related issues.....	77
Table 4.23: Frequency analysis of ownership related issues	78
Table 4.24: Descriptive analysis of dependency related issues	79
Table 4.25: Frequency analysis of dependency related issues.....	80
Table 4.26: Descriptive analysis of hidden cost related issues.....	81
Table 4.27: Frequency analysis of hidden cost related issues	82
Table 4.28: Descriptive analysis of MSS awareness	83
Table 4.29: Frequency analysis of MSS awareness.....	84
Table 4.30: Correlation between MSS usage and the level of security skills.....	88
Table 4.31: Correlation between MSS usage and perceived security enhancement..	89
Table 4.32: Correlation between MSS usage and need for 24x7 support.....	90
Table 4.33: Correlation between MSS usage and need to focus on core business	91
Table 4.34: Correlation between MSS usage and need for regulatory compliance...	92
Table 4.35: Correlation between MSS usage and trust related issues	93
Table 4.36: Correlation between MSS usage and ownership related issues.....	94
Table 4.37: Correlation between MSS usage and dependency related issues	95
Table 4.38: Correlation between MSS usage and hidden cost related issues	96
Table 4.39: One-sample statistics of level of information security skills.....	97
Table 4.40: One-sample test of level of information security skills.....	97
Table 4.41: One-sample statistics of MSS awareness	98
Table 4.42: One-sample test of MSS awareness.....	98



University of Moratuwa, Sri Lanka
 Electronic Theses & Dissertations
www.lib.mrt.ac.lk

Table 4.43: One-sample statistics of MSS usage.....	99
Table 4.44: One-sample test of MSS usage	99

List of Abbreviations

Abbreviation	Description
ASP	Application Service Provider
CIO	Chief Information Officer
FW	Firewall
ICT	Information and Communication Technology
IDS	Intrusion Detection Service
IPS	Intrusion Prevention Service
ISO	International Standards Organization
ISP	Internet Service Provider
IT	Information Technology
MS	Managed Security
MSS	Managed Security Service
MSM	Managed Security Monitoring
MSSP	Managed Security Service Provider
MSSPs	Managed Security Service Providers
NDA	Non Disclosure Agreement
SLA	Service Level Agreement
SLICTA	Sri Lanka Communication and Technology Association
SOC	Security Operations Centre
VPN	Virtual Private Network

