Role of the Boards and Senior Management within Formal, Technical and Informal Components: IS/IT Security Governance in the Malaysian Publicly Listed Companies

By

Nadianatra Musa
BSc (Hons.), Universiti Teknologi Malaysia (UTM), Malaysia, 2000
MSc (Information Systems), University of Tasmania, Australia, 2003

Submitted in fulfilment of the requirements for the Degree of
Doctor of Philosophy

School of Accounting and Corporate Governance
Faculty of Business
University of Tasmania

November, 2011

Declaration of Originality

This thesis contains no material which has been accepted for a degree by the University or any other institution, except by way of background information and duly acknowledged in the thesis, and to the best of the my knowledge and belief no material previously published or written by another person except where due acknowledgement is made in the text of the thesis, nor does the thesis contain any material that infringes copyright.

_____ _____

Nadianatra Musa Date

Statement of Authority of Access

This thesis may be made available for loan and limited copying in accordance with the Copyright Act 1968.

_____ _____

Nadianatra Musa Date

Statement of Ethical Conduct

The research associated with this thesis abides by the international and Australian codes on human and animal experimentation, the guidelines by the Australian Government's Office of the Gene Technology Regulator and the rulings of the Safety, Ethics and Institutional Biosafety Committees of the University.

_____ _____

Nadianatra Musa Date

Acknowledgements

I would like to express my gratitude to all those gave me the possibility to complete the thesis.

Foremost, I would like to express my sincere gratitude to my supervisors, Associate Professor Trevor Wilmshurst, Dr Gail Ridley, Dr Vishv Malhotra and Professor Bob Clift for the continuous support of my PhD study and research, for their patience, motivation, enthusiasm and immense knowledge. Their guidance helped me in all the time of researching and writing this thesis. I have worked with a number of people who contributed in assorted ways to the research, I gratefully thank them for their insightful comments, their willingness to share bright thoughts which were fruitful for shaping up my ideas and research. It was great to collaborate with you all.

Besides my supervisors, I would like to thank my employer, the Universiti Malaysia Sarawak (Unimas) and the Ministry of Higher Education Malaysia for being my sponsor and supporter throughout my PhD study.

I thank my research colleagues and friends in University of Tasmania, Lynne Gerke, Shaari, Hazianti, Andrew, Nahar, Mahdi, Shaz for sharing various thoughts at the office and many places.

Especially, I would like to convey my special thanks to my husband, Abdul Razak Abang Othman and my daughter, Dayang Mashitah Abdul Razak, who have always stood by me when I need them, always supported me all the time in my life. I owe my deepest gratitude to my parents Musa Bidin and Masnah Sahni, my siblings and all family members for their encouragement, patience and supporting me spiritually throughout my life.

I am indebted to my friends, Dayang Hanani Abang Ibrahim, Dr Kartinah Zen, Halikul Lenando, Nazim, Rosita, Yanti, Nehran, Mariatun, Sabri Samson, Anjung, Rafeah, Joyce and Roziah for creating such great friendships and for their stimulating support throughout my writing and research. I thank the Malay Tassie Society (Tasmania) and Malaysia Hall-Melbourne (Melbourne), for being supportive and caring friends.

Finally, I would like to thank everybody who was important for the successful realisation of the thesis, as well as expressing my apology that I could not mention them personally one by one.

Abstract

In IT governance, there are two types of responsibilities, first is IT value governance and second is IT risk governance. The primary objective of this study is to examine the second type of responsibility, IT risk governance and specifically looking into the involvement of the board, senior management and all management levels in IS/IT security.

Prior research has shown a lack of involvement by the board and senior management in understanding IS/IT security problems, unbalanced implementation of IS/IT security within the formal, technical and informal components and lack of internal controls application over IS/IT security. The gap found in this study has lead to the development of two major research questions, Research Question 1-In what way does the involvement of Boards and senior management impact on the implementation of IS/IT security governance? and Research Question 2-How can directing and monitoring actions in the technical, formal and informal components of IS/IT security governance in corporations be implemented effectively and efficiently? The two research questions have steered the development of the conceptual framework, the model of IS/IT security governance and the research methods.

The IS/IT security governance model is an extension of the conceptual framework, the model prescribes several areas relating to the elements of the three components, formal, technical and informal and component interactions (Relationship Type 1-Formal/Informal, Relationship Type 2-Formal/Technical and Relationship Type 3-Technical/Informal) within Malaysian Publicly Listed Corporations. The model suggests IS/IT security ought to be included within risk management and internal controls practices, through 'directing' and 'monitoring' actions and exclusively emphasises the supervision role and the relationship between the supervisor (giver) and the holder of responsibility. Because the nature of study is sensitive and confidential; the study has adopted a triangulation method. Data were collected using interviews and a mail survey as primary sources and website analysis as a secondary source. 12 interviews were conducted with CEOs, CIOs, other senior managers and IT manager from eight companies of Group A (Top) and Group B (Middle) across different industries. Despite a low response rate for the mail survey, the data have high validity as interviews and responses involved appropriate people in leading organisations in Malaysia from Group A(Top) and Group B(Middle)- high profit and large market capitalisation organisations and experienced senior managers. Content analysis over 210 annual reports of website data from Group A, Group B and Group C was conducted.

The data from interviews, survey and website analysis have supported the model of IS/IT security governance. The findings from the interview data are consistent with the elements of formal, technical and informal components and component interactions; risk management and internal controls over IS/IT security and 'directing' and 'monitoring' actions over IS/IT security are supported. The results of the survey have shown that the respondents had similar perspectives as the model. The website analysis revealed that two factors may determine IS/IT security governance, the group type and industry type.

Table of Contents

List of Tables

List of Figures