

**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 Indeks 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 menanggapi 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 thank 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 is 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

640417-08-6715

---

IC/Passport No.

Date: June 2019

---

\*\*Signature of Supervisor/Dean of CGS/  
Chief Librarian

Prof Ts Dr Omar Zakaria

---

\*\*Name of Supervisor/Dean of CGS/  
Chief Librarian

Date: June 2019

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

\*\* Witness

## TABLE OF CONTENTS

	<b>Page</b>
<b>ABSTRACT</b>	iii
<b>ABSTRAK</b>	v
<b>ACKNOWLEDGEMENTS</b>	vii
<b>APPROVAL</b>	viii
<b>DECLARATION OF THESIS</b>	x
<b>TABLE OF CONTENTS</b>	xi
<b>LIST OF FIGURES</b>	xviii
<b>LIST OF TABLES</b>	xx
<b>LIST OF ABBREVIATIONS</b>	xxiii
<b>CHAPTER</b>	
<b>1</b>	<b>INTRODUCTION</b> 1
1.1	Background of the Study 1
1.2	Problem Statement 3
1.3	Research Questions 4
1.4	Research Objectives 5
1.5	Research Significance and Contributions 5
1.5.1	Expanding the Concept of Critical Infrastructure Protection 5
1.5.2	Quick and Easy Cybersecurity Assessment Framework Blending the Combined Strength of Two Well-Known Standards 6
1.5.3	Generating a Standardised Cybersecurity Wellness Index 6
1.5.4	Using Trap Case Scenario as an Intervention Tool to Improve Reality Check 6
1.5.5	Benchmarking Multiple Organisations, Sectoral and National Levels Using the Same Framework 7
1.5.6	Approaching Cybersecurity Wellness the Same Way as Diagnosing Our Health – Using Vital Signs 7
1.6	Definition of Key Terms 8
1.7	Scope of Study 9
1.8	Thesis Structure 11
<b>2</b>	<b>LITERATURE REVIEW</b> 13
2.1	Introduction 13
2.2	Critical Infrastructure Protection Organisations and Critical Organisations 14
2.3	Current Frameworks 17

2.3.1	Cyber Wellness index by International Telecommunication Union (ITU)	17
2.3.2	National Cyber Security Index by the Etonian Government	19
2.3.3	Other Organisational Maturity Models	23
2.4	Proposed Symptomatic Approach to Cyber Security Wellness Evaluation	24
2.4.1	Symptomatic based cybersecurity wellness evaluation?	26
2.4.2	Reasons for Quick Cybersecurity Wellness Evaluation?	28
<b>3</b>	<b>RESEARCH METHODOLOGY</b>	<b>30</b>
3.1	Research Design	30
3.1.1	Suitability of Mixed Method Approach in this Study	30
3.2	Sampling Methodology	32
3.3	Data Collection	33
3.3.1	Closed-Ended Questionnaires	33
3.3.2	Semi-Structured Interviews	34
3.3.3	Focus Group Discussion	34
3.3.4	Document Review	35
3.3.5	Direct Observation	35
3.3.6	Triangulation as an important technique to correlate data	36
3.4	Data Analysis	36
3.5	Ethical Considerations	40
<b>4</b>	<b>CYBERSECURITY WELLNESS INDEX FRAMEWORK</b>	<b>41</b>
4.1	Designing a Bottom-Up Evaluation Approach	41
4.2	Design Criteria and Principles	44
4.2.1	National Institute of Standard and Technology (NIST) Approach as our Reference Work	45
4.2.2	International Standards Organisation (ISO) Approach as our Reference Work	48
4.2.3	Selecting and refining vital signs	49
4.3	Designing the weightage system	55
4.3.1	Designing 4-Levels Answers using Likert Scale	55
4.3.2	Data Qualification Criteria	56
4.3.3	Indicator of Confidence Index	56

4.3.4	Designing Cybersecurity Wellness Index	59
4.3.5	A Trap Case Scenario	61
4.4	Calculations of Cybersecurity Wellness Index	62
4.4.1	Annual Cybersecurity Incidents	62
4.4.2	Minimum and Maximum Possible Points Collected by Evaluated COs	62
4.4.3	Best Efforts Score	63
4.4.4	Calculating Cybersecurity Index	64
4.4.5	Generating Cybersecurity Wellness Index	65
4.4.6	Trap Case Scenario as a Reality Check	66
4.4.7	Sample Calculations Using Different Scenario	66
4.5	Calculating Aggregated Cybersecurity Wellness for Sectoral and Strategic Views	70
4.5.1	Aggregating and Averaging Group Index	71
4.5.2	Aggregating to Sectoral View	71
4.5.3	Aggregating to National View	72
<b>5</b>	<b>DATA ANALYSIS</b>	<b>73</b>
5.1	Semi-Structured Interviews	73
5.1.1	Facilitator One – Windhoek City Council and Nampower Ltd	74
5.1.2	Facilitator Two – United Nation Development Programme (UNDP) and Ministry of Land Reform (MLR)	77
5.1.3	Facilitator Three – Standard Bank of Namibia and Namibia Training Authority	79
5.1.4	Facilitator Four – NamClear and Namibia University of Science and Technology	81
5.1.5	Facilitator Five - MTC Namibia	83
5.1.6	Facilitator Six – Ministry of Home Affairs and Immigration and Namibia Institute of Pathology	85
5.1.7	Facilitator Seven – Ministry of Agriculture and Namibia Tourism Board	87
5.1.8	Facilitator Eight – Ministry of Finance	89
5.1.9	Facilitator Nine – Motor Vehicles Accident Fund	91
5.1.10	Facilitator Ten – Business Intelligent Property Authority and Namibia Financial Authority	92
5.1.11	Facilitator Eleven – Telecom Namibia	94
5.1.12	Facilitator Twelve – First Bank Namibia and World Health Organisation	96
5.2	Cybersecurity Wellness Index and Group Index for Semi-Structured Interviews	97

5.3	Focus Group Discussion	98
5.3.1	Facilitator One – Windhoek City Council and Nampower Ltd	99
5.3.2	Facilitator Two – United Nation Development Programme (UNDP) and Ministry of Land Reform (MLR)	101
5.3.3	Facilitator Three – Standard Bank of Namibia and Namibia Training Authority	103
5.3.4	Facilitator Four – NamClear and Namibia University of Science and Technology	105
5.3.5	Facilitator Five - MTC Namibia	107
5.3.6	Facilitator Six – Ministry of Home Affairs and Immigration and Namibia Institute of Pathology	108
5.3.7	Facilitator Seven – Ministry of Agriculture and Namibia Tourism Board	110
5.3.8	Facilitator Eight – Ministry of Finance	112
5.3.9	Facilitator Nine – Motor Vehicles Accident Fund	113
5.3.10	Facilitator Ten – Business Intelligent Property Authority and Namibia Financial Authority	115
5.3.11	Facilitator Eleven – Telecom Namibia	116
5.3.12	Facilitator Twelve – First Bank Namibia and World Health Organisation	118
5.4	Cybersecurity Wellness Index and Group Index for Focus Group Discussions	120
5.5	Key observations	121
<b>6</b>	<b>SYNTHESIS</b>	123
6.1	Final Ranking on Cybersecurity Wellness Index and Group Index	123
6.2	Comparison by Percentages of Thematic Function and Category According to Cybersecurity Vital Signs Scorecard	125
6.3	Comparison Using Cybersecurity Vital Signs	127
6.4	Graphical Representation of Results	128
6.5	Research Observations on the Proposed Framework	130
<b>7</b>	<b>CONCLUSIONS AND RECOMMENDATIONS</b>	132
7.1	Framework Evaluation	132
7.1.1	Overall Evaluations on the Proposed Framework	132
7.1.2	Applicability of the Framework	133
7.1.3	Reliability	133
7.1.4	Relevancy	134
7.1.5	Theoretical Validation	134

7.2	Research Contributions	134
7.2.1	Expanding the Concept of Critical Infrastructure Protection to Critical Organisations	134
7.2.2	Quick and Easy Cybersecurity Assessment Framework Based on Combined Strength of Well-Known World Standards	135
7.2.3	Standardised Cybersecurity Wellness Index Computation	135
7.2.4	Bottom-Up Approach in Cybersecurity Wellness Benchmarking	135
7.2.5	Trap Case Scenario as an Intervention tool to Improve Reality Check	135
7.2.6	Benchmarking Organisations with Aggregated Data to Form Sectoral and National Views Using the Same Framework	136
7.2.7	Approaching Cybersecurity Wellness the Same was as Diagnosing our Health – i.e. Using Vital Signs	136
7.3	Framework Limitations	136
7.4	Lessons Learnt	137
7.5	Future Research Works	138
7.6	Concluding Remark	139
	<b>REFERENCES</b>	140
	<b>APPENDICES</b>	144
	APPENDIX 1 - Combining NIST 2014 Framework and ISO 27001:2013 Annex A Into One Integrated and Simplified Framework (Source: NIST, 2014; ISO27001, 2013)	144
	APPENDIX 2 - Cybersecurity Questions Checklist Developed From Correlated Vital Signs	151
	APPENDIX 3 – Snapshots of Excel Template Prepared For Data Collection	171
	APPENDIX 4 –1 A Sample Letter of Consent to Participate	173
	APPENDIX 4 – 2 Annex A to the Letter of Consent to Participate	174
	APPENDIX 5 – Trusted Facilitator’s Group Declaration Form	175
	APPENDIX 6 – Extract of Data Collected by Trusted Facilitator One (1) using Semi Structured Interview	176
	APPENDIX 7 – Extract of Data Collected by Trusted Facilitator Two (2) using Semi Structured Interviews	178
	APPENDIX 8 – Extract of Data Collected by Trusted Facilitator Three (3)	180



using Semi Structured Interview	
APPENDIX 9 – Extract of Data Collected by Trusted Facilitator Four (4)	182
using Semi Structured Interview	
APPENDIX 10 – Extract of Data Collected by Trusted Facilitator Five (5)	184
using Semi Structured Interview	
APPENDIX 11 – Extract of Data Collected by Trusted Facilitator Six (6)	185
using Semi Structured Interview	
APPENDIX 12 – Extract of Data Collected by Trusted Facilitator Seven (7)	187
using Semi Structured Interview	
APPENDIX 13 – Extract of Data Collected by Trusted Facilitator Eight (8)	189
using Semi Structured Interview	
APPENDIX 14 – Extract of Data Collected by Trusted Facilitator Nine (9)	190
using Semi Structured Interview	
APPENDIX 15 – Extract of Data Collected by Trusted Facilitator Ten (10)	191
using Semi Structured Interview	
APPENDIX 16 – Extract of Data Collected by Trusted Facilitator Eleven (11)	193
using Semi Structured Interview	
APPENDIX 17 – Extract of Data Collected by Trusted Facilitator Twelve (12)	194
using Semi Structured Interview	
APPENDIX 18 – Signed Group Declaration Form and Signed Consent Form	196
APPENDIX 19 – Extract of Data Collected by Trusted Facilitator One (1)	229
using Focus Group Discussions	
APPENDIX 20 – Extract of Data Collected by Trusted Facilitator Two (2)	231
using Focus Group Discussions	
APPENDIX 21 – Extract of Data Collected by Trusted Facilitator Three (3)	233
using Focus Group Discussions	
APPENDIX 22 – Extract of Data Collected by Trusted Facilitator Four (4)	235
using Focus Group Discussions	
APPENDIX 23 – Extract of Data Collected by Trusted Facilitator Five (5)	237
using Focus Group Discussions	
APPENDIX 24 – Extract of Data Collected by Trusted Facilitator Six (6)	238
using Focus Group Discussions	
APPENDIX 25 – Extract of Data Collected by Trusted Facilitator Seven (7)	240
using Focus Group Discussions	
APPENDIX 26 – Extract of Data Collected by Trusted Facilitator Eight (8)	242
using Focus Group Discussions	
APPENDIX 27 – Extract of Data Collected by Trusted Facilitator Nine (9)	243
using Focus Group Discussions	
APPENDIX 28 – Extract of Data Collected by Trusted Facilitator Ten (10)	244

using Focus Group Discussions	
APPENDIX 29 – Extract of Data Collected by Trusted Facilitator Eleven (11)	246
using Focus Group Discussions	
APPENDIX 30 – Extract of Data Collected by Trusted Facilitator Twelve (12)	247
using Focus Group Discussions	
<b>BIODATA OF STUDENT</b>	249
<b>LIST OF PUBLICATIONS</b>	250

## LIST OF FIGURES

<b>FIGURE NO.</b>	<b>TITLE</b>	<b>PAGE</b>
1.1	Relationships between Motivation of this Research and Research Problem	4
2.1	Schematic Flows of Literature Reviews and Framework Design	13
2.2	NCSI Conceptual Framework (Source: EGA, 2016) Comparison between Cybersecurity Wellness and Cyberwellness	20
2.3	12 Indicators Used To Calculate the Index Mapping Research Problems to Design Principles and Design Criteria	21
2.4	The NCSI Score Card (Source: EGA, 2016)	21
2.5	Information Society Development Score Card (Source: EGA, 2016)	22
2.6	The Index Relation (Source: EGA, 2016)	22
4.1	Logical Flow Diagrams of the Framework Design and its Key Components	43
4.2	Example of calculating the Confidence Index	58
4.3	Snapshot of Excel Template on Confidence Index Position	58
4.4	Designing Cybersecurity Wellness Index System	59
4.5	The Proposed Cybersecurity Wellness Index Framework	60
4.6	Cybersecurity Wellness Index Template	61
4.7	Best Efforts Score	64
4.8	Example of Best Effort Score Calculation	64
4.9	Cybersecurity Index	64

<b>FIGURE NO.</b>	<b>TITLE</b>	<b>PAGE</b>
4.10	Penalty for having a Trap Case Scenario	65
4.11	Example calculation for Cybersecurity Index	65
4.12	Example calculation when a Trap Case Scenario prevails	65
4.13	Expression for Cybersecurity Wellness Index	65
4.14	Example calculation for Cybersecurity Wellness Index	66
4.15	A Best Case Scenario	67
4.16	A worst case scenario	68
4.17	An average case scenario	68
4.18	A below average case scenario	69
4.19	A Trap Case Scenario	70
4.20	Aggregating and averaging group index	71
4.21	Aggregating to a sectoral view	72
6.1	Samples of Graphical Data Analysis Presentation	129
6.2	Another Samples of Graphical Data Analysis Presentation	130
6.3	Sample of Combined Analysis Presented	130

## LIST OF TABLES

TABLE NO.	TITLE	PAGE
1.1	Scope and Delineation of this Research	10
2.1	Summary Comparison between Critical Organisations and Critical Infrastructure Protection Organisations	16
2.2	Top-Down Evaluation Criteria by the ITU-ABI Global Cybersecurity Index	18
2.3	Comparison between ITU and Estonia Evaluation Model	23
2.4	Comparison between Cybersecurity Wellness and Cyberwellness	27
3.1	Scorecard Breakdown Analysis Template	37
4.1	Mapping Research Problems to Design Principles and Design Criteria	44
4.2	NIST Framework Core Functions and Its Explanations	46
4.3	NIST Cybersecurity Framework Core (Simplified)	47
4.4	Considerations for adapting ISO 27001 security controls as vital signs for our proposed Framework	49
4.5	Mapping of the NIST Framework Core with categorisation of cybersecurity vital signs adapted from ISO Standards	50
4.6	Sample of Cybersecurity Questions Checklist Developed from Correlated Vital Signs	53
4.7	A summary of 4-level response using Likert Scale	55
4.8	Classifying Confidence Level and its Index value	56
4.9	Confidence Level Index and Its Interpretation	57
4.10	Minimum and maximum Index points that can be collected (excluding Trap Case Scenario)	63
5.1	Scorecard Breakdowns from Facilitator One	75

<b>TABLE NO.</b>	<b>TITLE</b>	<b>PAGE</b>
5.2	Scorecard Breakdowns from Facilitator Two	78
5.3	Scorecard Breakdowns from Facilitator Three	80
5.4	Scorecard Breakdowns from Facilitator Four	82
5.5	Scorecard Breakdowns from Facilitator Five	84
5.6	Scorecard Breakdowns from Facilitator Six	86
5.7	Scorecard Breakdowns from Facilitator Seven	88
5.8	Scorecard Breakdowns from Facilitator Eight	90
5.9	Scorecard Breakdowns from Facilitator Nine	91
5.10	Scorecard Breakdowns from Facilitator Ten	93
5.11	Scorecard Breakdowns from Facilitator Eleven	95
5.12	Scorecard Breakdowns from Facilitator Twelve	97
5.13	Cybersecurity Wellness Index and Group Indexes	98
5.14	Scorecard Breakdown from Facilitator One using FGD Method	100
5.15	Scorecard Breakdown From Facilitator Two using FGD Method	102
5.16	Scorecard Breakdown from Facilitator Three using FGD Method	104
5.17	Scorecard Breakdown from Facilitator Four using FGD Method	106
5.18	Scorecard Breakdown from Facilitator Five using FGD Method	108
5.19	Scorecard Breakdown from Facilitator Six using FGD Method	109
5.20	Scorecard Breakdown from Facilitator Seven using FGD Method	111

<b>TABLE NO.</b>	<b>TITLE</b>	<b>PAGE</b>
5.21	Scorecard Breakdown from Facilitator Eight using FGD Method	113
5.22	Scorecard Breakdown from Facilitator Nine using FGD Method	114
5.23	Scorecard Breakdown from Facilitator Ten using FGD Method	115
5.24	Scorecard Breakdown from Facilitator Eleven using FGD Method	117
5.25	Scorecard Breakdown from Facilitator Twelve using FGD Method	118
5.26	Summaries of Cybersecurity Wellness Index Ranking and Group Cybersecurity Wellness Index from Focus Group Discussions	120
6.1	Overall Comparisons on Cybersecurity Wellness Index	123
6.2	Comparison by Percentages of Cybersecurity Vital Signs Scorecard	125
6.3	Comparison by Selected Cybersecurity Vital Signs (Extracted From Two Data Collections Methods)	127

## **LIST OF ABBREVIATIONS**

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