INVESTMENT STRATEGY FOR INFORMATION SECURITY IN GOVERNMENT SECTOR ORGANIZATIONS IN SRI LANKA

Rohana Chaminda Akmeemana Palliyaguru

(109070J)

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

Master of Business Administration
in Information Technology

Department of Computer Science & Engineering

University of Moratuwa
Sri Lanka

February 2012

INVESTMENT STRATEGY FOR INFORMATION SECURITY IN GOVERNMENT SECTOR ORGANIZATIONS IN SRI LANKA

Palliyaguru R.C.A.

(109070J)

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

The Dissertation was submitted to the Department of Computer Science & Engineering of the University of Moratuwa in partial fulfillment of the requirement for the Degree of Master of Business Administration.

Department of Computer Science & Engineering

University of Moratuwa
Sri Lanka

February 2012

DECLARATION

“I certify that this thesis does not incorporate without acknowledgement any material previously submitted for a degree or diploma in any university to the best of my knowledge and belief it does not contain any material previously published, written or orally communicated by another person or myself except where due reference is made in the text. I also hereby give consent for my dissertation, if accepted, to be made available for photocopying and for interlibrary loans, and for the title and summary to be made available to outside organizations”

……………………………… ……………………………..

Signature of the Candidate Date

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

To the best of my knowledge, the above particulars are correct.

…………………………….

Supervisor

(Dr. Shantha Fernando)

ABSTRACT

As most of the government organizations in Sri Lanka are moving towards providing connected on-line services to the citizens, the growing number of defects in information system and illegal invasion is pushing them to invest more on information security.

Information security problems are as old as information exchange. But the decisions about the respective defense measures are mostly still taken based on heuristics and experience. There is a lack of general and reliable information security strategy that a government organization could use in order to make such decisions. As a result of that the information security status of government organizations are not at a level where it should be.

Therefore it is very important to have a acceptable information security strategy for information security investments in government sector organizations.

In general, before spending money on a product or service, decision makers want to know that the investment is financially justified. Information security is no different, it has to make business sense.

Typically it is necessary to use very robust analysis techniques to determine how best to spend resources in order to increase revenue and decrease costs or losses. But in the case of information security investments there is a lack of key performance and evaluation metrics to take proper investment decisions.

Using a case study approach, series of interviews were conducted with five government organizations in a variety of sectors in order to understand their investment and implementation strategies for information security. Also the general IS awareness of decision-makers and users are evaluated which has a major impact on the investment strategy of any organization.

This paper proposes an IS investment strategy by providing strategic approach for each stage in the investment life cycle: Select, Control and Evaluate.

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

ACKNOWLEDGEMENT

I would like to extend sincere thanks to my research supervisor, Dr. Shantha Fernando for his disciplined,encouraging guidance and providing a long term vision to the study.

The support and guidance given by our MBA course coordinator Ms. Vishaka Nanayakkara throughout this research process is highly appreciated.

My special thank to Dr. Raj Prasanna for giving me proper understanding about some problematic areas which I found during the research process.

I would also like to thank the Head of the Department of Computer Science and Engineering and all the staff members for the guidance and feed back given to me for making this research a success.

My special thank to COO of Sri Lanka CERT , Mr. Lal Dias and Director re-engineering government ICTA, Mr. Wasantha Deshapriya for supporting me in this endeavor.

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

I would like to thank the Director Generals, Commissioners, CIOs, and members of the management of government organizations who contributed to my research by providing me with their valuable time amongst busy working schedules, without which my objectives would not have been fulfilled.

Finally I would like to thank all of my batch mates of the MBT-IT 2010 batch.

Palliyaguru R.C.A.
MBA/IT/10/9070J

TABLE OF CONTENTS

DECLARATION...i

ABSTRACT..ii

ACKNOWLEDGEMENT...iii

TABLE OF CONTENTS..iv

LIST OF FIGURES..viii

LIST OF TABLES...ix

LIST OF APPENDICES..x

ABBREVIATIONS..xiv

1 CHAPTER 1: INTRODUCTION..1

1.1 Background and Motivation..1

1.2 Problem Statement..2

1.3 Research Objectives..3

1.4 Significance of the Study...3

1.5 Limitations and Delimitations..4

2 CHAPTER 2 : LITERATURE REVIEW..5

2.1 Introduction..5

2.2 Reason for Invest in Information Security..6

2.3 Current Level of Investment..7

2.4 Costs of Security Failures 8

2.5 Common Problems for Invest in Information Security...............................10

2.6 Information Security Awareness and organizational learning.....................10

2.7 Investment for Information Security and Decision Makers..........................11

2.8 Information Security Investment Economic Models...................................13

2.9 Return on Information Security Investment..14

2.10 Strategic Approach for Information Security..16

2.11 Investment Management Process..17

3 CHAPTER 3 : RESEARCH METHODOLOGY & DESIGN...............................19

3.1 Introduction..19

3.2 Research Design..19

3.3 Research Approach..19

3.4 Research Strategy..20

3.5 Development of the Conceptual Framework..22

3.6 The Conceptual Framework..23

3.6.1 Descriptions for Concepts 26

3.6.1.1 Select...26

3.6.1.2 Control...31

3.6.1.3 Evaluate...32

3.6.1.4 Information Security Awareness and Responsibilities..........................33

3.6.2 Source of Selected Parameters..35

4 CHAPTER 4 : DATA COLLECTION...37

4.1 Data Collection Methods...37

4.1.1 Interviews...37

4.1.2 Focus Groups...38

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

4.1.3 Observation..38
4.1.4 Collection of Documented Material...38
4.1.5 Collection of Narrative...39
4.1.6 Open Ended Questions in Questionnaires...39
4.2 Selected Method for Data Collection...39
4.2.1 Sampling 39
4.2.2 Iterative Data Collection...41
4.3 Interview Guide Design Methodology...43
5 CHAPTER 5: DATA ANALYSIS..46
5.1 Case Study Data Analyzing Techniques...46
5.1.1 Pattern Matching..46
5.1.2 Explanation Building...47
5.1.3 Logic Models..47
5.1.4 Time-Series Analysis..47
5.1.5 Cross-Case Synthesis...48
5.2 Selected Data Analyzing Technique...48
5.3 "Select" Dimension..48
5.3.1 Inputs...48
5.3.1.1 Continuous Monitoring...48
5.3.1.2 Plan of Action and Milestones...49
5.3.1.3 External Evaluations...49
5.3.1.4 Specialist IS Advise...50
5.3.1.5 New Mandates...50
5.3.1.6 Evolving Threats..51
5.3.1.7 Information Security Policy..51
5.3.1.8 Other Considerations..51
5.3.2 Prioritize..52
5.3.2.1 Prioritization Scheme..52
5.3.2.2 Prioritization Stakeholders...52
5.3.2.3 Prioritization Criteria and Weights..53
5.3.2.4 Risk Assessment and Ranking...53
5.3.3 Decision..54
5.3.3.1 Decision Stakeholders...54
5.3.3.2 Awareness on Information Security Investment...........................55
5.3.3.3 Funding for IS..56
5.4 "Control" Dimension...56
5.4.1 Consistently Monitoring the Projects...56
5.4.2 Involving the Right People..57
5.4.3 Documenting all Actions and Decisions..57
5.4.4 Update Analyses on each Investment's Costs and Benefits...............57
5.4.5 Assess Milestones Completion...57
5.4.6 Analyze Goal Achievement..58
5.5 "Evaluate" Dimension...58
5.5.1 Compare with Earlier Projections...58
5.5.2 Continuity and Adjustments...59

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

5.5.3 Lessons Learned..59
5.6 "IS Awareness and Responsibilities" Dimension....................................60
5.6.1 General Awareness on IS..60
5.6.2 Awareness on IS Policy...61
5.6.3 Incident Reporting Mechanism...62
5.6.4 IS Responsibilities of Staff Levels..62
5.7 Current Overall Status of Investment Strategy.......................................63
6 CHAPTER 6 : RECOMMENDATIONS AND CONCLUSIONS......................................66
6.1 Recommendations for "Select" Dimension...67
6.1.1 Inputs...67
6.1.1.1 Continuous Monitoring..67
6.1.1.2 Plan of Action and Milestones..67
6.1.1.3 External Evaluations...68
6.1.1.4 Specialist IS Advise...68
6.1.1.5 New Mandates...68
6.1.1.6 Evolving Threats...69
6.1.1.7 Information Security Policy..69
6.1.1.8 Other Considerations...69
6.1.2 Prioritize...70
6.1.2.1 Prioritization Scheme..70
6.1.2.2 Prioritization Stakeholders...70
6.1.2.3 Prioritization Criteria and Weights...70
6.1.2.4 Risk Assessment and Ranking..71
6.1.3 Decision...71
6.1.3.1 Decision Stakeholders..71
6.1.3.2 Awareness on Information Security Investment..71
6.1.3.3 Funding for IS...72
6.2 Recommendations for "Control" Dimension..72
6.2.1 Consistently Monitoring the Projects..72
6.2.2 Involving the Right People..72
6.2.3 Documenting all Actions and Decisions...73
6.2.4 Update Analyses on each Investment's Costs and Benefits...............................73
6.2.5 Assess Milestones Completion..73
6.2.6 Analyze Goal Achievement..73
6.3 Recommendations for "Evaluate" Dimension...74
6.3.1 Compare with Earlier Projections..74
6.3.2 Continuity and Adjustments..74
6.3.3 Lessons Learned...74
6.4 Recommendations for "IS Awareness and Responsibilities" Dimension. 75
6.4.1 General Awareness on IS...75
6.4.2 Awareness on IS Policy..75
6.4.3 Incident Reporting Mechanism..75
6.4.4 IS Responsibilities of Staff Levels...76
6.5 Conclusion...76
REFERENCE LIST..77

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

APENDIX-I: Guide for the unstructured interview (Step 1)....................................82
APENDIX-II: Guide for the semi-structured interview (Step 2)..............................84
APPENDIX III: Collected Data...89

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

LIST OF FIGURES

Page

Figure 2-1: Security vs. costs chart 8
Figure 2-2: Diagram of Cyber Security Investment decisions Inputs and Outputs....13
Figure 3-1 : Inputs for conceptual framework...22
Figure 3-2: Investment management process..24
Figure 4-1 : Data collection methodology...42
Figure 5-1 : Current Status of Proposed Dimensions...65
Figure 6-1 : Complete Research Methodology..66

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

LIST OF TABLES

Page

Table 3-1: Parameter Mapping....................36
Table 4-1 : Sample selection....................40
Table 4-2 : Concept-Question mapping....................45
Table 5-1: Values for Parameters....................63
Table 5-2 : Current Status of Parameters....................64

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

LIST OF APPENDICES

Appendix Description Page

APENDIX-I : Guide for the Unstructured Interview (Step 1)....................................82

APENDIX-II : Guide for the Semi-Structured Interview (Step 2)............................84

APPENDIX III : Collected Data...89

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

ABBREVIATIONS

Abbreviation	Description
CD	Compact Disc
CIO	Chief Innovative Officer
ICT	Information and Communication Technology
ICTA	Information and Communication Technology Agency
IS	Information Security
PIR	Post implementation review
SLAS	Sri Lanka Administrative Service
VPN	Virtual Private Network

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