ADAPTIVE USER BEHAVIOR RISK SCORING MODEL
AN APPROACH TO THE SECURITY RISK ANALYSIS AND CONTROL SPECIFICATION OF COMPUTER USER

By

Krisdian Eko Sutedja
22015112

MASTER'S DEGREE
in

INFORMATION TECHNOLOGY
FACULTY OF ENGINEERING AND INFORMATION TECHNOLOGY

SWISS GERMAN UNIVERSITY
EduTown BSD City
Tangerang 15339
Indonesia

August 2016

Revision after the Thesis Defense on July 19th, 2016

STATEMENT BY THE AUTHOR

I hereby declare that this submission is my own work and to the best of my knowledge, it contains no material previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any other degree or diploma at any educational institution, except where due acknowledgement is made in the thesis.

Krisdian Eko Sutedja

Student Date

Approved by:

Dr. Mulya R. Mashudi, S.T., M.Sc.

Thesis Advisor Date

Charles Lim, M.Sc.

Thesis Co-Advisor Date

Dr. Ir. Gembong Baskoro, MSc.

Dean Date

ABSTRACT

ADAPTIVE USER BEHAVIOR RISK SCORING MODEL
AN APPROACH TO THE SECURITY RISK ANALYSIS AND CONTROL SPECIFICATION OF COMPUTER USER

By

Krisdian Eko Sutedja
Dr. Mulya R. Mashudi, S.T., M.Sc., Advisor
Charles Lim, M.Sc., Co-Advisor

SWISS GERMAN UNIVERSITY

When people say, “Your company worst security vulnerability is still located between the keyboard and the chair”, it shows how even until today, there is still the ever-daunting tasks concerning information security that must be faced by any organizations, which is not to fall victim to the weakest link regarding the information security – the human factor. More efforts were invested by the organization into technology development and enhancement, rather than focusing on the people and processes aspects. But actually, the important component in doing the protection regarding the organization’s assets is the understanding of the “Enemy”. The organization should no longer only focus on the technological perspective of the information security. We also need to have the “Insider knowledge” in order to do user behavior analysis effectively.

This research main contribution is that the proposed model would help the organization to get the visibility in order to effectively identify potential fraudulent computer users and the risks by applying risk-based approach to analyze the collected user activities data in finding computer users with the high risk level, and to define

applicable security risk controls in order to mitigate the risks which come from the computer user behavior.

Keywords: Risk Scoring, User Behavior, Risk Control, ISO/IEC 27002, Computer User.

DEDICATION

I dedicate this work to my beloved family who were praying for me every day and for all the support and encouragement from them, to all those striving to deliver more secure information systems, and also to my one and only country, Indonesia.

ACKNOWLEDGEMENTS

I wish to thank the members of my committee for their support, patience and good humor. Their gentle but firm direction has been most appreciated. Greatest appreciation to Dr. Mulya R. Mashudi, S.T., M.Sc. (Advisor) and Mr. Charles Lim, M.Sc. (Co-Advisor) which were particularly very helpful in guiding me toward a better methodology in research study writing.

I have found my coursework throughout the Curriculum and Instruction program to be stimulating and thoughtful, providing me with the tools with which to explore both past and present ideas and issues.

TABLE OF CONTENTS

Page