THE RELATIONSHIP BETWEEN SECURITY CULTURE AND SECURITY PRACTICES IN PROTECTING CRITICAL NATIONAL INFRASTRUCTURE IN MALAYSIA

BY

MOHAMAD FIRDHAUS BIN MOHAMAD LAJIS

INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

2021

THE RELATIONSHIP BETWEEN SECURITY CULTURE AND SECURITY PRACTICES IN PROTECTING CRITICAL NATIONAL INFRASTRUCTURE IN MALAYSIA

BY

MOHAMAD FIRDHAUS BIN MOHAMAD LAJIS

A dissertation submitting in fulfillment of the requirement for the degree of Master of Protective Security Management

Kulliyyah of Information and Communication Technology
International Islamic University Malaysia
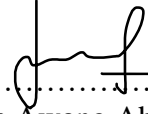
JULY 2021

ABSTRACT

This thesis looks into the relationship between security culture and security practices in Malaysia when it comes to protecting Critical National Infrastructure. There has been a great deal of interest in this relationship as a result of the recent and widespread recognition that poor security practises, rather than insufficient technical controls, are the root cause of security issues. Furthermore, it is argued that security culture is required to cultivate and support security practices. This implies that they have a relationship, and that by understanding this relationship, improvements to Critical National Infrastructure protective security can be made. Hence, this research creates a rigorous conceptual framework for identifying the specific security culture characteristics that support and guide security practices aimed at improving Critical National Infrastructure protective security. The framework is then used as the foundation for quantitative studies that empirically investigate the exact relationship between security culture and security practices. Based on the findings, this study concludes that a comprehensive approach is needed to cultivate the security culture characteristics that are important in order to support and guide security practises and positively influence employees' security behaviour in CNI. This discovery is a significant step forward in the future systematic cultivation of security culture and security practices to support and guide security practices to influence employee behaviours in order to improve CNI protective security.

ABSTRACT IN ARABIC

هذه الأطروحة تحقق في العلاقة بين الثقافة الأمنية والممارسات الأمنية في ماليزيا عندما يتعلق الأمر بحماية البنية التحتية الوطنية الحيوية. وقد كان هناك قدر كبير من الاهتمام بهذه العلاقة بسبب الاعتراف مؤخرا وعلى نطاق واسع بأن الممارسات الأمنية السيئة، بدلا من عدم كفاية الضوابط التقنية، هي السبب الجذري للمسائل الأمنية. وعلاوة على ذلك، يقال إن الثقافة الأمنية مطلوبة لتنمية ودعم الممارسات الأمنية. وهذا يعني أن لديهم علاقة، وأنه من خلال فهم هذه العلاقة، يمكن إدخال تحسينات على أمن حماية البنية التحتية الوطنية الحرجة. ومن ثم، فإن هذا البحث يخلق إطارا مفاهيميا صارما لتحديد خصائص الثقافة الأمنية المحددة التي تدعم وتوجه الممارسات الأمنية الرامية إلى تحسين الأمن الوقائي للبنية التحتية الوطنية الحيوية. ثم يستخدم الإطار كأساس للدراسات الكمية التي تحقق تجريبيا في العلاقة الدقيقة بين الثقافة الأمنية والممارسات الأمنية. واستنادا إلى النتائج، تخلص هذه الدراسة إلى أن هناك حاجة إلى نهج شامل لزراعة خصائص الثقافة الأمنية التي تعتبر مهمة لدعم وتوجيه الممارسات الأمنية والتأثير بشكل إيجابي على السلوك الأمني للموظفين في CNI. ويمثل هذا الاكتشاف خطوة مهمة إلى الأمام في الزراعة المنهجية المستقبلية للثقافة الأمنية والممارسات الأمنية لدعم وتوجيه الممارسات الأمنية للتأثير على سلوك الموظفين لتحسين الأمن الوقائي CNI.

APPROVAL PAGE

I certify that I have supervised and read this study and that in my opinion, it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a thesis for the degree Master of Protective Security Management.

……………………………………………
Normi Sham Awang Abu Bakar
Supervisor

I certify that I have read this research and that in my opinion it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a thesis for the degree Master of Protective Security Management.

………………………………………
Jamaludin Ibrahim
Examiner

This dissertation was submitted to Centre for IT Advancement and is accepted as a fulfillment of the requirement for the degree of Master of Protective Security Management.

………………………………………
Madihah S. Abd. Aziz
Head, Centre for IT Advancement

This dissertation was submitted to the Kulliyyah of Information and Communication Technology and is accepted as a fulfillment of the requirement for the degree of Master of Protective Security Management.

………………………………………
Abd. Rahman Ahlan
Dean, Kulliyyah of Information and Communication Technology (KICT)

DECLARATION

I hereby declare that this dissertation is the result of my own investigations, except where otherwise stated. I also declare that it has not been previously or concurrently submitted as a whole for any other degrees at IIUM or other institutions.

Mohamad Firdhaus bin Mohamad Lajis

Signature …………………………   Date …………………………
6 September 2021

INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

DECLARATION OF COPYRIGHT AND AFFIRMATION OF FAIR USE OF UNPUBLISHED RESEARCH

THE RELATIONSHIP BETWEEN SECURITY CULTURE AND SECURITY PRACTICES IN PROTECTING CRITICAL NATIONAL INFRASTRUCTURE IN MALAYSIA

Affirmed by Mohamad Firdhaus bin Mohamad Lajis

..........…/……………….…………   ....……..……....……..
           Signature   6 September 2021
                                           Date

ACKNOWLEDGEMENT

All credit goes to الله the Almighty, whose Grace and Mercy have been with me throughout my studies. Despite the fact that it has been difficult, His Mercy and Blessings on me have made the enormous job of finishing my dissertation much easier.

I would really like to express my gratitude to the persons listed below for their encouragement and assistance, without which I would not have been able to complete this dissertation.

First and foremost, I want to express my gratitude to my adoring parents and entire family. Their encouragement and support have helped me get through this difficult time.

I would like to send a special message of love and gratitude to my wife, Sharifah Nurshafazillah Rosli, for her patience, understanding, personal support, constant encouragement, and unconditional sacrifice. This appreciation extends to my son, Muhammad Furqan Fawwaz, who is a constant source of joy and satisfaction in my life. You're both great motivators and encouragers for me.

I also like to thank my supervisor, Assoc. Prof. Dr. Normi Sham Awang Abu Bakar, for her invaluable advise, dedication, and direction, as well as for encouraging and focusing me during my Masters' journey. The discussion I had with her proved to be quite beneficial to my work. I'd also want to express my gratitude to Prof. Dr. Husnayati bt Hussin and Dr. Lim Joo Soon for their advice, support, and encouragement. The suggestions and arguments on how to write my dissertation kept me focused and motivated to finish it.

I would also want to use this opportunity to express my deep gratitude and appreciation for my superior, immediate superior, and colleagues' assistance and patience. Several explanations were presented to me during the tough period of writing my dissertation.

Mohamad Firdhaus bin Mohamad Lajis

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF STATUTES

Central Committee of Key Points Standing Order No.1/2008
Emergency (Essential Powers) Act 1979 (Act 216)
Official Secret Act 1972 (Act 88)
Protected Places and Protected Areas 1959 (Act 298)
Emergency (Essential Power) Ordinance 1964
Essential (Key Points) Regulation 1965
Key Point Standing Order 1993

LIST OF ABBREVIATIONS

ATM	*Angkatan Tentera Malaysia* (Malaysia Armed Forces)
ATSP	*Arahan Tetap Sasaran Penting* (Key Point Standing Order) 1993
BCM	Business Continuity Management
CGSO	Chief Government Security Office, Prime Minister's Department, Malaysia
CI	Critical Infrastructure
CNI	Critical National Infrastructure
CPPNM	Convention on the Physical Protection of Nuclear Material
CSM	CyberSecurity Malaysia, Ministry of Communication and Multimedia Malaysia
DAESH	Islamic State of Iraq and the Levant
DV	Dependent Variable(s)
EPCIP	European Programme for Critical Infrastructure Protection
EU	European Union
ICT	Information and Communication Technology
IAEA	International Atomic Energy Agency
IS[1]	Information Security
IS[2]	Islamic State(s)
ISMS	Information Security Management System
IT	Information Technology
IV	Independent Variable(s)
JPSP	*Jawatankuasa Pusat Sasaran Penting* (Key Points Central Committee)
JSPN	*Jawatankuasa Sasaran Penting Negeri* (Key Points State Committee)
MCMC	Ministry of Communication and Multimedia Malaysia
MCO	Movement Control Order
MCP	Malaysian Communist Party
MoHA	Ministry of Home Affairs
MoSTI	Ministry of Science, Technology and Innovation
NCSP	National Cyber Security Policy
NSC	National Security Council
NSS	Nuclear Security Series
PhD	Doctor of Philosophy
PKM	*see MCP*
PPS	Physical Protection System
RMP	Royal Malaysia Police
SC	Security Culture
SP	Security Practice(s)
SPM	*Sijil Pelajaran Malaysia* (Malaysian Certificate of Education)

CHAPTER ONE

INTRODUCTION

1.1   RESEARCH BACKGROUND

The Critical Infrastructure (CI) plays an important role in assuring the welfare of the nation. It exists and manages by the government in any countries and known as Critical National Infrastructure (CNI). The factors that ensure the security of the CNI will lead to the stability of national political scenario, sustainable economic growth, stability of demography factor and the efficiency of government administration.

The existence of CNI will support the economic growth of the nation. As one of the sectors in the Critical Infrastructure is weaponry, it holds the strategic function of the security and national defence system. As Critical National Infrastructure also generates national resources and foods, this will ensure the continuous supply of the needs of water and food to the citizen.

Nowadays, the needs of electricity become essential. Hence, the government need to ensure that the supply of electricity is not interrupted. This is vital to the industries and commerce sectors as they generate income to the nation. On top of those entire factors, it's actually generated job and sources of income to the people of the nation.

In the context of public harmony, the need for basic necessities such as electricity, water and telecommunication imply that it is very important that the infrastructure services are not disrupted. This is important to ensure that the Critical National Infrastructure products and services will always be available and reliable for the nation to ensure public confidence towards government.

1

The infamous history of the CNI failure occurred on 3rd August 1996, when power was cut off for several hours in Kuala Lumpur, Selangor, Johor, Melaka, and Negeri Sembilan when a transmission line at Sultan Ismail Power Station in Paka, Terengganu was tripped at 5.17 p.m., causing all power stations in Peninsular Malaysia to go offline (The Star, 2009). This has resulted in massive losses for the industries and has tarnished the government's image and reputation regarding how the CNI is managed.

As a result, failure of these Critical National Infrastructures to supply products and services to the nation could have disastrous consequences, such as unsustainable economic growth. This will tarnish the government's reputation for development by casting doubt on the government's ability to govern the country. This situation will cause political unrest and drive away investors.

Therefore, it is important to implement improved security and safeguard to any identified threat, vulnerability and weakness in insuring the continuity of supply. However, the implementation of any security practices need the commitment and understanding from the employees.

In general, most organisations rely on technology-based solutions to improve facility security. Although these solutions are important in security (Straub & Nance, 1990), relying solely on them is unlikely to totally eliminate risk (Dhillon & Backhouse, 2001; Siponen, 2006; Cavusoglu, Cavusoglu, Son, & Benbasat, 2009). Meanwhile, previous research indicates that security incidents are still on the rise, despite organisations' increased investment in technology-based solutions (AIRC, 2008; Symantec, 2009). This situation suggests that technical solutions are insufficient for managing security (Pahnila, Siponen, & Mahmood, 2007; Siponen & Willison, 2009)

Eventually, there has been a call for organizations to shift the focus from improving the security to identifying and implementing social-culture measures (Ruighaver, Maynard, & Chang, 2007; Zakaria, 2007; Ramachandran, Srinivasan, & Tim, 2008). Hence, the idea to have security culture in support of technical solution for total security of organization has come in place.

Therefore, commitment and involvement from all level of employees are very important; right from top management to the lower level management. Each of them plays an important role in securing and ensures the protection of CNI. The development of a security culture will aid in the protection of the CNI. A comprehensive understanding of the relationship between security cultures and security practices is important for installation to influence employees' security behaviour towards improving CNI's protective security.

1.2   PROBLEM STATEMENT

As being stated earlier, the existence of Critical National Infrastructure is so crucial and like a honey pot to crime. It can be sources of income for criminal or burglar. As example, the thief can obtain metal scrap from electric substation. They also can get fuel from electric power plant while the robbers can get money from financial institution. If the adversary is terrorism, they can obtain explosive from mining and firearms from weaponry factory. This is hard to be executed if the adversaries did not have the opportunity in breaching the security barrier.

Previously, security threat is more focus on preventing the Critical Infrastructure assets from being stolen, destruction due to the fire or flood, and sabotage by Malayan Communist Party (MCP). However, current issues make the threat become complex and fraught with uncertainties. The threat landscape has evolved from conventional to

3

international terrorism and cyber threat. Hence, in facing the challenge and handling the crisis, the strategy and mechanism developed need to be resilient and able to overcome any threat.

In current scenario, the Islamic State (IS) also known as DAESH globally has planned to attack government facilities and CNI as the way to attracted government focus on them. Malaysia is no exception to the threat where Putrajaya as government administrative centre and Palace of Justice, Putrajaya has been announced as the target of the attack (Agenda Daily, 2015).

In ensuring the CNI protection, most of protective security system is designed for Physical Protection System (PPS). A complete physical protection system provides all required functions of an effective security system including Detection, Delay or Deter, and Response. These functions should be performed in order and within a length of time that is less than the time required for the terrorist, saboteur, or even disgruntled employee, to complete their task.

A well-designed protection system provides protection in depth with multiple layers of security that must be defeated in sequence, minimizes the consequences of single component failure, and exhibits balanced protection no matter which path of attack the adversary choose. Protection can be obtained through various combinations of technology (hardware and software), people, and procedures.

Meanwhile, the organizational information is a crucial part in every entity that needs a total protection. The fragility of information protection makes it easily compromised. The information leakage not only focused on technology system, but also on the behaviour of insider.

The leakages of information from the weakness of technology system are usually able to counter-act through the technology or the system itself. This is because

4

most of the organizations have focus their information security practice largely on technical issues like encryption/decryption, access controls, and intrusion detection system in recent years (Shuchih & Lin, 2007).

Hence, the implementation of any security practices needs the commitment and understanding from the employees. A survey conducted Information Security Magazine (2002) shows that most information security problems are caused by the negligence of people, rather by the attack events. This results supports that human behaviour is a vital point of organizational information leakage which need to be overcome.

Employees as the insider who hold the strategic and valuable information of the organization might become a target by the rivals to manipulate. This situation viewed as the major concern in the implementation of information security practices because of often reported as a threat (Lim, Ahmad, Chang, & Maynard, 2010; Workman, Bommer, & Straub, 2008). As past research identified that the employees' behaviour can jeopardize the success of protective security of the organizations (Straub, 1986; Pahnila, Siponen, & Mahmood, 2007; Workman, Bommer, & Straub, 2008).

Recent studies show that the employees are often found to be careless, unaware of security directives and fail to comply with organizational security policies and procedures (Furnell & Thomson, 2009; Bulgurcu, Cavusoglu, & Benbasat, 2010). However, this problem can be overcome when the employees have the well-shaped behaviour by the security culture. It is supported by many studies that address the important of the security culture in protecting the organization (Sizer & Clark, 1989; Schwarzwalder, 1999; Breidenbach, 2000; Solms, 2000; Andress & Fonseca, 2000; Clark-Dickson, 2001; Beynon, 2001).

In addition, research shows that the organizational culture has an impact on employee behaviour (Hofstede, Neuijen, Ohayv, & Sanders, 1990; Schein, 1992).

Furthermore, Hofstede et al. (1990) found the shared perceptions of daily practices are the main part of organization's culture and conclude that the organizational culture affects ordinary members of organization through shared practices.
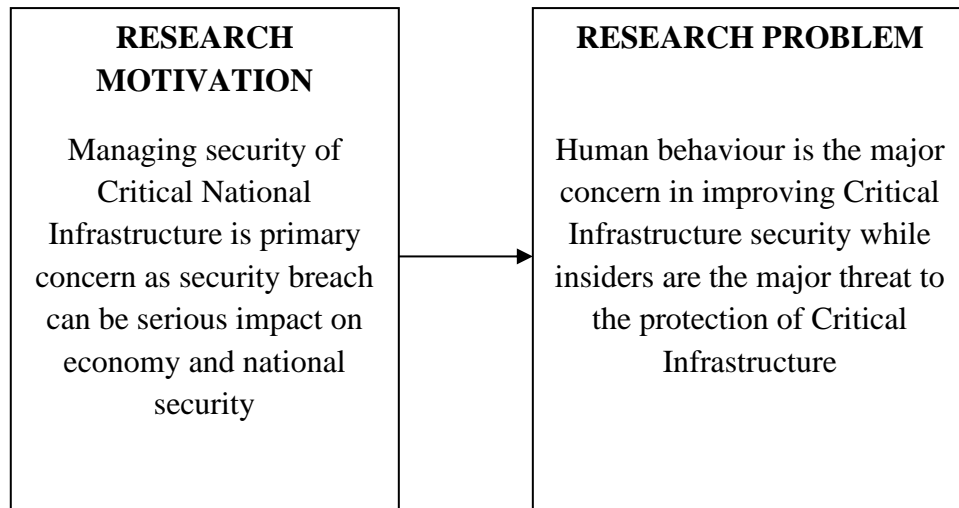
RESEARCH MOTIVATION	RESEARCH PROBLEM
Managing security of Critical National Infrastructure is primary concern as security breach can be serious impact on economy and national security	Human behaviour is the major concern in improving Critical Infrastructure security while insiders are the major threat to the protection of Critical Infrastructure

Figure 1.1: The relationship between research motivation and research problem

Meanwhile, the security culture can be shaped by the security policy as it is implemented through a combination of people, processes and technology controls. The policy influences the way in which employees interact with assets and ultimately directs their behaviour to be compliant with legislative, regulatory and contractual requirements (Viega, 2016).

Hence, all protective security system whether physical protection system or information protection systems developed will be useless if employee did not follow and practice the security policy or procedures diligently. Therefore, the security culture is vital in protecting the CNI which should be cultivated in the routine activities of each employee as a step in improving the security problems (Thomson, Solms, & Louw, 2006; Solms, 2000).

1.2.1 Research Objectives

In ensuring the security of CNI is not jeopardized and they can continuously supply their products and services, any kind of threat towards CNI protective security should be eliminated or at least, minimized. Government of Malaysia has gazetted the CNI Standing Order as known as *Arahan Tetap Sasaran Penting* (ATSP) on 13 Oct 1993 to show the importance of CNI to be protected.

The idea of the study is to expand the existing understanding of the relationship between security culture and security practices by exploring the security culture characteristics that support and guide security practices. The existing literature review does not reveal a specific correlation between security culture characteristics and security practices in protective security field. Security culture may influence employee behaviour to improve installation's security through routine security practices as the security culture includes security beliefs, values and practices.

Hence, this study is developed based on this perspective and can be translated into these objectives: -

(a) To analyse the relationship between Security Culture (SC) and the Security Practices (SP) in protecting the CNI;

(b) To identify Security Culture Characteristics that can affect the security practices and furthermore reduced the protection level of Critical Infrastructure; and

(c) To examine the influence of Security Culture on employees' behaviour toward protecting CNI.

1.2.2 Research Questions

These research questions are formulated to answer the research objectives:

(a)   What is the relationship between Security Culture Characteristics and the security practices in protecting the CNI?

(i) What are the Security Practices that exist in CNI?

(ii) What are the Security Culture Characteristics that exist in CNI?

(b)   What are the Security Culture characteristics that affect the security culture practices in protecting the CNI?

(c)   How will the Security Culture influence the employees' behaviour to protect the CNI?

1.2.3   Hypotheses

Based on the Research Objectives and Research Questions, the hypotheses generated from the theoretical framework can be formulated as follows:

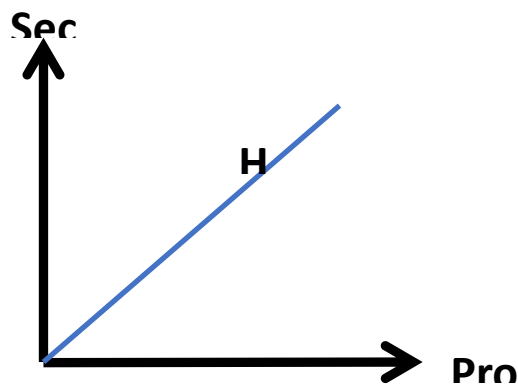H_1: The higher security culture developed in CNI, the higher the CNI is protected.

Figure 1.2: First Hypothesis.

H_2: The lack of security culture among employees of CNI will increase it's security threat level.
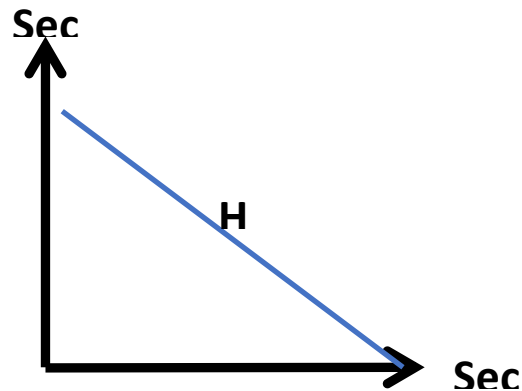
8

Figure 1.3: Second Hypothesis.

1.3 SCOPE OF THE STUDY

The excellent performance of CNI depends on the commitment from the owner and/or operator together with employees. Generally the number of Critical Infrastructures in Malaysia is too many and divided into many sectors, it is suggested that only 6 to 10 Critical Infrastructure installations selected to be involved in this research. This study will focus on sectors that related to utilities like power sector (power plant and power distribution facilities), water sector (water treatment plant and dam), oil and gas, and telecommunication sector which have more concern to the public.

The name of the installation involved cannot be revealed in this research as the installation listed as Critical National Infrastructure is protected under Official Secret Act (OSA) 1972. Hence, in order to make this study not to cross or breach any law and regulations, the name of CNI involved in this study will not be revealed.

Since the focus of the study is more towards employees' behaviour, the number of respondent in each sector will not be rigid and may differ when the research is conducted. In addition, the study adopts a quantitative approach where the detailed description and discussion of the research design including the selection of research methods is presented in Chapter 3. It is targeted to have 150 respondents which is the

9

employees of the CNI from various rank to have various understanding on their behaviour.

The quantitative approach was used to determine security culture characteristics and security practises, with the approach being used to validate, triangulate, complement, and establish a correlation between both security culture characteristics and security practises, allowing CNI management to identify security culture characteristics and develop security practises that improve CNI's protective security.

As far as being discussed, the identified Independent Variables (IV) extracts from security culture characteristics from Lim et al. (2012) will be included for this study. They are: -

    (a)   Evidence-based Decision Making;

    (b)   Long-term Plan and Commitment;

    (c)   Proper System and Process;

    (d)   Continuous Change and Improvement;

    (e)   Employee Involvement;

    (f)   Collaboration and Cooperation;

    (g)   A Shared Security Vision;

    (h)   Internal and External Focus; and

    (i)   Consistency.

Meanwhile the identified Dependent Variable (DV) is about the security practice of employees to protect the CNI. The research will investigate the relationship between the identified IV and DV. It also will investigate the impact of security culture against security practices. However, in Chapter 2 the security practices will be elaborate