

UNIVERSITI TEKNOLOGI MARA

**COMPONENTS OF A
CYBER SECURITY FRAMEWORK
FOR THE PROTECTION OF
THE CRITICAL NATIONAL
INFORMATION INFRASTRUCTURE
OF MALAYSIA
AGAINST CYBER THREATS**

MOHD SHAMIR BIN HASHIM

Thesis submitted in fulfillment
of the requirements for the degree of
Master of Science
(Information Management)

Faculty of Information Management

August 2019

ABSTRACT

The dependability on the Internet by the Critical National Information Infrastructure (CNII) of countries has triggered the need to protect such infrastructures against cyber threats. This is because operational disruptions to the CNII will have a major negative impact on the country such as threats to the national security and the economy. A lot of countries are coming up with a cyber security framework mainly for the protection of the CNII. This study looks at the cyber security initiative of five (5) countries to determine what are the elements to be considered in developing a cyber security framework for the protection of the CNII against cyber threats. Having a cyber security framework with the necessary elements will ensure that the framework provides a holistic approach in providing cyber security to the CNII. In this digital age, the CNII are heavily relying on ICT to cope up with the modern-day communication demands. This has cause countries to consider the cyber environment and the CNII as critical areas and need to be protected. Realizing the detrimental effect of cyber threats, governments are developing cyber security frameworks and having specific machineries to look into the matter. Therefore, the objectives of this study are to determine the components for an cyber security framework for protecting Malaysia CNII against cyber threats, and to determine how to protect the Malaysia CNII against cyber threats base on the identified components

ACKNOWLEDGEMENT

Firstly, I wish to thank Allah S.W.T for with His grace I am able to embark on my Masters study and completing this long and challenging journey successfully. My gratitude and thanks also go to my supervisor Prof Madya Dr Mohamad Noorman Masrek for the guidance, support and most of all patience in seeing me through this study. I would also like to express my gratitude to my work supervisors in CyberSecurity Malaysia for giving me the working hours flexibility in order for me to complete my program. Not to forget the staff of the International and Government Engagement, CyberSecurity Malaysia for the support provided to facilitate my work.

My appreciation goes to the participants from the Critical National Information Infrastructure of Malaysia whom have provided me with good feedbacks during the interview sessions.

Finally, this thesis is dedicated to my family members who has continuously provide me with the emotional support I need to reach this point.

Thank you. Alhamdulillah.

TABLE OF CONTENTS

	Page
CONFIRMATION BY PANEL OF EXAMINERS	ii
AUTHOR’S DECLARATION	iii
ABSTRACT	iv
ACKNOWLEDGEMENT	v
TABLE OF CONTENTS	vi
LIST OF TABLES	xi
LIST OF FIGURES	xii
LIST OF ABBREVIATIONS	xiii
CHAPTER ONE: INTRODUCTION	1
1.1 Research Background	1
1.2 Problem Statement	2
1.2.1 The Critical National Information Infrastructures	3
1.2.2 The Need for Cyber Security Framework for the CNII	4
1.2.3 Identifying the Components of a Cyber Security Framework for CNII	5
1.3 Research Questions	6
1.4 Research Objectives	6
1.5 Scope of the Study	6
1.6 Significance of the Study	8
1.7 Thesis Outline	9
1.8 Chapter Summary	11
CHAPTER TWO: LITERATURE REVIEW	12
2.1 Introduction	12
2.2 Definition of Terms	12
2.2.1 Cyber Security	13
2.2.2 Framework	14
2.2.3 Cyber Space	15
2.2.4 Cyber Threats	16

2.2.5	The Critical National Information Infrastructure	19
2.3	Cyber Security Framework	20
2.4	Previous studies on the Protection of the CNII	21
2.5	Current Cyber Security Framework Initiatives	25
2.5.1	US Common Security Framework	25
2.5.2	The National Institute of Standards and Technology	26
2.5.3	The International Telecommunication Union	27
2.5.4	Organization for Economic Co-operation and Development	28
2.5.5	The GFCE-Meridian	29
2.6	Insights from Present Initiatives Reviews	30
2.7	Selected Countries for the Study	32
2.7.1	Australia	33
2.7.2	Singapore	39
2.7.3	The United Kingdom	43
2.7.4	The United States of America	50
2.7.5	Malaysia	56
2.8	National Cyber Security Policies Review	62
2.9	Gap Analysis	64
2.10	Component for a Cyber Security Framework	65
2.11	Conceptual Framework	65
2.12	Chapter Summary	67
CHAPTER THREE: RESEARCH METHODOLOGY		69
3.1	Introduction	69
3.2	Research Paradigm	69
3.3	Interpretivist Paradigm and Qualitative Method	72
3.4	Research Approach	72
3.5	Research Process	74
3.6	The Case Study Research Method	76
3.7	Conducting the Case Study	78
3.7.1	Defining the case	78
3.7.2	Selecting the cases	79
3.7.3	Collecting the data	80
3.7.4	Analysing, interpreting and reporting case studies.	81