

UNIVERSITI TEKNOLOGI MARA

**INVESTIGATING THE PRACTICES OF
INFORMATION SECURITY INCIDENT
MANAGEMENT SYSTEM IN NETWORKS
THREATS:
A CASE IN TM'S IPCORE NETWORK**

NORKHAMSIAH BINTI ABDUL MALIK

IT Project submitted in partial fulfillment
of the requirements for the degree of
Master of Science in Information Technology

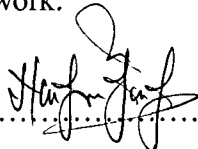
Faculty of Computer and Mathematical Sciences

July 2015

AUTHOR'S DECLARATION

I declare that the work in this IT Project was carried out in accordance with the regulations of Universiti Teknologi MARA. It is original and is the results of my own work, unless otherwise indicated or acknowledged as reference work. This IT Project has not been submitted to any other academic institution or non-academic institution for any degree or qualification.

I, hereby, acknowledge that I have been supplied with the Academic Rules and Regulations for Post Graduate, Universiti Teknologi MARA, regulating the conduct of my study and research.

Name of Student : Norkhamsiah binti Abdul Malik
Student I.D. No. : 2012330747
Programme : Master of Science in Information Technology
Faculty : Computer and Mathematical Sciences
IT Project Title : Investigating the Practices of Information Security Incident Management System in Network Threats: A Case in TM's IPCore Network.
Signature of Student : 
Date : 14 July 2015

ABSTRACT

Nowadays, access to reliable information has become an essential factor leading to success in business. In this regard, adequate security of information and systems that process it is critical to the operation of all organizations. Therefore organizations must understand and improve the current status of their information security in order to ensure business continuity in the future. Hence, a research was conducted using Information Security Management System (ISMS) standards as reference model to highlight the practices applied in handling network threats at Telekom Malaysia Berhad (TM) organisation focusing on IPCore Network. This study addressed the control failures or weaknesses during information security incident management practice applied in organisations. This research had shown the relationship between control failure and the incident management system practice that have been applied in TM organisation. During this research, interview sessions were conducted as methodology mechanism, which involving three respondents who are responsible in incident management system environment in TM organisation. By using content analysis, the finding revealed best practice elements that there are involved the process of identifying the incidents, prioritizing incidents based on business impact, tracking incidents to closure, integrating with major IT management systems, and implementing the best practices guidelines and lesson learnt for future improvement. An effective incident management system should be capable of handling incidents event starting from planning and preparing until lesson learnt process. Therefore, this study revealed the TM organisation practice on activities throughout the incident management process, assessment issues faced during handling incident process, and determinant elements influencing the information security management system. Thus, this research proposed future recommendations for ensuring the optimization on incident management process performance effectiveness and efficiency. The adoption of the practice presented in the paper may enable similar telecommunication industry in building the capacity to better manage information security management system with précising the incident management system domain specifically.

ACKNOWLEDGEMENT

First and foremost, Alhamdulillah, the deepest gratitude of all shall be bestowed to Allah the Almighty and The Merciful for all the insight which He gave to us that lead to the completion of this research. Without His blessings and consent, I might not have enough courage and determination to complete this research. All my thanks and appreciation will be lay upon Him for giving me a good health and spirit throughout the journey.

My deepest gratitude is extended to Dr Jasber Kaur A/P Gian Singh, for all assistance, advice, guidance, encouragement, new ideas and invaluable support given as my project supervisor for a better quality in my research. Thank you for being such a great mentor. I also would like to express my gratitude and sincere appreciation to Puan Suzana Zambri for teaching me on preparing analysis result by specific tools, NVivo.

My deepest appreciation to Jabatan Perkhidmatan Awam and Malaysian Government for giving me an opportunity in furthering my studies. Moreover, not forgetting very special thankful to all staff of Telekom Malaysia Berhad (TM), participant and all the lecturers, friends also colleagues of Master Science (Information Technology) for their support and encouragement during the process of completing this research.

Finally, I would like to express my deepest gratitude to my beloved parents and family especially to my husband for understanding and the endless support throughout the journey of glory. Thank you so much for taking part and involving in this research, they have been my motivation and inspiration of my thesis completion.

Thank you.

TABLE OF CONTENTS

	Page
AUTHOR'S DECLARATION	i
ABSTRACT	ii
ACKNOWLEDGEMENT	iii
TABLE OF CONTENTS	iv
LIST OF TABLES	viii
LIST OF FIGURES	ix

CHAPTER ONE: INTRODUCTION

1.1	Introduction	1
1.2	Research Background	1
	1.2.1 Information Security	2
	1.2.2 Security Standard and Practice	2
1.3	Problem Statement	4
1.4	Research Aim	7
1.5	Research Questions	7
1.6	Research Objectives	7
1.7	Scope of the Research	7
1.8	Significance of the Research	8
1.9	Research Design Summary	9
1.10	Thesis Outlines	11

CHAPTER TWO: LITERATURE REVIEW

2.1	Introduction	13
2.2	Information Security Management System (ISMS)	13
2.3	Information Security Management System (ISMS) in Malaysia	16
2.4	Information Security Incident Management	17