CYBERSECURITY WELLNESS INDEX EVALUATION FRAMEWORK FOR CRITICAL ORGANISATIONS

HUSIN BIN JAZRI

DOCTOR OF PHILOSOPHY (COMPUTER SCIENCE)

UNIVERSITI PERTAHANAN NASIONAL MALAYSIA

2019

CYBERSECURITY WELLNESS INDEX EVALUATION FRAMEWORK FOR CRITICAL ORGANISATIONS

HUSIN BIN JAZRI

Thesis submitted to the Centre for Graduate Studies, Universiti Pertahanan Nasional Malaysia, in fulfillment of the requirements for the Degree of Doctor of Philosophy (Computer Science)

2019

- In Memories of My Late Mother and Sister; and To My Daughters and Sons With Love -

ABSTRACT

Cyber threats pose serious security challenges to organisations and nation states. To deal with the dynamics of such cyber threats, governments as well as international organisations introduced initiatives to measure performance at both organisational and national levels to counter such cyber threats. For instance, United Nations agency, the International Telecommunication Union (ITU) developed the Cyberwellness Index while countries like Estonia developed the Government National Cybersecurity Index while the UK developed the National Cyber Security Centre Maturity Framework. These measurement tools and indexes, however, are very resource intensive, time consuming and are not effective enough to respond to the dynamic and fluid changes in today's cyber threat environment. It is critical that such measurement tools function like real time technical solutions. This research introduces a new Management Model and Framework that not only simplify the performance measurement framework but when deployed in practice, it is able to respond fast to counter the rapidly changing threat environment. The research designs a symptomatic based Cybersecurity Wellness Index Evaluation Framework that uses symptomatic Cybersecurity Vital Signs to evaluate cybersecurity risks for Critical Organisations. This new and dynamic model uses the simplest and quickest indicators to generate faster results thus allowing organisations to be better prepared to cope with the rapidly changing cyber threats dynamics. The Framework evaluates cybersecurity wellness of Critical Organisations at the operational level with the data aggregated as a group index to serve sectoral and strategic level evaluation. This proposed Framework adapts the NIST Framework for Improving Critical Infrastructure Cybersecurity Core Functions as the main basis or template of evaluation and at the same time makes use of Annex A of ISO/IEC 27001:2013 to generate Cybersecurity Vital Signs that are needed for the proposed Framework to function efficiently and effectively. The proposed Framework evaluates cybersecurity wellness of 20 critical organisations using a Multiple Case Studies Research Method. It uses the Purposive Sampling Method to select the target organisations. Each of 114 vital signs selected contributes to an accumulated score that makes up the Cybersecurity Wellness Index of the evaluated organisations. A mixed research method was selected as the overall research design. Data was collected and vital signs were evaluated using semi-structured interviews and focus group discussions on 20 critical organisations with 12 trained trusted facilitators being deployed. Thematic Analysis was used to analyse all data collected and triangulated respectively against thematic functions and categories to generate scorecard that makes up Cybersecurity Wellness

Index of each organisation and a group of 20 organisations collectively. The research findings validate that the proposed Framework works and offers a simplified index based cybersecurity wellness maturity model that can be used to measure organisations' cybersecurity performance against evolving cyber threats dynamics.

ABSTRAK

Ancaman siber merupakan satu cabaran besar di peringkat nasional dan organisasi. Untuk menangani kedinamikan ancaman berkenaan, pihak kerajaan dan organisasi-organisasi antarabangsa telah memperkenalkan inisiatif untuk mengukur prestasi keselamatan siber di peringkat organisasi dan kebangsaan untuk mengatasi ancaman siber berkenaan dengan lebih berkesan. Sebagai contoh, agensi Pertubuhan Bangsa-Bangsa Bersatu seperti International Telecommunication Union (ITU) telah memperkenalkan Indek Kesejahteraan Siber dan negara seperti Estonia telah memperkenalkan Indeks Keselamatan Siber Kebangsaan. Dalam masa yang sama, UK telah memperkenalkan Kerangka Maturiti Pusat Keselamatan Siber Negara. Walaupun usaha telah dilakukan, kebanyakan pengukur prestasi dan indeks masa kini kebanyakannya masih memerlukan sumber yang intensif untuk dilaksanakan, memakan masa yang agak lama dan tidak begitu efektif untuk menangai suasana kedinamikan dan perubahan ancaman siber masa kini, tidak sebaik penyelesaian peringkat teknikal yang lebih pantas dan berkesan. Untuk tujuan ini, kajian ini bercadang untuk memperkenalkan satu model pengurusan yang baru dalam bentuk kerangka yang memudahkan lagi penilaian prestasi agar dapat memberi respon yang pantas bagi menandingi perubahan ancaman yang dinamik. Penyelidikan ini telah merekabentuk pendekatan secara simptomatik berpandukan kepada Kerangka Indeks Penilaian Kesejahteraan Keselamatan Siber dengan menggunakan tanda-tanda penting keselamatan siber dalam menilai risiko keselamatan siber di organisasi-organisasi kritikal. Model baru ini menggunakan indikator mudah untuk menilai dengan cepat bagi membolehkan organisasi-organisasi terlibat menjadi lebih bersedia untuk menghadapi kedinamikan ancaman siber. Kerangka ini boleh menjana indeks kesejahteraan keselamatan siber dalam setiap organisasi kritikal dan juga menjana indeks secara berkumpulan dalam masa yang sama untuk kegunaan penilaian di peringkat sektoral dan strategik. Untuk menjana indeks ini, kerangka yang dicadangkan telah mengadaptasikan Kerangka NIST sebagai panduan utama penilaian dan dalam masa yang sama menggunakan Annex A kepada ISO/IEC 27001:2013 untuk mendapatkan 114 tanda-tanda penting keselamatan siber yang diperlukan. Kerangka cadangan ini telah menilai indeks kesejahteraan keselamatan siber 20 organisasi kritikal terpilih menggunakan kaedah Kajian Kes Berganda dan Kaedah Sampel Bertujuan. Setiap dari 114 tanda-tanda penting yang terpilih itu menyumbang kepada jumlah skor prestasi keseluruhan seterusnya menjana indeks kesejahteraan keselamatan siber bagi setiap organisasi yang disampel. Data telah dikumpulkan dan tanda-tanda penting keselamatan siber telah dinilai menggunakan

interbiu separa struktur dan juga fokus diskusi berkumpulan oleh 12 kumpulan fasilitator yang mahir dan terlatih. Analisis Secara Tema telah digunakan untuk menganalisis kesemua data dan disilang-kaitkan dengan fungsi dan kategori organisasi menggunakan kaedah analisis secara bertema bagi menjana jumlah kad skor yang konsisten untuk pengiraan Indeks Kesejahteraan Keselamatan Siber bagi setiap organisasi yang disampel dan juga secara berkumpulan. Keputusan kajian ini telah mengesahkan kerangka yang dicadangkan ini dapat berfungsi dengan baik dan boleh menawarkan alternatif indeks ringkas kesejahteraan keselamatan siber. Kerangka indeks ini boleh digunakan secara efektif untuk menilai prestasi kesejahteraan keselamatan siber organisasi yang disampel mengikut kedinamikan ancaman siber yang berubah-ubah secara berterusan.

ACKNOWLEDGEMENTS

Firstly, I would like to thanks Al-Mighty God for giving me the wisdom and perseverance to go through this research work from the start to its completion. With many challenges along the way, only Al-Mighty God can help me to pull through. Secondly, I seek forgiveness from my late mother, for leaving her so long abroad, instead of taking care of her on a daily basis and she departed on 02 June 2018 while this thesis in the making. Her daily telephone calls and prayers kept me going to finish what I have started. May Al-Mighty God be pleased with her and fulfilled her prayers. Her loves, cares and mercy were in abundance and taught me to value them with honour more than anything else. Thirdly, I would like to thank my families that I had neglected while I was working to complete this thesis and I need to find some money to pay my dues. May God forgive all my weaknesses and shortcomings and compensate everyone that had been affected by these neglects. Fourthly, I would like to thank my good supervisor, Prof Omar Zakaria from the National Defence University of Malaysia, for providing me wisdoms and guidance and persevere with me during my difficult times. To him, may Al-Mighty God grant more wisdom and give him stronger will to go through his medical treatments and get well very soon. Last but not least, I would like to thank my employer, the Namibia University of Science and Technology who had entrusted me among their best lecturers, and allow me to grow profoundly and awarded me with the prestigious Teaching Excellence Award for what I was worth for. It was so gratifying and I will continue to serve with the best of my abilities before my contract lasts. To the National Defence University of Malaysia, thank you for allowing me to continue with my PhD works until the end from a distance and continue with the thesis corrections in Malaysia with good support. God bless.

APPROVAL

The Examination Committee has met on **04 January 2019** to conduct the final examination of Husin bin Jazri on his degree thesis entitled 'Cybersecurity Wellness Index Evaluation Framework for Critical Organisations'. The committee recommends that the student be awarded the Doctor of Philosophy (Computer Science).

Members of the Examination Committee were as follows.

Suzaimah binti Ramli, PhD
Associate Professor
Faculty of Defence Science and Technology
Universiti Pertahanan Nasional Malaysia
(Chairman)

Dato' Tengku Mohd bin Tengku Sembok, PhD
Professor Emeritus
Faculty of Defence Science and Technology
Universiti Pertahanan Nasional Malaysia
(Internal Examiner)

Rabiah binti Ahmad, PhD
Professor
Faculty of Information and Communications Technology
Universiti Teknikal Melaka (UTeM)
(External Examiner)

Norafida binti Ithnin, PhD
Associate Professor
Faculty of Engineering
University Technology Malaysia (UTM)
(External Examiner)

APPROVAL

This thesis was submitted to the Senate of the Universiti Pertahanan Nasional Malaysia and has been accepted as fulfillment of the requirements for the degree of **Doctor of Philosophy (Computer Science)**. The member of the Supervisory Committee was as follows.

Ts Omar bin Zakaria, PhD
Professor
Faculty of Defence Science and Technology
Universiti Pertahanan Nasional Malaysia
(Main Supervisor)

UNIVERSITI PERTAHANAN NASIONAL MALAYSIA

DECLARATION OF THESIS

Student's full name : Husin bin Jazri

Date of birth : 17 April 1964

Title : Cybersecurity Wellness Index Evaluation Framework for Critical Organisations

Academic session : Semester 1 – 2014/2015 until Semester 8 2018/2019

I declare that this thesis is classified as:

☐ **CONFIDENTIAL** (Contains confidential information under the official Secret Act 1972)*

☐ **RESTRICTED** (Contains restricted information as specified by the organisation where research was done)*

☒ **OPEN ACCESS** I agree that my thesis to be published as online open access (full text)

I acknowledge that Universiti Pertahanan Nasional Malaysia reserves the right as follow

1. The thesis is the property of Universiti Pertahanan Nasional Malaysia.
2. The library of Universiti Pertahanan Nasional Malaysia has the right to make copies for the purpose of research only.
3. The library has the right to make copies of the thesis for academic exchange.

Signature	**Signature of Supervisor/Dean of CGS/ Chief Librarian
640417-08-6715	Prof Ts Dr Omar Zakaria
IC/Passport No.	**Name of Supervisor/Dean of CGS/ Chief Librarian
Date: June 2019	Date: June 2019

Note: *If the thesis is CONFIDENTAL OR RESTRICTED, please attach the letter from the organisation stating the period and reasons for confidentiality and restriction.
** Witness

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABREVIATIONS

CERT	Computer Emergency Response Team
CI	Critical Infrastructure Organisation
CII	Critical Information Infrastructure Organisation
CIP	Critical Infrastructure Protection
CNII	Critical National Information Infrastructure Organisation
COs	Critical Organisations
GCI	Global Cybersecurity Index and Cyberwellness Profile
ICS	Industrial Control System
ICT	Information and Communication Technology
ISO	International Standard Organisation
ISMS	Information Security Management System
ITU	International Telecommunication Union
NCSI	National Cyber Security Index
NIST	National Institute of Science and Technology
SCADA	Supervisory Control and Data Acquisition
QCWF	Quick Cybersecurity Wellness Framework
WEF	World Economic Forum

CHAPTER ONE

INTRODUCTION

1.1 BACKGROUND OF THE STUDY

The dynamics of cyber threats globally have impacted many organisations that use ICT as the enabling technology for businesses (Ponemon, 2016). Some businesses were closed and many are faced with ever changing risks, and may not survive the attacks without good support systems (Ponemon, 2016). High profile cyber security breaches cases continue to prevail and are the subjects of continuous case studies (HM UK Government, 2016; HM UK Government, 2015; US-CERT, 2012). Despite many efforts and new initiatives being introduced, cybersecurity breaches have not subsided ever since the historic Code Red Worm outbreak in the year 2001 and keep on reaching to a new height year after year, with more ransomware (Renaud, 2017) and its variants (Fimin, 2017) made to the news headlines.

In order to cope with these cyber threat dynamics and its complexities, some kind of security metrics tools are urgently needed to help see what was coming and the risks associated with it (Wong, 2012). There are already some encouraging works toward measuring cyber wellness such as by the International Telecommunication Union (hereafter, ITU) in 2015 and the Estonian project which started in 2016 to provide strategic visibility at national level, just to name a few, but not many cyber security management tools out there can match the dynamics of cyber security threats (Ponemon, 2016).

As threats and harms caused by cyber-attacks have never really subsided, instead evolved into different forms and variations with new dynamics, there is an urgent need to re-examine many of our current assumptions and approaches, and look for a new position that can possibly help us to address these cybersecurity threats dynamics in a much simpler, holistic and effective way (ENISA, 2018). Thus, this research is focused to explore an alternative position, meaning something different from what is currently being practiced and implemented with the hope of a better approach and thinking