FRAMEWORK OF HUMAN BEHAVIOR TO MITIGATE THE INSIDER THREAT

JIHAD WAJEEH BADAWI

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

Faculty of Computer Science and Information Systems
Universiti Teknologi Malaysia

JANUARY 2013

I dedicate this project to my respected and beloved Parents, thank you
for the moral and financial support you've given me throughout my academic life.
To my respected supervisor, Dr. Norafida Binti Ithnin and friends,
thank you for your support, prayers, and advices.

ACKNOWLEDGEMENT

In the Name of Allah, most Gracious, most Merciful. I would like to be thankful to the almighty Allah who is the creator, protector of the whole universe and who gave me the strength to do this thesis work in time.

I sincerely give gratitude to my supervisor, Dr. Norafida Ithnin, for her support throughout the project, her patience and for allowing me to work in my own way. Her wide knowledge and her logical way of thinking have been of great value to me. Her understanding, encouraging and personal guidance have provided a good basis for this thesis.

Also I would like to give my gratitude to all my friends and classmates in University Technology Malaysia. Finally, I would like to express my deep respect and appreciation to my parents and my brothers & sisters. They encouraged me to continue my study and I wouldn't do this research without their spiritual, financial help and support.

ABSTRACT

Insider threat is rapidly becoming the largest information security problem that organizations face. With granted access to internal systems, it is becoming increasingly harder to protect organizations from malicious insiders. The typical methods of mitigating insider threat are simply not working, primarily because insider threat is a people problem which is problematic at best. The insider threat problem is more elusive and perplexing than any other threat. Assessing the insider threat is the first step to determine the likelihood of any insider threat. Technical solutions do not suffice since insider threats are fundamentally a people issue. Therefore the aims of this research are to identify countermeasures addressing Insider Threat, as well as improve the behavior of end users by knows the factors that influence human behavior in order to mitigate the insider threat and to propose new a Framework of Human Behavior to limit or Mitigate the Insider Threat. In this research the questionnaires was distributed to the employees and one of the expert in CICT, Universiti Teknologi Malaysia, after distributing the questionnaires data was collected and analyzed by using (SPSS) program, and finally by getting the result of questionnaires, comments and suggestions from the expert the new framework of human behavior to mitigate the insider threat was proposed.

ABSTRAK

Dewasa ini, serangan Insider dengan pantas telah menjadi masalah keselamatan maklumat yang terbesar yang dihadapi oleh kebanyakan organisasi. Dengan akses yang sah dalam sistem dalaman, ianya menjadi semakin sukar untuk dilindungi daripada serangan jahat ini. Kaedah sedia ada pada masa kini untuk mengurangkan masalah serangan Insider ini adalah tidak mampu mengatasinya mungkin disebabkan serangan Insider adalah masalah yang secara amnya adalah berkaitan dengan manusia. Masalah serangan Insider ini adalah sangat abstrak dan kompleks berbanding dengan serangan-serangan siber yang lain. Dengan mengukur masalah serangan Insider ini adalah langkah pertama untuk mengenalpasti kebarangkalian terjadinya serangan seumpama ini. Walaubagaimanapun, penyelesaian dengan kaedah teknikal adalah tidak cukup kerana serangan Insider ini secara asasnya adalah masalah yang melibatkan manusia. Oleh itu, objektif penyelidikan ini adalah untuk mengenalpasti serangan balas yang melibatkan serangan Insider sekaligus meningkatkan tingkah laku pengguna akhir di dalam sesebuah organisasi. Dalam usaha untuk mengurangkan serangan Insider adalah dengan mengusulkan rangka kerja tingkah laku manusia yang baru. Dalam penyelidikan ini, borang soal selidik telah diedarkan dikalangan pekerja-pekerja serta kepada salah seorang pakar keselamatan maklumat di CICT, Universiti Teknologi Malaysia dan selepas itu data-data telah dikumpul dan dianalisa dengan menggunakan perisian SPSS. Akhir sekali, hasil keputusan yang diperoleh daripada borang soal selidik, komen-komen dan juga cadangan-cadangan daripada pakar, rangka kerja tingkah laku manusia yang baru telah diusulkan.

CHAPTER 1

INTRODUCTION

1.1 Introduction

Risks from insider threats are critical weapons to harm the value assets of the organization, and arise in many facets at different layers of system abstractions. It is very difficult to discover the insider and identify his characteristics because of his legitimate access to facilities, physical assets, critical information and where the vulnerability of the organization exists. Insider refers to a member of the organization who has granted access to the resource of the organization and can use certain privileges for confidential information. The threat is also defined as "Intended expression of inflicting pain or punishment of future harm", combing these words together an insider threat is anyone has permitted access and causes harm to organization asset accidently or intentionally (Colwill, 2009).

1.2 Problem Background

Most problems related to computer security are happening due to people, ultimately they are responsible for causing harm to the system, and therefore it will help as a basis for this project. People are the weakest link in Computer and Information Security (Bulgurcu, 2008) technical issues are not responsible here in information security just it's known as purely people issue.

It is possible to show that human behavior is useful in computer modeling to determine the likelihood of damage from the inside, allowing security personnel to implement suitable tools to reduce the insider threat and the amount of damage that occurs (Puleo, 2006).

Users, researchers, and administrators they are worried about the outsider's attacking the systems and networks, but actually they should be worried about the insider threats. Legitimate users have access in multiple ways to put the data, systems, and organization of work at a risk. Malicious behavior probably not malicious, but it may well intended to undesirable consequences (Roy Sarkar, 2010, Pfleeger *et al*., 2010)

Users commit to steal sensitive information or fraud in an organization when motivated by money, revenge, and competitive advantage. Every organization it has diverse variety of consultants, employees, and partners, then it's difficult to protect form the insider threat. (Roy Sarkar, 2010).

Problem from the insider threat it causes harm to the system or the organization more than any other threat. To identify the insider threat it should be by determines the vulnerability of any attacks. However technical solutions are not enough since the internal threats is essentially a question of people. Therefore, the following three-pronged approach - technology assessment, behavioral and organizational is necessary to facilitate the insider threats to predict and anticipate any attack from the inside and thus improve the security of the organization. (Roy Sarkar, 2010)

1.3 Problem Statement

The insider threat is becoming quickly the biggest information security problem faced by the institutions. With access granted to the internal systems, and it became increasingly difficult to protect organizations from insider threats. One of the main reasons that organizations facing is they cannot buy the honesty of the employees. Like factors affecting the employees are competition among the organizations, disgruntled employee, bribe and less salary. The current organization employees and former organization employees both are threats posing to organization information, which is problematic at best. Therefore the purpose of this project is to mitigate the insider threat by developing a new framework that contains components that will affect to the human behavior, In this project there are four frameworks and these frameworks they have problems like lack of the factors that influence of human behavior and its need to be modified, so in this case a Framework will propose to solve the following problem.

How to propose A Framework for Insider Threat considering human behavior in relation to the existing Frameworks?

It’s necessary to find out the weaknesses of existing frameworks by comparing them.

i. What are the existing frameworks of human behavior related to insider threat?
ii. How to develop a framework to limit or mitigate the insider threat?
iii. How to evaluate the proposed framework (human behavior to mitigate the insider threat)?

1.4 Aim of this Study

Insider threat is a problem that all organizations are facing, as employee action or ignorance can potentially lead to incidents so that the organization may even not survive, so the aims of this research are to identify countermeasures addressing Insider Threat, as well as improve the behavior of end users by identify the factors that influences human behavior in order to mitigate the insider threat and to develop a conceptual framework of human behavior to limit or mitigate the insider threat.

1.5 Research Objectives

In order to answer the questions asked previously the researcher designed the following objectives:

i. To find out the common threats, countermeasures of insider threat and to investigate the insider threat frameworks that covering human behavior
ii. To develop a framework to limit or mitigate insider threats related to human behavior.
iii. To evaluate the proposed framework of insider threat.

1.6 Project Scope

This research focuses on the ethical employees or agent usually has originally no intention of causing damage. Hired employees with the intention of harming confidentiality excluded, as well as those paid by outsiders to enter the organization and do harm.

By excluding people who already have the intention to cause harm or damage from this research, it is possible to get an idea of what behavioral scientists might consider "normal" behavior of a typical employee. Using this basis, it is possible to differentiate between employees with high risk of causing damage to natural and familiar.

The scope of this project that identifies the boundaries is listed below:

i. The study will focus on developing a framework of human behavior to mitigate the Insider Threat
ii. The study will be conducted mainly in the administrative computing environment in CICT, University Technology Malaysia.

1.7 Significance of the Research

The importance of this project helps to use countermeasures against insider threats. It enables organizations to get a better understanding and clear picture of the threats that happened by insiders.

The aim of this project is to know the relationship between countermeasure and the insider threats, and to build a framework for human behavior to mitigate the insider threats.

1.8 Organization of Report

This report consists of six chapters; the first chapter covers the introduction, problem background, and problem statement, aim of this study, research objectives, scopes and the significant of this research. Chapter 2 covers the literature review on insider threat, human behavior, countermeasures of insider threat, and frameworks of insider threat behavior. Chapter 3 consists of a methodology that is used in this research. Chapter 4 is designing the proposed conceptual framework of human behavior to mitigate the insider threat. Chapter 5 consist of analyze the questionnaires, and interview with expert, finally chapter 6 covers the project achievement, project constraint, and future work.

REFERENCES

Abend, V., Peretti, B., Axlerod, C. W., Barry, K., Donahue, D., Wright, K., Panchery, J. (2008). Cyber Security for the Banking and Finance Sector. Wiley Handbook of Science and Technology for Homeland Security.

Albert, C.andDorofee, A. J. (2001). Octave criteria, version 2.0.

Anderson, R. H. (1999). Research and Development Initiatives Focused on Preventing, Detecting, and Responding to Insider Misuse of Critical Defense Information Systems: DTIC Document.

Anderson, R. H.andBrackney, R. (2004). Understanding the insider threat.

Aquino, K., Tripp, T. M.andBies, R. J. (2001). How employees respond to personal offense: The effects of blame attribution, victim status, and offender status on revenge and reconciliation in the workplace. Journal of Applied Psychology, 86(1), 52.

Avison, D. E.andWood-Harper, A. (1990). Multiview: an exploration of information systems development: Blackwell Scientific.

Bishop, M. (2005a). The insider problem revisited.

Bishop, M. (2005b). Position: Insider is relative.

Bishop, M.andGates, C. (2008). Defining the insider threat.

Bosworth, S.andKabay, M. E. (2002). Computer security handbook: Wiley.

Brackney, R. C.andAnderson, R. H. (2004). Understanding the insider threat: Proceedings of a march 2004 workshop (Vol. 196): Rand Corp.

Bulgurcu, B. (2008). The antecedents of information security policy compliance. University of British Columbia.

Carroll, M. D. (2006). Information security: examining and managing the insider threat.

Cheung, I.andDatardina, M. (2011). Managing Insider Threat.

Cole, E.andRing, S. (2006). Insider threat: Protecting the enterprise from sabotage, spying, and theft: Syngress Media Inc.

Coles-Kemp, L.andTheoharidou, M. (2010). Insider Threat and Information Security Management. Insider Threats in Cyber Security, 45-71.

Colwill, C. (2009). Human factors in information security: The insider threat–Who can you trust these days? Information Security Technical Report, 14(4), 186-196.

Cornelissen, W. (2009). Investigating insider threats: problems and solutions.

Da Veiga, A.andEloff, J. H. P. (2010). A framework and assessment instrument for information security culture. Computers & Security, 29(2), 196-207. doi: 10.1016/j.cose.2009.09.002

Dhillon, G. (1999). Managing and controlling computer misuse. Information Management & Computer Security, 7(4), 171-175.

EIU, B. C. (2009). The Economist Intelligence Unit: Various.

Flinders, M. (2010). A voyage to Terra Australis: Salzwasser-Verlag Gmbh.

Garfinkel, R., Gopal, R.andGoes, P. (2002). Privacy protection of binary confidential data against deterministic, stochastic, and insider threat. Management Science, 749-764.

Greitzer, F. L., Moore, A. P., Cappelli, D. M., Andrews, D. H., Carroll, L. A.andHull, T. D. (2008). Combating the insider cyber threat. Security & Privacy, IEEE, 6(1), 61-64.

IEC, I. 15408 (1999): Information Technology–Security techniques–Evaluation criteria for IT security: Part 1/2/3.

Kandias, M., Mylonas, A., Virvilis, N., Theoharidou, M.andGritzalis, D. (2010). An insider threat prediction model. Trust, Privacy and Security in Digital Business, 26-37.

Kavanagh, M. J.andThite, M. (2008). Human resource information systems: Basics, applications, and future directions: Sage Publications, Inc.

Kraemer, S., Carayon, P.andClem, J. (2006). Characterizing violations in computer and information security systems.

Kreicberga, L. (2010). Internal threat to information security.

Leach, J. (2003). Improving user security behaviour. Computers & Security, 22(8), 685-692.

Magklaras, G.andFurnell, S. (2001). Insider threat prediction tool: Evaluating the probability of IT misuse. Computers & Security, 21(1), 62-73.

Martinez-Moyano, I. J., Rich, E., Conrad, S., Andersen, D. F.andStewart, T. R. (2008). A behavioral theory of insider-threat risks: A system dynamics approach. ACM Transactions on Modeling and Computer Simulation (TOMACS), 18(2), 7.

McCormick, M. (2008). Data theft: A prototypical insider threat. Insider Attack and Cyber Security, 53-68.

McIlwraith, A. (2006). Information security and employee behaviour: how to reduce risk through employee education, training and awareness: Gower Publishing Company.

Melara, C., Sarriegui, J. M., Gonzalez, J. J., Sawicka, A.andCooke, D. L. (2003). A system dynamics model of an insider attack on an information system.

Miller, S. L., Maner, J. K.andBecker, D. V. (2010). Self-protective biases in group categorization: Threat cues shape the psychological boundary between "us" and "them". Journal of personality and social psychology, 99(1), 62.

Mills, R. F., Peterson, G. L.andGrimaila, M. R. (2009). Insider Threat Prevention, Detection and Mitigation. Cyber-Security and Global Information Assurance: Threat Analysis and Response Solutions.

Moore, A. P., Cappelli, D. M., Joseph, H.andTrzeciak, R. F. (2006). An Experience Using System Dynamics to Facilitate an Insider Threat Workshop. Unpublished Paper, Carnegie Mellon University CERT Software Engineering Institute.

Neumann, I. D., Torner, L.andWigger, A. (1999). Brain oxytocin: differential inhibition of neuroendocrine stress responses and anxiety-related behaviour in virgin, pregnant and lactating rats. Neuroscience, 95(2), 567-575.

Nunes Leal Franqueira, V.andvan Eck, P. (2006). Defense against insider threat: a framework for gathering goal-based requirements.

Pahnila, S., Siponen, M.andMahmood, A. (2007). Employees' behavior towards IS security policy compliance.

Parsons, K., McCormac, A., Butavicius, M.andFerguson, L. (2010). Human Factors and Information Security: Individual, Culture and Security Environment.

Pfleeger, S. L., Predd, J. B., Hunker, J.andBulford, C. (2010). Insiders behaving badly: addressing bad actors and their actions. Information Forensics and Security, IEEE Transactions on, 5(1), 169-179.

Predd, J., Pfleeger, S. L., Hunker, J.andBulford, C. (2008). Insiders behaving badly. Security & Privacy, IEEE, 6(4), 66-70.

Puleo, A. J. (2006). Mitigating insider threat using human behavior influence models: DTIC Document.

Roy Sarkar, K. (2010). Assessing insider threats to information security using technical, behavioural and organisational measures. Information Security Technical Report, 15(3), 112-133.

Royds, C. Management Plan for Antarctic Specially Protected Area (ASPA) No. 121 Cape Royds, Ross Island.

Schultz, E. E. (2002). A framework for understanding and predicting insider attacks. Computers & Security, 21(6), 526-531.

Thompson, B., Haber, S., Horne, W., Sander, T.andYao, D. (2009). Privacy-preserving computation and verification of aggregate queries on outsourced databases.

Wood, B. (2000). An insider threat model for adversary simulation. SRI International, Research on Mitigating the Insider Threat to Information Systems, 2, 1-3.

Wyman, O.andCarpenter, G. (2008). Co-operative Bank: Customer Champion: MMC, Brussels.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES