

Ahmad, Arniyati (2016) *A cyber exercise post assessment framework: In Malaysia perspectives*. PhD thesis.

<http://theses.gla.ac.uk/7553/>

Copyright and moral rights for this thesis are retained by the author

A copy can be downloaded for personal non-commercial research or study, without prior permission or charge

This thesis cannot be reproduced or quoted extensively from without first obtaining permission in writing from the Author

The content must not be changed in any way or sold commercially in any format or medium without the formal permission of the Author

When referring to this work, full bibliographic details including the author, title, awarding institution and date of the thesis must be given

# A CYBER EXERCISE POST ASSESSMENT FRAMEWORK: IN MALAYSIA PERSPECTIVES

ARNIYATI AHMAD

SUBMITTED IN FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF  
*Doctor of Philosophy*

SCHOOL OF COMPUTING SCIENCE  
COLLEGE OF SCIENCE AND ENGINEERING  
UNIVERSITY OF GLASGOW

SEPTEMBER 2016

© ARNIYATI AHMAD

### **Declaration**

I declare that this dissertation was composed by myself, that the work contained herein is my own except where explicitly stated otherwise in the text, and that this work has not been submitted for any other degree at the University of Glasgow or any other institutions.

*Arniyati Ahmad*

*06 September 2016*

Some of the material presented within this dissertation has previously been published in the following papers:

### **Conference Proceedings**

1. A.Ahmad, C.W.Johnson, T.Storer. An Investigation on Organisation Cyber Resilience . World Academy of Science, Engineering and Technology, International Science Index. Page 3762-3767. 17th International Conference on Information Systems Security Management (ICISSM 2015) Conference Proceeding.July, 29-30, 2015 at Istanbul, Turkey.2015.
2. A.Ahmad, C.W.Johnson, T.Storer. Impact of Scenario Based Exercises on Organisation Resilience in Critical Infrastructure Organisations, 3rd International Conference on Technology Management, Business And Entrepreneurship Proceeding, 2014 at Malacca, Malaysia.

### **Journal Papers**

1. A.Ahmad, C.W.Johnson, T.Storer. A Cyber Exercise Post Assessment: Adoption of the Kirkpatrick Model. AISS: Advances in Information Sciences and Service Sciences. Vol. 7. No. 2. pp. 01 - 08. 2015.
2. A.Ahmad, C.W.Johnson, T.Storer. Impact of Scenario Based Exercises on Organisation Resilience in Critical Infrastructure Organisations. Journal of Technology Management and Business. Vol 2. No 1 (2015)
3. A.Ahmad, C.W.Johnson, T.Storer. An Investigation on Organisation Cyber Resilience. World Academy of Science, Engineering and Technology. International Science Index 103. International Journal of Computer, Electrical, Automation, Control and Information Engineering. 9(7), 1374 - 1379.2015.

## **Abstract**

Critical infrastructures are based on complex systems that provide vital services to the nation. The complexities of the interconnected networks, each managed by individual organisations, if not properly secured, could offer vulnerabilities that threaten other organisations' systems that depend on their services. This thesis argues that the awareness of interdependencies among critical sectors needs to be increased. Managing and securing critical infrastructure is not isolated responsibility of a government or an individual organisation. There is a need for a strong collaboration among critical service providers of public and private organisations in protecting critical information infrastructure. Cyber exercises have been incorporated in national cyber security strategies as part of critical information infrastructure protection. However, organising a cyber exercise involved multi sectors is challenging due to the diversity of participants' background, working environments and incidents response policies. How well the lessons learned from the cyber exercise and how it can be transferred to the participating organisations is still a looming question. In order to understand the implications of cyber exercises on what participants have learnt and how it benefits participants' organisation, a Cyber Exercise Post Assessment (CEPA) framework was proposed in this research. The CEPA framework consists of two parts. The first part aims to investigate the lessons learnt by participants from a cyber exercise using the four levels of the Kirkpatrick Training Model to identify their perceptions on reaction, learning, behaviour and results of the exercise. The second part investigates the Organisation Cyber Resilience (OCR) of participating sectors. The framework was used to study the impact of the cyber exercise called X Maya in Malaysia. Data collected through interviews with X Maya 5 participants were coded and categorised based on four levels according to the Kirkpatrick Training Model, while online surveys distributed to ten Critical National Information Infrastructure (CNII) sectors participated in the exercise. The survey used the C-Suite Executive Checklist developed by World Economic Forum in 2012. To ensure the suitability of the tool used to investigate the OCR, a reliability test conducted on the survey items showed high internal consistency results. Finally, individual OCR scores were used to develop the OCR Maturity Model to provide the organisation cyber resilience perspectives of the ten CNII sectors.

## **Acknowledgements**

All praises to the Almighty God for giving me the strength, knowledge and guidance throughout my life.

I am very grateful to the Ministry of Higher Education, Malaysia and my employer, the National Defence University of Malaysia, for the scholarship and study leave awarded to me.

My sincere gratitude to Professor Dr. Christopher Johnson as my main supervisor and the Head of Department of School of Computing Science, for his endless encouragement and guidance throughout this amazing journey. Without his excellent advices and motivations, this work would not have been possible. Special thanks to my second supervisor, Dr. Timothy Storer for his challenging questions, supports and great helps in this journey.

I dedicate this thesis to my dearest mother, Hajjah Mariyah Giyoo, the best ever mother in this world for her endless prayers, sacrifices, supports and encouragement throughout my life. My dedication specifically goes to my late father, Haji Ahmad Abu Bakar, for his unfulfilled dreams to see all his children successful in life.

My deepest gratitude to my dearest husband, Dr Zulkarnain Md Ali for his endless love, physical and emotional supports throughout my PhD journey. Without his infinite understanding, supports and encouragement, everything would not be easier for me. I specially dedicate this thesis to my dearest kids, Muhammad Yusof, Aisyah Humaira, Fatimah Zahra and Muhammad Yasir for their time to be with me all this while, and their unlimited emotional supports.

My sincerest thanks to my dearest siblings and all relatives; Edayurani Ahmad & family, Haji Omar Danni Ahmad & family, Hajjah Surianni Ahmad & family, Haji Zulkifli Md Ali & family, Haji Zulhisham Md Ali & family for all their prayers, helps and supports.

Special thanks to all my friends and school staffs; Dr. Ying He, Dr. Yulun Song, Dr. Md. Sadek Ferdous, Nurazian Mior Dahalan, Maria Evangelopoulou, Stefan Raue, Gianfranco Elena, Lydia Marshall, Helen McNee, Gail Reat and others who have been very helpful and understanding in this wonderful journey.

*-To my beloved family-*

# Table of Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Introduction . . . . .	1
1.2	Background of the Research . . . . .	2
1.3	Research Problem Statements . . . . .	4
1.4	Thesis Statement . . . . .	5
1.5	Research Questions . . . . .	6
1.6	Research Objectives . . . . .	6
1.7	Thesis Contributions . . . . .	7
1.8	Organisation of the Thesis . . . . .	7
<b>2</b>	<b>Literature Review on Cyber Exercises</b>	<b>10</b>
2.1	Introduction . . . . .	10
2.2	Academic Cyber Exercises . . . . .	11
2.2.1	Information Security Curriculum Development . . . . .	11
2.2.2	Information Security Skill Development . . . . .	13
2.2.2.1	Learning Assessment . . . . .	14
2.2.2.2	Lab Environment for Cyber Exercises . . . . .	14
2.2.2.3	Automation Tool for Cyber Exercises . . . . .	15
2.3	Competitive Cyber Exercise . . . . .	15
2.3.1	Benefits of Competitive Cyber Exercise . . . . .	16
2.3.1.1	Organising Cyber Exercises . . . . .	19
2.3.1.2	Tools for Cyber Exercises Performance . . . . .	20
2.4	Uses of Cyber Exercise in Other Field of Research . . . . .	21



2.5	Collaborative Cyber Exercises . . . . .	22
2.5.1	Purpose of Collaborative Cyber Exercises . . . . .	22
2.5.2	Findings on Collaborative Cyber Exercises . . . . .	23
2.5.2.1	Collaborative Cyber Exercise Categories . . . . .	23
2.5.2.2	Types of Collaborative Cyber Exercise . . . . .	25
2.5.2.3	Organising Collaborative Cyber Exercise . . . . .	27
2.5.2.4	Monitoring and Evaluation Methodologies of Collaborative Cyber Exercises . . . . .	28
2.6	Summary of Research on Cyber Exercises . . . . .	29
2.7	Chapter Contribution . . . . .	31
2.7.1	Strength and Weaknesses of Cyber Exercises Category . . . . .	31
2.8	Summary . . . . .	33
<b>3</b>	<b>Contributions of Cyber Exercises to Critical Information Infrastructure Protection (CIIP)</b>	<b>34</b>
3.1	Introduction . . . . .	34
3.2	Definitions of Critical Infrastructure (CI) . . . . .	35
3.3	Emerging Cyber Threats Targeting Critical Information Infrastructure . . .	37
3.3.1	Perpetrators Targeting CII . . . . .	37
3.3.2	Availability of Tools for Cyber Attacks . . . . .	38
3.3.3	Cyber Attacks on Critical Infrastructures Sectors . . . . .	38
3.4	Issues and Challenges in Critical Information Infrastructure Protection . . .	40
3.4.1	Nature of Cyberspace . . . . .	40
3.4.2	Dependencies and Interdependencies . . . . .	41
3.4.3	Consequences of Interdependencies . . . . .	42
3.5	Importance of Collaboration Efforts . . . . .	43
3.6	Cyber Exercise in Cyber Security Strategy . . . . .	44
3.7	Cyber Exercises Implementation . . . . .	46
3.8	Cyber Exercise in Malaysia . . . . .	48
3.8.1	National Cyber Security Policy (NCSP) in Malaysia . . . . .	48
3.8.2	Critical National Information Infrastructure (CNII) in Malaysia . .	49

3.8.3	Cyber Incidents in Malaysia . . . . .	50
3.8.4	National Cyber Exercises in Malaysia . . . . .	51
3.8.5	International Cyber Exercises in Malaysia . . . . .	51
3.9	Chapter Contribution . . . . .	52
3.10	Summary . . . . .	52
<b>4</b>	<b>A Cyber Exercise Post Assessment Framework</b>	<b>53</b>
4.1	Introduction . . . . .	53
4.2	Organising A Cyber Exercise . . . . .	54
4.3	Limitations of Cyber Exercises Post Assessment Methodologies . . . . .	56
4.4	Cyber Exercise Post Assessment Framework . . . . .	56
4.4.1	Kirkpatrick Training Model . . . . .	57
4.4.1.1	Comparison on Training Models . . . . .	58
4.4.1.2	Popularity of the Kirkpatrick Training Model . . . . .	59
4.4.1.3	Kirkpatrick Training Model in Other Research . . . . .	59
4.5	Adoption of the Kirkpatrick Training Model . . . . .	60
4.5.1	Participant Evaluation . . . . .	60
4.6	Organisation Evaluation . . . . .	62
4.7	Chapter Contribution . . . . .	62
4.8	Summary . . . . .	62
<b>5</b>	<b>An Investigation into the Impacts of a Cyber Exercise in Malaysia</b>	<b>63</b>
5.1	Introduction . . . . .	63
5.2	An Investigation into impacts of the X Maya Cyber Exercise . . . . .	64
5.2.1	Purpose of the Study . . . . .	64
5.2.2	Ethical Approval . . . . .	64
5.3	Research Methodology . . . . .	65
5.3.1	Semi Structured Interview . . . . .	65
5.4	Pilot Study . . . . .	66
5.5	Data Collection . . . . .	67
5.5.1	Sampling Strategy . . . . .	67

5.6	Demographic Data . . . . .	68
5.6.1	Experience in X Maya Exercises . . . . .	69
5.6.2	Response on Working Experience in Organisation . . . . .	69
5.6.3	Response on Working Experience in Industry Sector . . . . .	69
5.6.4	Participation in Security Training . . . . .	70
5.7	Data Analysis . . . . .	70
5.8	Categorised Results . . . . .	77
5.8.1	Level 1: Reactions . . . . .	77
5.8.2	Level 2 :Learning . . . . .	80
5.8.3	Level 3 : Behaviours . . . . .	82
5.8.4	Level 4 : Results . . . . .	83
5.9	Discussion . . . . .	84
5.10	Chapter Contribution . . . . .	86
5.11	Summary . . . . .	86
<b>6</b>	<b>A Preliminary Investigation on Organisation Resilience</b>	<b>87</b>
6.1	Introduction . . . . .	87
6.2	Scenario and Scenario-Based Exercise (SBE) . . . . .	88
6.3	Organisation Resilience . . . . .	89
6.3.1	Background of Organisation Resilience Benchmark Tool (BRT-53) .	89
6.4	An Investigation into Organisation Resilience of CII sectors . . . . .	91
6.4.1	Purpose of the Study . . . . .	91
6.5	Research Methodology . . . . .	92
6.5.1	Research Instrument . . . . .	92
6.5.2	Ethical Approval . . . . .	92
6.6	Data Collection . . . . .	93
6.7	Data Analysis . . . . .	94
6.7.1	Demographic Analysis . . . . .	94
6.7.1.1	Response on Organisation Type . . . . .	94
6.7.1.2	Response on Organisation Size . . . . .	95
6.7.1.3	Response on Participants' Role . . . . .	95

6.7.1.4	Response on Work Experiences in the organisation . . .	96
6.7.2	Reliability Analysis . . . . .	96
6.7.3	Correlation Analysis . . . . .	97
6.7.3.1	Correlation Test between SBE Experience and OR Dimensions . . . . .	98
6.7.3.2	Correlation Test between SBE Experience and OR Dimensions . . . . .	98
6.7.3.3	Correlation Test between SBE Experience with OR Indicators . . . . .	99
6.7.4	A OneWay ANOVA of OR Significant Test . . . . .	100
6.7.4.1	An Significant Test on OR between Two SBE Groups . .	100
6.8	Result Discussion . . . . .	101
6.9	Summary . . . . .	102
<b>7</b>	<b>An Investigation on Organisation Cyber Resilience of Ten CNII Sectors</b>	<b>103</b>
7.1	Introduction . . . . .	103
7.2	Cyber Resilience . . . . .	104
7.2.1	Organisation Cyber Resilience . . . . .	106
7.2.2	World Economic Forum . . . . .	106
7.3	An Investigation on Organisation Cyber Resilience of Ten CNII Sectors in Malaysia . . . . .	107
7.3.1	Purpose of The Study . . . . .	107
7.3.2	Ethical Approval . . . . .	108
7.4	Research Methodology . . . . .	108
7.4.1	Research Instrument . . . . .	108
7.4.2	Pilot Study . . . . .	108
7.4.2.1	Demographic Analysis of Participants . . . . .	110
7.4.2.2	Response on the Appropriateness Use of Language in the Survey Questions . . . . .	110
7.4.2.3	Response on the Number of Questions of Each of Component . . . . .	111
7.4.2.4	Response on the Content of Each Component . . . . .	111

7.4.2.5	Response on the Confidentiality of the Survey Questions	111
7.5	Data Collection	112
7.6	Data Analysis	112
7.6.1	Demographic Analysis	113
7.6.1.1	Response on Organisation Size	113
7.6.1.2	Response on Participants' Roles	114
7.6.1.3	Response on Work Experience in the Organisation	114
7.6.1.4	Response on Work Experience in Industry Sectors	114
7.6.1.5	Cyber Risk Management Programme	115
7.6.1.6	Participants' Involvements in Cyber Risk Management Programmes	115
7.6.1.7	Participation in Security Training	116
7.6.1.8	Participants with Security Certification	116
7.6.2	Data on Cyber Exercise	117
7.6.2.1	Response on Level of Cyber Exercise	117
7.6.2.2	Response on Types of Cyber Exercise	117
7.7	A Reliability Test on C-Suite Executive Survey	117
7.7.1	Cronbach's Alpha On C-Suite Executive Checklist Items	118
7.8	Pearson Correlation Test on Organisation Cyber Resilience Components	119
7.9	Significant Study on Organisation Cyber Resilience of Ten CNII Sectors	120
7.9.1	Data Analysis on Organisation Cyber Resilience (OCR)	121
7.9.2	Results of A One-Way ANOVA Test	121
7.10	Organisation Cyber Resilience Maturity Model	122
7.11	Result Discussion	124
7.12	Chapter Contribution	124
7.13	Summary	124
<b>8</b>	<b>Conclusion and Future Work</b>	<b>125</b>
8.1	Conclusion	125
8.1.1	Findings to the Research Question 1	125
8.1.2	Findings to the Research Question 2	126

8.1.3	Findings to the Research Question 3 . . . . .	126
8.1.4	Findings to the Research Question 4 . . . . .	127
8.1.5	Findings to the Research Question 5 . . . . .	128
8.2	Research Limitations . . . . .	129
8.3	Significant Contributions . . . . .	130
8.4	Future Works . . . . .	131
8.5	Significant Usage of the Collaborative Cyber Exercise Post Assessment Framework . . . . .	132
<b>A</b>	<b>Permission Application for C-Suite Executive Survey</b>	<b>133</b>
<b>B</b>	<b>Permission Application for Organisation Resilience Survey</b>	<b>134</b>
<b>C</b>	<b>Interview Consent Form</b>	<b>135</b>
<b>D</b>	<b>Sample of Interview Coding Script</b>	<b>138</b>
<b>E</b>	<b>A Pilot Test Survey on C-Suite Executive Checklist</b>	<b>140</b>
<b>F</b>	<b>Online Organisation Cyber Resilience Survey</b>	<b>143</b>
<b>G</b>	<b>Post Hoc of Comparison Sectors Result</b>	<b>151</b>
<b>H</b>	<b>Online Organisation Resilience Survey</b>	<b>153</b>
	<b>Bibliography</b>	<b>164</b>

# List of Tables

2.1	Comparison Summary between Capture the Flag (CTF) and Collegiate Cyber Defense Competition (CDCC) [CAB <sup>+</sup> 07]	18
2.2	Types of Cyber Exercises [GR10]	26
2.3	A Summary of Strength and Weaknesses of Cyber Exercises Categories	32
3.1	List of Cyber Attacks on Critical Sectors [MR12], [ISS14]	39
3.2	Incorporation of Cyber Exercise in Cyber Security Strategy	45
3.3	Collaborative Cyber Exercise Implementations -Part I	46
3.4	Collaborative Cyber Exercise Implementations (Continue Part II)	47
3.5	Policy Thrust and Thrust Driver in NCSP Malaysia [Has11]	49
3.6	Collaborative Cyber Exercises in Malaysia	51
4.1	Comparison of Cyber Exercises Guides	55
5.1	Interview Questions Involved X Maya Respondents	66
5.2	Interview Participants	68
5.3	Information on Interview Activities	68
5.4	Experience in X Maya Exercises	69
5.5	Response on Work Experience in Organisation	69
5.6	Response on Work Experience in Industry Sector	69
5.7	Response on Cyber Security Training	70
5.8	Code Themes for Coding and Categories Interview Data	74
5.9	Description of Themes Code	75
5.10	Inter-rater reliability for text categorisation	76
5.11	Kappa Coefficient Values and Interpretation	76

5.12	Final Category and Number of Items . . . . .	76
5.13	Results Categorised in Level 1: Reactions . . . . .	80
5.14	Results Categorised in Level 2: Learning . . . . .	82
5.15	Results Categorised in Level 3: Behaviour . . . . .	83
5.16	Results Categorised in Level 4 : Results . . . . .	84
6.1	Organisation Resilience Benchmark Tool (BRT-53) [Ste10],[WKR <sup>+</sup> 13] . .	90
6.2	Participants' Response to Organisation Resilience Survey . . . . .	94
6.3	Participants' Response on Organisation Type . . . . .	95
6.4	Participants' Response on Organisation Size . . . . .	95
6.5	Participants' Response on Role in Organisation . . . . .	95
6.6	Participants' Response on Work Experience in Organisation . . . . .	96
6.7	Reliability of OR Dimensions and Indicators . . . . .	97
6.8	Distribution of Respondents with SBE Experience . . . . .	98
6.9	Correlation between SBE and OR . . . . .	98
6.10	Correlation Test between SBE and Adaptive Capacity . . . . .	99
6.11	Correlation Test between SBE and Management Keystone Vulnerabilities .	99
6.12	Correlation between SBE Experience with OR Indicators . . . . .	99
6.13	Pearson Correlation between SBE with OR Dimensions and Indicators . . .	100
6.14	Descriptive Analysis of SBE Groups . . . . .	101
6.15	ANOVA Tests on Scenario Based Exercise Experience Groups . . . . .	101
7.1	Research on cyber resilience . . . . .	105
7.2	C-Suite Executive Checklist Survey Items [Wor12a] . . . . .	109
7.3	Demographic Analysis of Participants in the Pilot Study . . . . .	110
7.4	Response on the Appropriateness of Language of the Survey . . . . .	110
7.5	Response on the Number of Question in Survey . . . . .	111
7.6	Response on OCR's Components . . . . .	111
7.7	Response on the Confidentiality of the Survey . . . . .	112
7.8	Response in Organisation Size . . . . .	113
7.9	Response on Role in Organisation . . . . .	114



7.10	Response on Work Experience in Organisations . . . . .	114
7.11	Response on Work Experience in Respective Sectors . . . . .	115
7.12	Response on Cyber Risks Management Programme in Organisations . . . . .	115
7.13	Response on Involvement in Cyber Risks Management Programme . . . . .	116
7.14	Response on Cyber Security Training . . . . .	116
7.15	Response on Security Certification . . . . .	116
7.16	Response on Cyber Exercise Involvement by Cyber Exercise Levels . . . . .	117
7.17	Cronbach's Alpha Analysis . . . . .	118
7.18	Item Total Statistics for C-suite Executive Checklist Survey . . . . .	119
7.19	Mean and Standard Deviation of OCR, AvgGV,AvgPRG, and AvgNTW . . . . .	120
7.20	Pearson Correlation Results of OCR with of AvgGV,AvgPRG, and AvgNTW . . . . .	120
7.21	Descriptive Analysis of 10 CNII Sectors . . . . .	121
7.22	OCR One-Way ANOVA Results . . . . .	122
7.23	Organisation Cyber Resilience Maturity Stages . . . . .	122
D.1	Sample of Interview Coding Script . . . . .	138

# List of Figures

1.1	Research Direction . . . . .	5
1.2	Map of the Thesis . . . . .	9
2.1	Public and private sectors involved in cyber exercises [Adapted from [PT12]]	24
2.2	Type of cyber exercises [PT12] [Adapted from ENISA survey 2012] . . . .	27
2.3	Cyber Exercises Monitoring Methodologies [PT12] [Adapted from ENISA survey 2012] . . . . .	28
2.4	Evaluation Methodologies of Cyber Exercises [Adapted from [PT12]] . . .	29
2.5	Research Overview on Cyber Exercises . . . . .	31
3.1	CIP, CIIP and Cyber security terminologies[CS12] . . . . .	36
3.2	Dependencies and Interdependencies in Four Layers Model [Bia06] . . . .	42
4.1	A Cyber Exercise Post Assessment Framework . . . . .	57
5.1	Ethical Approval for Data Collection on X Maya Participants . . . . .	65
5.2	Data Analysis Process . . . . .	71
5.3	A Sample of Interview Transcript in Original Form . . . . .	72
5.4	A Sample of Interview Transcript in English . . . . .	72
6.1	Ethical Approval for Data Collection on Organisation Resilience Study . .	92
6.2	LinkedIn Groups . . . . .	93
7.1	Number of Respondents . . . . .	113
7.2	Response on Cyber Exercises Attended by Cyber Exercise Type . . . . .	118
7.3	Correlation Scatterplots of AvgGV, AvgPRG, AvgNTW with OCR . . . . .	120
7.4	Organisation Cyber Resilience Maturity Model of the 10 CNII Sectors . . .	123

# Chapter 1

## Introduction

### 1.1 Introduction

Critical infrastructures provide vital services that support the stability, functionality and economy of every country. Critical infrastructures include telecommunications, electrical power systems, banking and finance, transportation, water supply systems and emergency services. These sectors are categorised differently based on a country's definition of critical infrastructures [Cho10]. They are considered critical because their incapacitation or destruction would have a debilitating impact on national security and the economic and social welfare of a nation [Cav07].

As critical infrastructures are built on interconnected networks, systems and applications that support each other's interest and interact at different levels; failure in one infrastructure may impact the functionality of other infrastructures [SDPS09]. The current trends, promoting to connect anything to the Internet, has encouraged a growing number of vulnerabilities and cyber threats across industries and societies [Wig14].

Cyber threats are become more sophisticated in nature and difficult to trace. As a result, many cyber threats are difficult to identify by a single organisation [ZW12]. A collaborative information sharing on cyber threats and cooperation on cyber crisis emergency among multi organisations and sectors are necessary. As major critical services are owned by private organisation, protecting critical services and goods need a strong commitment by private and public collaboration [Nic06].

One initiative as highlighted in [LBSDG13], was through joint public and private of multi sectors in a collaborative cyber exercise as included in the national cyber security strategies in many countries. Cyber exercises as suggested by [GR10] and [PT12], are to test the preparedness of public and privates organisations against cyber threats that potentially affect organisations services. It also promotes awareness of interdependencies and vulnerabilities

among critical infrastructure organisations [WDG04]. As reported in [PT12], cyber exercises have increased in popularity. They have been conducted in Europe, UK, US, and Asia to test community preparedness on cyber crises that could potentially affect the critical information infrastructure and to boost resilience among critical infrastructure organisations [GR10],[PT12].

This chapter provides the background that motivates the research and is divided into nine sections. Section 1.2 introduces the background of the research and Section 1.3 discusses the research problems. Section 1.4 defines the thesis statement that drives this research. Section 1.5 addresses five research questions, and Section 1.6 highlights seven objectives in this research. Section 1.7 emphasises the contributions of the thesis and Section 1.8 shares publication related to this research. Section 1.9 summaries the organisation of this thesis by providing an outline of each chapter.

## 1.2 Background of the Research

Critical infrastructures, defined by the USA Patriot Act as in [Bal04] consist of two terms ; '*critical*' implies the dependence of a nation or the public on physical and information assets to the extent that loss, lack or inefficiency of any would have a serious impact. The word '*infrastructure*' denotes the basic structures and facilities necessary for a country or an organisation to function efficiently. Various threats, from natural and man-made disaster, system failures and cyber attacks could affect critical infrastructure services.

As nations and critical infrastructures became more reliant on computer networks for their operation, as suggested in [Lui12], vulnerabilities in the information infrastructure systems could be exploited to penetrate unsecured computer networks, disrupt, or even shut down critical functions. Moreover, cyberterrorism as highlighted in [Lew03], *is the use of computer network tools to shut down critical national infrastructures (such as energy, transportation, government operations), or to force or intimidate a government or civilian population*. An example of cyberterrorism were Distributed Denial of Service (DDoS) attacks on Estonia's information technology infrastructure over a prolonged period from April to May in 2007 [COT13]. The attacks targeted banking, media, police websites and paralyzing internet communication with attacks coming from 128 sources outside Estonia [COT13]. Severe economic losses were experienced due to the inability to perform online transactions [Her11]. The attacks occurred through the use of globally dispersed and virtually unattributable botnets of 'zombie' computers [Her11]. The hackers hijacked computers including many home PCs in places like Egypt, Russia, and the United States and used them in a 'swarming' DDoS strategy [Her11]. These uncovered the vulnerability of critical information infrastructures (CII) of all nations [Cav07].

The US National Research Council reported in [Wil03], the potential for attacks on control systems that has garnered serious attention around the globe. Also described in [NWD<sup>+</sup>12], that the most commonly discussed were cyber threats on industrial control systems including supervisory control and data acquisition (SCADA) systems and distributed control (DC) systems. The SCADA systems are normally used to remotely monitor data of a large geographical area and to transmit commands to remote assets such as valves and switches [Wei10]. These control systems can be found in water utilities, oil pipelines, nuclear plants, chemical plants and etcetera [MR12]. In previous practices, SCADA Systems are often isolated systems that were not connected or accessed by other networks. But, due to the need for information sharing between isolated SCADA systems are now often connected as networks. This opens up SCADA infrastructure of security and vulnerabilities as described in [FF05],[Wei10] and [MR12] .

In June 2010, a cyber worm dubbed 'Stuxnet' had struck the Iranian nuclear facility at Natanz indicated a cyber attack targeting critical infrastructure [sym10]. Stuxnet altered the frequency of the electrical current to the drives causing them to switch between high and low speeds for which they were not designed [FR11]. This switching caused the centrifuges to fail at a higher than normal rate [FR11]. According to [sym10], Stuxnet entered the computers in two ways, either through email attachments or downloaded from malicious websites . It allowed attackers to compromise systems by exploiting zero-day vulnerabilities in client-side software [FR11]. Once executed, the Trojan installed a backdoor that allowed an attacker to control the computer and perform a variety of compromising actions [NF11]. These included modifying, executing and deleting files; executing malicious files; and, most importantly, gaining access to the compromised corporation's network, which then opened up the target to additional attacks [sym10]. Stuxnet has infected over 60,000 computers in Iran; other countries affected include India, Indonesia, China, Azerbaijan, South Korea, Malaysia, the United States, the United Kingdom, Australia, Finland and Germany [FR11].

Obviously, the impact of sophisticated cyber attacks have changed the landscape of cyber-crime, enormously increasing the need for a cross-boundary collaboration [Hys07]. As suggested in [PT12], cyber exercise is an important tool to assess the preparedness of a community against cyber crises, technology failures, and critical information infrastructure incidents. This research addresses the importance of collaborative cyber exercises involved multi sectors and its contributions to national critical information infrastructure protection.

## 1.3 Research Problem Statements

There has been a long history of conducting exercises to prepare for natural disasters and other physical hazards [GR10]. However, cyber exercises did not gain significant attention until 2003, due to the focus of literature in cyber exercises are more on academic exercise, with limited resources on cyber exercise involved a collaboration of multi sectors organisations. This research investigates cyber exercise categories of academic, competitive and cyber crisis exercises involved multi sectors. Chapter 2 provides literature review of types, purposes and research of these exercises.

Critical infrastructures were often unprepared for medium and longer term disruption to their communications systems [PT12]. One reason highlighted in [The13], is the difficulties of senior management finding the time required by emergency planning groups, because organisations could not easily commit resources to the activities that have a high social value, but no significant value in financial contributions in return. Chapter 7 investigates the importance of senior management commitment to support the cyber risk that contribute to organisation cyber resilience using C-Suite Executive Checklist developed by World Economic Forum in 2012. Through the participants' perceptions, this research also investigates the involvement of senior management in nurturing cyber resilience in their organisations. Chapter 7 addresses the evaluation of organisations' cyber resilience across ten critical national information infrastructure (CNII) sectors.

In addressing this issue, government create incentives that motivate the coordination and collaboration of multiple industries in a national response program. It is important to have a national response program involving emergency coordination between the government, businesses, citizens, and other nations during a cyber-attack incident [WDG04]. The national program can provide centralized coordination especially when dealing with critical information infrastructure [Amo12]. The program should be rehearsed regularly to prepare the national response. Chapter 3 address the importance of cyber exercise as national cyber security strategy implementations in some countries like the UK, US, Europe and Malaysia.

More importantly, organising cyber exercises that involved multi sectors are challenging due to the diversity of participants' background, working environments and incidents response policies [Mar09]. How well lessons are learned from cyber exercises and how they can be transferred to the participating organisations remains a looming question [MFS<sup>+</sup>11]. Some lesson learned from cyber exercises in other countries are also discussed in Chapter 3. Furthermore, a cyber exercise post assessment framework was used to study the participants' lesson learned was addressed in Chapter 4. Subsequently, research has been conducted to investigate the importance of cyber exercises involved multi sectors and how they benefit their organisations. The details of these studies are discussed in Chapters 5, 6 and 7.

## 1.4 Thesis Statement

This thesis investigates the importance of cyber crisis exercises that involved multi sectors under Critical National Information Infrastructure (CNII) in two directions as depicted in Figure 1.1. Both studies used data collected from a cyber crisis exercise called X Maya in Malaysia:

First, it investigates how a cyber crisis exercise can benefit participants' individual learning and how their experience in the exercises is transferred to their organisation. The investigation of participants' learning uses a post assessment framework to gather and categorise interview data from X Maya participants.

Second, it investigates how the C-Suite Executives checklist can be used to assess Organisation Cyber Resilience (OCR) of CNII participated sectors. The C-Suite Executives survey was developed by the World Economic Forum in 2012. It focuses on three main components: governance, programme and network. The average score across these components contributes to the Organisation Cyber Resilience (OCR) of different sectors. Finally, based on the individual score, the Organisation Cyber Resilience Maturity Model (OCRMM) was developed for the ten CNII sectors involved with X Maya.

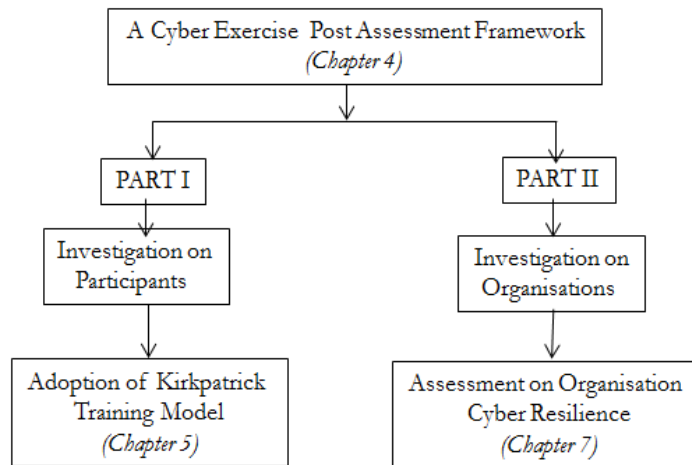


Figure 1.1: Research Direction

## 1.5 Research Questions

This research was conducted to provide answers for research questions (RQs) as addressed below:

1. RQ1: What are cyber exercises categories?
2. RQ2: How do cyber exercises contribute to critical information infrastructure protection?
3. RQ3: How can cyber exercises be beneficial to participants and their organisations?
4. RQ4: What are the impacts of cyber exercises to participants and their organisations?
5. RQ5: How to assess organisation cyber resilience of CNII sectors involved in cyber exercises?

## 1.6 Research Objectives

This study is focusing on cyber crisis exercises involved a collaboration of ten critical national information infrastructure (CNII) sectors that test a national cyber security policies and procedures. The exercise called X Maya conducted as annual cyber exercise in Malaysia. It is an important tool to boost cyber resilience in CNII sectors. The study aims to support these cyber exercises through:

1. To gather and classify information related to cyber exercises.
2. To identify cyber exercises categories from existing cyber exercises literature.
3. To identify cyber exercises implementations and contributions to critical information infrastructure protection.
4. To provide a framework for a cyber exercise post assessment.
5. To investigate the implications of X Maya to participants and their organisation.
6. To investigate the usability of organisation cyber resilience survey used to assess organisation cyber resilience of participated sectors in X Maya.
7. To assess organisation cyber resilience of CNII sectors involved in cyber exercises in Malaysia.



## 1.7 Thesis Contributions

### 1. A cyber exercises post assessment framework

This research used a post assessment framework that adopts the four-level Kirkpatrick training model to collect, code and categorise the participants interview data in order to investigate the learning outcome from four levels: reaction about the exercise, the learning skills experienced during the exercise, the behaviour developed during the exercise, and the result, i.e., how the benefits are transferred to their organisation. At the organisational level, the framework provides an assessment of organisation cyber resilience of CNII sectors involved in the exercise.

### 2. Reliability test on C-Suite Executive survey

The study has validated the internal consistency of the C-Suite Executive survey. The reliability test results on C-Suite Executive items survey showed a very high internal consistency of Cronbach alpha values of 0.976, which supports the use of survey for organisation cyber resilience assessment.

### 3. Organisation cyber resilience assessment to critical sectors

This work provides an assessment of organisation cyber resilience for ten critical information infrastructures sectors and developed an organisation cyber resilience maturity model for the sectors.

## 1.8 Organisation of the Thesis

This research is structured into eight chapters, as shown in Figure 1.2; it provides the connection between chapters with the research questions and research objectives. An overview of each chapter is as follows:

**Chapter 2 - Literature Review on Cyber Exercises:** This chapter provides background literature on cyber exercise categories. It focuses on three types cyber exercises of academic, competitive and collaborative cyber exercises. The scope, purposes and research directions of these exercises are covered in this chapter.

**Chapter 3 - Cyber Exercise Contributions to Critical Information Infrastructure Protection (CIIP):** This chapter introduces the definitions of critical infrastructure and critical information infrastructures. It discusses issues in protecting CII, including emerging cyber threats targeting critical information infrastructure. This chapter also highlights the importance of cyber exercises through the incorporation of cyber exercises in Critical Information Infrastructure Protection (CIIP) and National Cyber Security Strategies. It also describes cyber

exercises in several countries. Finally, it introduces our cyber exercise case study, X Maya in Malaysia.

**Chapter 4** - A Cyber Exercise Post Assessment Framework: This chapter explains the two main components of the research framework. The first component related to participants assessment, which adopted the four-level Kirkpatrick training model to assess the implication of the cyber exercise to participants learning effectiveness on four levels: their reaction, learning, behaviour and results from their involvement in the cyber exercise.

**Chapter 5** - An Investigation into the Impacts of X Maya Cyber Exercise in Malaysia. This chapter investigates the first part of the post assessment framework. It elaborates the implications of cyber exercise for participants using the four-level Kirkpatrick training model. This study shows of how the benefits of the cyber exercises can be transferred to participants working organisations. This chapter presents a qualitative study conducted with X Maya participants in Malaysia.

**Chapter 6** - A Preliminary Investigation on Organisation Resilience: This chapter elaborates a study on organisation resilience using organisation resilience benchmark tool developed by the University of Canterbury in New Zealand. This chapter provides the investigation on the correlation between scenario based exercise and organisation resilience of CII sectors

**Chapter 7** - An Investigation on Organisation Cyber Resilience of Ten CNII Sectors in Malaysia: This chapter presents a study conducted to assess the cyber resilience of CNII sectors involved in collaborative cyber exercises in Malaysia. It provides a detailed data analysis of cyber resilience and the development of an organisational cyber resilience maturity model for CNII sectors.

**Chapter 8** - Conclusion and Future Work: The final chapter of the thesis summarises the findings of the studies, discussing limitations and proposing new directions for future research in this area.

## A Mapping Between Research Questions, Research Objectives and Thesis Chapters

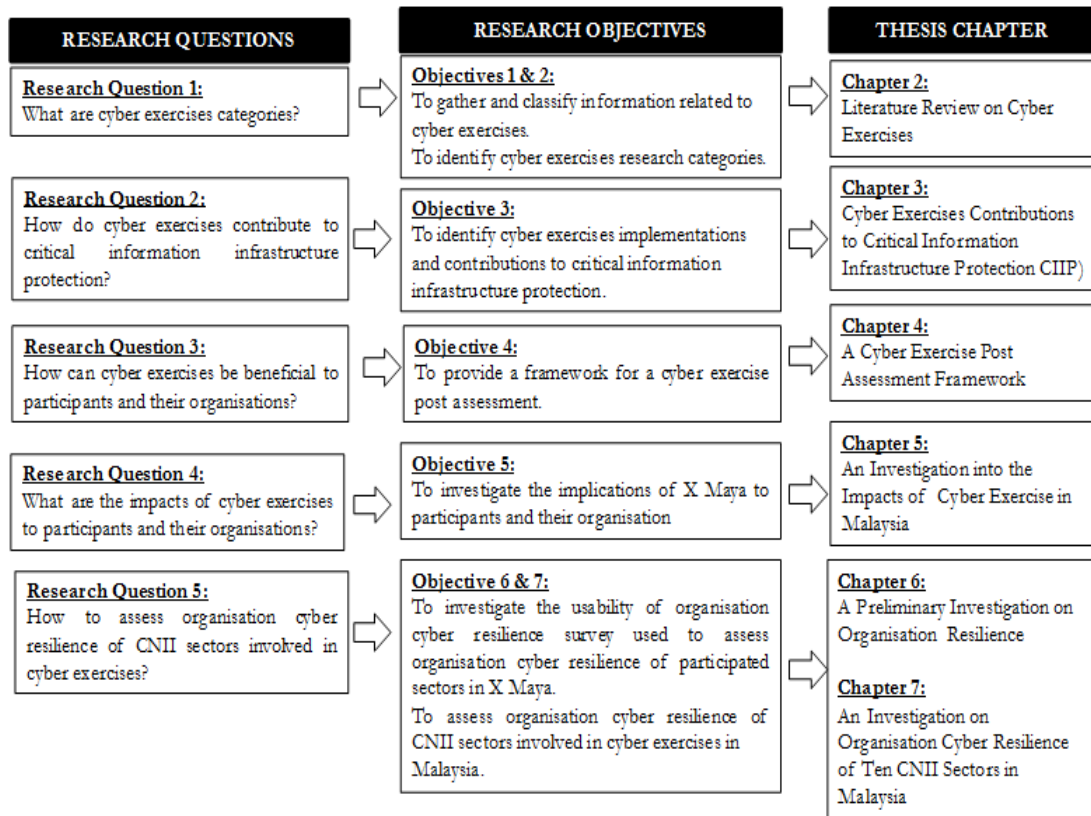


Figure 1.2: Map of the Thesis

## Chapter 2

# Literature Review on Cyber Exercises

### 2.1 Introduction

As described in [GR10], a cyber exercise is *an exercise whose objectives primarily focus on protecting, defending and recovering cyber assets and operations from a cyber attack or incident*. Many educational institutions have used and implemented cyber exercises as part of their computer science curriculum as shared in [SRB<sup>+</sup>04], [LC05],[MF06],[Gri04], [DJRR03],[SFV13],[HRD<sup>+</sup>05] and [BWS<sup>+</sup>14]. In addition, some have organised competitions with commercial partners as capstone exercises, ad hoc hack-a-thons, and scenario-driven competitions [HRD<sup>+</sup>05]. [RNS13] claimed that cyber security exercises have become powerful simulating and planning tools for training, competition, and emergency scenarios. As suggested in [AGLL09] that academic and competitive (CDX) cyber exercises designs provide a collaborative environment for sharing lesson learned and develop best practices across academies. While in [SFV13] describes a cross institutional collaboration in designing and developing hands-on practical to discover vulnerabilities in SCADA systems.

With the increasing of cross border cyber incidents and attacks, cyber crisis cross border cooperation efforts are continuously developing. Countries like the US, the UK, Australia and Japan have included collaborative cyber exercises in their cyber security strategy. Based on cyber exercises survey findings in [PT12], 84 countries worldwide have participated in multinational exercises. A total of 22 European countries were found to have conducted national cyber exercises. Existing literature on cyber exercises can be categorised into three types: academic, competitive, and collaborative.

This chapter aims to answer the first research question (RQ1), 'What are cyber exercises categories?'. It was divided into eight sections. Section 2.2 shares a review of academic

cyber exercises. Section 2.3 provides a review of competitive cyber exercises. Section 2.4 provides information on the use of collaborative cyber exercises in other area of research. Section 2.5 offers a review of collaborative cyber exercises. Finally, Section 2.6 gives a summary of research directions of cyber exercises. Section 2.7 emphasises the contribution of this chapter. Section 2.8 summarises the chapter.

## 2.2 Academic Cyber Exercises

Most literature on academic cyber exercises focuses on individual learning through formal education. Four main research topics highlighted in this category are as follows:

1. Curriculum design and development for IT, computer security education, or information assurance (IA) training that offers an active learning environment through cyber exercises. These involve several types and models of curriculum designs as shared in [SRB<sup>+</sup>04], [LC05],[MF06],[Gri04],[DJRR03],[SFV13],[HRD<sup>+</sup>05] and [BWS<sup>+</sup>14].
2. Development and assessment of the essential security skills needed in an information security career as described in [AGLL09],[DJHN09],[MF06], [DJRR03], [SFV13],[Gri04] and [ADMW10] .
3. Configuration of cyber exercise labs or environments for student learning and assessment as explained in [SRB<sup>+</sup>04],[SFV13],[BWS<sup>+</sup>14],[LC05],[WM12] and [CPH13].
4. Development of automation tools for scenario development, lab configuration, and student evaluation elaborated in [WM12].

### 2.2.1 Information Security Curriculum Development

Cyber security exercises provide professionals in academia and training industries with a tool to evaluate and assess the ability of students to apply the concepts and skills covered in their course curriculum [DJHN09]. Such exercises have increasingly been adopted as capstone exercises for training and education programs [DJHN09]. According to [BWS<sup>+</sup>14], to integrate a cybersecurity exercise into the curriculum, required some works to create and set up new hands-on exercises that can easily be adapted to any specific course. Therefore, the integration of hands-on cyber exercises into course curriculum involves several types and models of curriculum design for colleges and universities as follows:

*Hands on practice via cyber exercises in the classroom.* [SRB<sup>+</sup>04] designed and delivered four new hands-on educational exercises in information assurance (IA) for undergraduate and graduate curricula at the University of Maryland, Baltimore County (UMBC). The exercise

topics comprised 1) protection against buffer overflow attacks, 2) vulnerability scanning, 3) password security and policy, and 4) insecurity of the Wired Equivalent Privacy (WEP) protocol. Each exercise included background material, problem-solving activities, discussion questions, and supporting software and instructions for the instructor. For each exercise, the student carries out structured activities using a laptop from a mobile cart that can be rolled into any classroom. The flexibility of the modular exercises enable students to practice it in class periods of various lengths of time. It is also suitable for students at various experience levels.

*Practice hands on cyber exercise in lab.* [LC05] developed a syllabus for information security courses that contained a lab component. Lab activities required for students included : 1) writing port scanners, 2) writing a propagating virus, 3) writing an exploit program, 4) creating a shell to gain root privilege, 5) packet sniffing, 6) injecting a packet, 7) a war games competition, and 8) attack teams hacking a secure network. In addition, [MF06] discussed the IT security curriculum offered at RWTH Aachen University for a two-semester university degree : The first semester had three elements: (i) a lecture on basic concepts of computer security, (ii) a lecture on computer forensics, and (iii) a research seminar on current trends in computer security where students give a presentation. The second semester consisted of (i) a lecture on security failures in Web applications and (ii) an extensive practical lab in which students apply offensive and defensive techniques within an isolated test network.

*Cyber exercise in organisation information security management courses.* Most curriculum designs focused on the development of technical skills but lacked a focus on organisational security management. However, [Gri04] described the development and implementation of a scenario-based information security management exercise as the capstone project in a graduate business information security course at Texas A & M University. The scenario-based exercise provides students hands on experience in the planning, analysis, design, implementation, and maintenance of an organizations information security program. Successful completion of this course is a requirement for students who wish to obtain a certificate in the Management of Information Security [Gri04].

*Cyber defence exercise (CDX) in military colleges.* [DJRR03] and [AGLL09] describe the use of Cyber Defense Exercises (CDX) at a military college. Cyber Defense Exercises provide two significant benefits to the cadets at West Point: 1) education and 2) leadership development. Students were assessed on their ability to maintain network services while detecting and responding to network security intrusions and compromises.

*Use of cyber exercise for experiential learning in engineering programs.* The use of cyber exercises was not been integrated only in computer security curriculums. It has also gained significant attention in engineering programs. In Australia, educators from two universities have recognised the cultural issues of engineers with SCADA systems engineering skills

and IT personnel in network security with an IT background [SFV13]. In 2013, [SFV13] shared their experience designing a learning approach to help students to bridge this gap. The learning was developed to gain theoretical knowledge of SCADA systems vulnerabilities to cyber-attacks via experiential learning and acquire practical skills through actively participating in hands-on exercises.

*Cyber exercises as a recruitment tool for Computing Science students.* [ADMW10] described the use of cyber exercises as a computer science student recruiting tool. They used the exercise to harnesses student interest by providing an eight-hour cyber training and competition framework designed to be attended by computer science candidates .

### 2.2.2 Information Security Skill Development

Hands-on cyber exercises have been integrated with the Information Security curriculum as discussed in Section 2.4.1 to provide the four main foundational skill sets of Information Assurance:

*Administrator Skills.* Administrator skills are important to provide students with technical and practical knowledge in configuring networks, servers, databases, and application to create information assets and systems for the business environment and operations as mentioned in [FPB10] and [AD<sup>+</sup>06]. Moreover, [BWS<sup>+</sup>14] suggested the development of a security mind-set with analytical skill. The necessary analytical skill as described in [BWS<sup>+</sup>14] is the ability to think about how systems can fail and be made to fail in different ways. These skill enables people to understand the reasons for these relationships, and the ability to draw meaningful conclusions or inferences [BWS<sup>+</sup>14].

*Defensive Skills.* Defensive security skills are needed for information security students to understand how to configure and manage various types of security equipment [HRD<sup>+</sup>05]. Students must know how to use tools and techniques to monitor normal and abnormal activities performed in the business environment and address any vulnerability that can risk the operations and functionality of the business [AD<sup>+</sup>06]. This is a continuous process that involves 1) creating security policies, 2) implementing security measures, 3) monitoring the security state, and 4) fixing any vulnerability found.

*Offensive Skills.* Offensive skills synonymous with hacking [LC05]. Student use these skills to test security measures. These skills are needed to perform penetration tests. Students must know how to use hackers tools and techniques to find vulnerabilities in systems and business environments [LC05]. Moreover, [MF06] conducted an experiment to prove that teaching offensive methods yields better security professionals than teaching defensive techniques alone.

*Forensic Skills.* Forensic skills are the ability to identify the source of threats and their impact on systems, and to restore systems function as described in [MF06] and [CAB<sup>+</sup>07].

### 2.2.2.1 Learning Assessment

Regarding the use of cyber exercises to measure outcomes against security standards, [DJHN09] explained how measure performances against specific standards. He presented an indexed matrix to be included in cyber exercises. The index matrix was a cross-referencing between the exercise objectives and selected standards. This approach can be used as a foundation for cyber exercise development and as a performance measurement against specific standards [DJHN09].

### 2.2.2.2 Lab Environment for Cyber Exercises

Several types of lab or environment settings are used to conduct cyber exercises for learning and assessment:

*Isolated Lab.* In 2004, [SRB<sup>+</sup>04] suggested, to prevent inadvertent damage to other systems, exercises that involve dangerous programs (e.g., worms, viruses, and attack tools) must be safely isolated. An isolated lab is extremely beneficial for students to learn how to manage systems through direct experience by acting as administrators of an actual system. This includes making mistakes and recovering from them [SRB<sup>+</sup>04]. Furthermore, such a lab can provide experience of real computers and network hardware, which students can experiment with [WM12]. In [SJ03] discussed the Information Warfare Analysis and Research (IWAR) Laboratory. This is an isolated laboratory with a heterogeneous environment and that has become a vital part of the IA curriculum at West Point. The lab was designed and developed by a West Point cadet (student) team. As highlighted in [WM12], the limitation of this lab is that it can only be accessed on campus, is isolated from all other network, and is expensive to maintain .

*Virtual Lab.* In [CPH13] discussed the benefits of virtual labs over physical labs as follows: 1) less time is required to set up the lab, 2) it reduces the cost of licensing software, and 3) it is easy to use because it is simple to copy a configured virtual machine to the desktops in a lab. They also shared the design of a virtual lab using the VMwares vSphere platform with vCloud Director that is used to support the academic needs of more than 400 students .The authors provided a key set of requirements for setting up a hands-on lab [CPH13] : 1) the lab must be Internet accessible, 2) the lab must be the same for on- and off-campus students, 3) the lab must be self-contained, 4) the lab must allow self-provisioning, 5) the lab must perform well, and 6) the lab needs to be easy to use. Even virtual lab offers cost reduction and ease of maintenance, it is lacking in providing a real organisation environment.



### 2.2.2.3 Automation Tool for Cyber Exercises

A number of tools have been developed to manage and organise cyber exercises:

*Tele-Lab*. [WM12] explained about a Tele-Lab platform that combines a virtual lab with a Web-based training system that allows remote lab access through the Internet. Such a lab is suitable for local classes and for self- and distance-learning approaches.

*Intelligent Training Exercise Environment (itee)*. [ETM15] elaborated about an intelligent training exercise environment (ITEE), a fully automated Cyber Defense Competition platform. The essential features of an ITEE are as follows: 1) automated attacks, 2) automated scoring with immediate feedback using a scoreboard, and 3) background traffic generation. The main advantages of the platform are that 1) it provides easy integration into existing curriculum, 2) the platform is highly automated to enable execution with up to 30 teams by one person using a single server, 3) the platform implements a modular approach called learning spaces for implementing different competitions and hands-on labs, and 4) the ITEE platform was successfully tested during a live CDX and has proven useful during several hands-on classes in the context of a university curriculum.

## 2.3 Competitive Cyber Exercise

Competitive cyber exercises enhance academic exercises by providing a platform for participants to demonstrate their knowledge and skills in controlled environments. The use of competitive cyber exercises as an active and collaborative learning environment allows coursework to be tested in real environment [Con06]. Furthermore, topics can be set at varying degrees of difficulty during hands-on competitions, including [SMR<sup>+</sup>14] network design, system administration, cost-benefit analysis, forensics, and leadership [AGLL09].

[AGLL09] argued that CDX should be part of any computer security curriculum to strengthen and enhance classroom learning. The Cyber Defence Exercise or CDX was an early computer security competition designed to foster education and awareness among future military leaders [AGLL09]. The exercise highlighted the important role of information assurance (IA) in protecting the nations critical information systems [SRS<sup>+</sup>02]. CDX challenges teams of students from each academy to design, build, and successfully defend a real-world computer network against simulated intrusions.

Most competition participants demonstrated more enthusiasm about using their skills in a cyber environment. Competitive cyber exercises are purposely used to channel this enthusiasm and interest [HRD<sup>+</sup>05]. As addressed in [AGLL09], many students have commented that they have learned more in the CDX preparation and execution rather than the rest of their four years as a computer science student.

[Con05] highlighted that the purpose of competitions are to provide an educational environment for students to critically examine their abilities. The assessment is different from a standard examination because : 1) it is team based, which allows students to work in teams and capitalise on different team members strengths and 2) it is conducted over three days with continuous feedback to the teams, enabling them to make changes in their approaches and activities in response to the measured effectiveness. The overall result of the exercise was that the teams, students, and faculty members achievements in the competition [Con05]. Most literature on competitive cyber exercises focuses on six main topics as follows:

1. Types of competitive cyber exercises described in [HRD<sup>+</sup>05],[BKGT11] and [CAB<sup>+</sup>07].
2. Scale of competitive based cyber exercises addressed in [HRD<sup>+</sup>05].
3. Guidelines to organise a competitive cyber exercises also provided in [DJRR03], [FPB10], [PF09] and [Mat07]
4. Competition Infrastructure was shared in [CPH13].
5. Assessment rules and methodologies involved in the competitive cyber exercise provided in [WM08] and [CAB<sup>+</sup>07].
6. Development of automation tools for participants' performance evaluation were shared in [SMR<sup>+</sup>14] and [CRC<sup>+</sup>12].

### 2.3.1 Benefits of Competitive Cyber Exercise

Competitive cyber exercises enhance academic exercises by providing students with a platform to practise their knowledge and skills in a real environment. Several benefits of the Cyber Defense Competition (CDX) over academic cyber exercises:

*CDX provides an integrated environment.* One of the major problems of an information security program is that knowledge and skill sets are learned through different classes in separate modules. As suggested in [BKGT11], the CDX competition provides knowledge integration, which is the key to successful college learning. CDX allows students to demonstrate their understanding and skills with respect to network security at a detailed level in an integrated environment .

*CDX apply classroom learning to a real-world situation.* Subjects that are difficult to address in the classroom can be dealt with in the competition environment, which mimics a real organisation's work setting [BKGT11]. Besides offering curriculum-based lessons, the exercise also offers lessons in teamwork, leadership, and coordination, as participants must

deal with change, and work with other students or faculty from other departments as mentioned in [HRD<sup>+</sup>05] and [AGLL09].

Literature on competitive cyber exercise topics share the experience of organising and participating in school competitions, the Collegiate Cyber Defense Competition (CDCC), or Capture the Flag (CTF) exercises:

*School Competition Cyber Exercise.* Schools were assessed on their students ability to maintain network services while detecting and responding to network security intrusions and compromises as described in [AGLL09] and [DJRR03].

*Collegiate Cyber Defense Competition (CDCC).* In a CDCC setup, each student team is assigned to a network that must be defended and secured [HRD<sup>+</sup>05],[Con06]. As described in [CAB<sup>+</sup>07], at the beginning of the exercise, student teams are given a grace period of a few hours before the competition to take an inventory of their networks. They also try to secure and patch all the equipment. After the grace period ends, outsider attackers start to attack their networks. This *red team* tries to penetrate the network. Attacks are run against all of the teams, and if successful, further attacks are leveraged against the penetrated systems [CAB<sup>+</sup>07]. There is also a *white team* of industry professionals who act as judges and monitor the network to verify that services are operational. They score the teams on the completion of business tasks throughout the competition. Scoring is based on keeping required services up, preventing security breaches, and completing business objectives throughout the two days of competition. These tasks contribute to the overall scores of the teams. As described by [CMZ10] and [BKGT11], the team with the most points wins and goes on to compete at the US National CDCC .

*Capture the Flag (CTF).* [CSM08] described CTF cyber exercise competitions, which involve both offensive and defensive components. Students are assigned to a machine or network that they must defend against attack while simultaneously attempting to hack into their competitors networks. Points are awarded for successfully breaking into a machine as well as successful defence [CAB<sup>+</sup>07]. Students use existing security toolkits to assess a scenario and gain points by obtaining flags. These flags require varying degrees of skill and test students knowledge [FPB10] . However, unlike other events, it requires a very diverse skill set, has a strong focus of teamwork, and emphasise the ability to convey results as well as achieve specific technical objectives as referred in [CSM08] and [DEC<sup>+</sup>11].

[CAB<sup>+</sup>07] compared the International Capture the Flag Competition (iCTF) and the National Collegiate Cyber Defense Competition (CCDC). The International Capture the Flag Competition (iCTF) conducted in 2005 involved 21 teams from universities in North America, Europe, South America, and Australia. While the National Collegiate Cyber Defense Competition was organized by the University of Texas at San Antonio with major sponsorship from the U.S. Department of Homeland Security. Four regional cyber game competitions

were held across the U.S. included Southeast, Mid Atlantic, Southwest and Midwest. Regional champions were held and a team was jointly fielded by five U.S. military academies. The comparison was based on the competition approach, competition scale, complexity of the competition environment, rules of the competition, and scoring mechanism as listed in Table 2.1.

**Table 2.1** Comparison Summary between Capture the Flag (CTF) and Collegiate Cyber Defense Competition (CDCC) [CAB<sup>+</sup>07]

	<b>iCTF05</b>	<b>CCDC06</b>
Defense vs. Offense	Offense (without red team)	Defense
Content	Focused on detective work	Emphasizes task completion with some considerations given to detective work and problem solving
Scale	International, fully distributed	Competitions conducted in a single location with the organizers controlling all the machines
Complexity of Environment	Consisted of a single Linux image loaded on VMware for each site. All sites are connected via a virtual network	Multiple machines and network devices with a mixture of operating systems
Rules	All competition network traffic had to be on the competition network. Teams were allowed to have external Internet access without monitoring	All traffic had to go through competition network. No external media allowed. Only freeware or approved commercial software was allowed.
Scoring	Based on service availability, flags captured, and original exploits. Except for evaluating original exploits, scoring is automated	Equally based on task completion, service availability, and red team assessments. A combination of manual and automated scoring.

### 2.3.1.1 Organising Cyber Exercises

In organising a competitive cyber exercise, there are four essential components: the competition approach, competition environment and scale, performance assessment in the competition, and competition designs steps that should be considered:

*Competition approach.* Competition designs could be based on several approaches as suggested by [SH12] and [FPB10] 1) defence oriented, 2) offense oriented, or 3) mixed approaches. A defence-oriented setup will involve one or several teams that defend systems against attacks.

An offense-oriented setup will involve one or several teams carrying out attacks. Defensive teams are often called *blue teams* and offensive teams are often called *red teams*. Mixed approaches involve both active blue teams and active red teams, where the red teams attack the blue teams' systems or all teams attack each other [FPB10]. Two other types of actors are frequently involved in competitions: members of green and white teams [FPB10]. The *green team* manages the environment and ensures that the systems used in the competition operate as intended and that all actors have proper access to the environment [SH12]. The *white team* referees the competition and manages the incentives for the red and blue teams by creating the competition rules and scenario [PF09].

Furthermore, the configuration of the competition can be based on three generic models as proposed in [HRD<sup>+</sup>05] : 1) participants receive only requirements and must develop their own systems or networks; 2) participants receive pre-configured systems and services that they must maintain and protect; or 3) participants receive specific systems and a network configuration and must protect them.

*Competition environment and scale.* The competition environment normally managed by the green team includes [SH12]: the network topology, operating systems, application software, configuration, and user account. As in academic cyber exercises, the competition cyber exercise environment can also employ virtual, heterogeneous, isolated, or distributed network configurations. For the competition scale as stated in [CAB<sup>+</sup>07], that small-scale cyber exercises are often used as capstone exercises for projects, while large-scale exercises are organised in a distributed way.

*Performance assessment in the competition.* During the competition, students are strictly limited in both time and the actions they can perform during the exercise [HRD<sup>+</sup>05]. The competition should objectively assess the participants' skill set within the competition period. The participants must be assessed after completion, specifically with regard to knowing where and when attacks occurred, whether attacks were identified, and how they were addressed [HRD<sup>+</sup>05]. Thus, a scoring system must be designed to measure the students' performance during the competition.

The scoring mechanism must be either manual or automatic to count participants' points. As suggested in [CAB<sup>+</sup>07] 1) task completion, 2) the availability of services, and 3) penetration assessment as three categories to score cyber game participants. The availability of services measures participants' ability to keep required services (e.g., a Web server or mail server) running [CAB<sup>+</sup>07]. Two types of penetration assessment measures are required: 1) participants' ability to prevent attackers from accessing the computer system and 2) ability to design new ways to gain access to others' computer systems [CAB<sup>+</sup>07].

In [WM08] suggested another scoring system in which the winner will be determined by the largest number of points earned during the competition. A team may accumulate up to 6,000 points from the various measurements of availability and assessment of performance during injections. The accumulated point values are set as follows:

1. Functional services (based on periodic polling interval of core services): 2000 points
2. Successful completion of assigned business tasks: Points are awarded based on complete or partial fulfilment of the assigned task and will vary by task with an aggregate total of 2000 points
3. Red team assessments: Red teams will rate the relative security of the student teams with a possible total of 2,000 points. The red team will have access to the service availability information to assist them in the determination of their scores.

*Competition Design Steps.* Competition design involves seven steps as suggested in [FPB10] and [PF09] involved: 1) determine the objectives of the exercise, 2) select the competition approach based on the competition objectives, 3) develop the topology or setting for software and hardware, 4) build a scenario for the exercise, 5) set up rules for the competition, 6) provide metrics for measuring the efficiency of the competition, and 7) gather lessons learned by participants and the organiser.

### 2.3.1.2 Tools for Cyber Exercises Performance

The development of tools to automate the organisation of competitive cyber exercise includes the following:

*Tracer FIRE software.* The software provides participants with a set of commonly used cyber security software tools [SMR<sup>+</sup>14]. It also provides detailed measures of moment-to-moment activities. The Tracer FIRE software environment has been instrumented to log the use of software tools, including the opening and closing of windows, the content of windows and keystrokes, and mouse clicks within each window [SMR<sup>+</sup>14]. These logs provide a detailed record of participant behaviour within the context of specific challenges that may be

combined with data concerning correct or incorrect answer submissions, time committed to challenges, and the abandonment of challenges [SMR<sup>+</sup>14].

*CyberCog software.* It designed to emulate a number of tools frequently used for cyber security defence tasks, such as security alert monitors, network and system logs, network maps, network vulnerabilities, user databases, and Internet-based data sources. It also provides a Web-based system populated with data for analysis during a competition [CRC<sup>+</sup>12].

## 2.4 Uses of Cyber Exercise in Other Field of Research

Sections 2.3 and 2.4 shared the usage of cyber exercises in learning context. But the use of cyber exercises are not limited for educational purposes only, this section addresses the adoption of cyber exercises to support research from other domains:

*Competition network data as a source of labelled dataset.* Research on network data analysis to test network security techniques and intrusion detection systems has used labelled data available from the DARPA 1998 and 1999 attack datasets. The dataset traffic is labeled in specific criteria to support security analysis. However, the DARPA datasets have declined over time because of aging content and continually emerging threats. To overcome the shortage of labelled datasets, [SOC<sup>+</sup>09] demonstrated how network data from cyber exercise competitions can be instrumented to generate modern labelled datasets.

*Cyber exercise to understand problems in water distribution systems.* [GOS06] designed a red team/blue team exercise to help water utilities understand the dynamics of the distribution system contamination problems. The red team simulates the contamination of a water distribution system and the blue team defends the system by installing monitors to detect the presence of the contaminant (CWS) .

*Testing on industry system operation.* Cyber exercises can also identify particular threats to specific industries. Through cyber exercises, safety-critical engineers are encouraged to consider adverse behaviour that might be the result of malware rather than a more routine coding or configuration error. The diagnosis of any attack requires interaction and coordination between IT service providers, who often have a minimal understanding of the safety-critical nature of particular operations [Joh12].

*Investigation on investment decisions on cyber security.* An exercise involved over twenty five players was conducted at a workshop of the Institute for Information Infrastructure Protection (I3P) addressing Process Control Systems (PCS). The exercise explored the impact of potential government regulation on the complex decision processes of determining appropriate investment levels for added cyber security by individual companies. At the workshop the exercise provided an opportunity for knowledgeable security professionals to collaborate and

compare their investment decisions against those of other similar companies and against the results of the expected value decision analysis[CCHL]. Details of research on collaborative cyber exercises address in Section 2.5.

## 2.5 Collaborative Cyber Exercises

As critical information infrastructures are based on complex systems of interconnected networks [O'R07], security involves complex collective problems. Because of the interdependencies and tight coupling between systems [SDPS09], any risks faced by organisation will require significant multi-organisational action across organisations [WDG04]. Collaborative cyber exercise provide a platform to simulate large scale attacks across sectors, industries and government.

A collaborative cyber exercise is an important tool to assess the preparedness of a community against cyber crises, technology failures, and critical information infrastructure incidents [PT12]. Furthermore, collaborative cyber exercises promote information sharing that helps a community to detect potential risks and prevent cyber attacks at an early stage. It also facilitates incident response activities in communities [ZW12].

In addition, collaborative cyber exercises help organisations to strengthen their critical information infrastructure by preparing for actual cyber interruptions [PT12]. It provides evaluations and objective assessments of existing cyber incident response policies and procedures [WDG04]. Through such exercises, cyber incident response plans can be developed, refined, and tested [RMM10].

### 2.5.1 Purpose of Collaborative Cyber Exercises

There are three different reasons to conduct collaborative cyber exercises as defined in [WDG04]:

*Awareness exercises.* This is the simplest exercise, which aims to expose the participants to the threats and issues of a particular domain, and make participants aware of their responsibilities. The goal of this exercise is to bring individuals together, to make them aware of possible security events which their organisation might experience. This will help them to formulate a response and how to get staff involved with such response.

*Education and training exercises.* The goal of education and training exercises, is to prepare participants with response techniques, that they maybe required to perform when security incident occur. The training exercise is used to train the participants, who are aware of security issues but are not trained in current technology or methods to address the threats.



*Drill exercises.* A drill exercise is conducted in order to provide participants opportunities to practice processes, procedures and tools to respond to events in a specific domain. The purpose of this exercise is to test participants' ability, to detect and respond in a coordinated manner to an attack or disruption.

The following collaborative objectives were most frequently highlighted in a survey of 84 cyber exercises in [PT12]:

1. To build awareness of cyber threats;
2. To examine the capabilities of participating organisations to prepare for and respond to the effects of cyber-attacks;
3. To identify and highlight roles, responsibilities, and authority for responding, as well as to test decision-making and procedures between public and private actors;
4. To assess cyber security emergency readiness, prepare, test, and evaluate (national) procedures and processes;
5. To raise awareness of infrastructure interdependency issues with a particular focus on cyber security;
6. To build trust among states, enhancing interstate and inter-agency cooperation.

## 2.5.2 Findings on Collaborative Cyber Exercises

### 2.5.2.1 Collaborative Cyber Exercise Categories

Survey results by [PT12] on public and private sector involvement in cyber exercises in Figure 2.1, revealed that 57% of the exercises involved joint exercises between public and private sectors, while 41% involved public sectors and 2% involved private sector only. The results shown that the lacking of private sectors in testing their security and contingency plans. This is important because of major critical infrastructures belong to the private sectors.

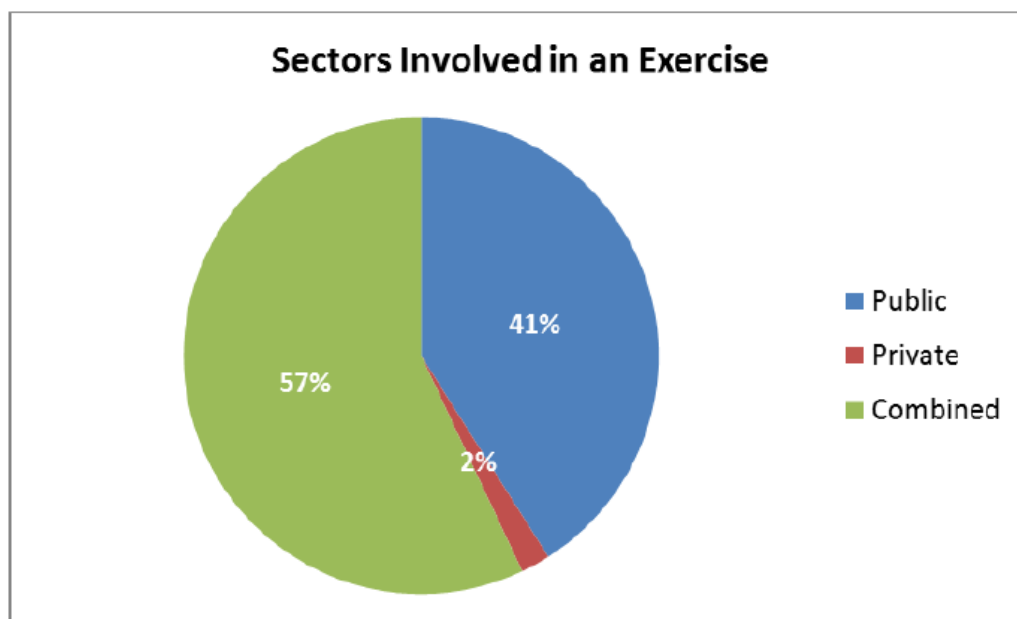


Figure 2.1: Public and private sectors involved in cyber exercises [Adapted from [PT12]]

[WDG04] described joint public and private exercises as:

*Sector or industry level exercises.* Sector or industry level exercises involve multiple organisations; external entities to an organization, such as customers, suppliers, peer or competing firms; and assorted government agencies. These exercises are challenging to organise and require a high degree of cooperation and coordination between entities.

An example of this type of exercise was UK White Noise, the first full-scale exercise conducted in 2009. This was developed by a joint government and industry forum known as the Electronic Communications Resilience and Response Group (EC-RRG). The exercise focused on communications failure with cascading effects across the whole public switched telephone network (PSTN) [Whi10].

*Cross-sector exercises.* Cross-sector exercises involve two or more industries and require a high level of coordination. The need for exercises at these levels is important to understand the impact of interdependencies between industry sectors.

The Blue Cascade cross border tabletop infrastructure interdependencies exercise was held on June 12, 2002 in Welches, Oregon. It was conducted by the Pacific North West Economic Region (PNWER) and cosponsored by the U.S. Navy, Federal Emergency Management Agency (FEMA Region 10), and the Canadian Office of Critical Infrastructure Protection and Emergency Preparedness (OCIEP). The exercise involved more than 150 representatives from 70 private and public sector organisations. The exercise focused on the linkages between and among infrastructures that could make the Pacific Northwest vulnerable to cascading impacts in the event of an attack or disruption, and which could complicate response

and recovery. Critical infrastructures participating in the exercise included energy (electric power, oil, and natural gas), telecommunications, transportation, water supply systems, banking and finance, emergency services, and government services [Blu02].

*Community based exercise.* Community-based exercises include local government operations represented by local law enforcement, emergency operations, and city management. If a local utility is owned or operated by the city, it is represented by critical infrastructure firms. These include telecommunications, local hospitals, ports, and universities [CW06].

For example, the Cyber Storm I community exercise, was conducted in February 2006. It was organised by National Cyber Security Division (NCSD) under the US Department of Homeland Security (DHS). The full-scale cyber exercise provided participants with a controlled environment in which to exercise a coordinated cyber incident response, including information sharing mechanisms, procedures for establishing situational awareness, public and private organisational decision making, and public communications during a cyber incident related to national crisis [Cyb06].

Over 100 public and private agencies, associations, and corporations participated in the exercise from over 60 locations and 5 countries. The exercise included participation of more than 30 private sector corporations and associations in its planning, execution, and after action analysis. The exercise scenario simulated a large-scale cyber campaign affecting or disrupting multiple critical infrastructure elements primarily within the energy, information technology, transportation, and telecommunications sectors [Cyb06].

### 2.5.2.2 Types of Collaborative Cyber Exercise

[GR10] defines two types of cyber exercises as in Table 2.2:

**Discussion-based.** Discussion-based exercises enable planners and participants to examine scenarios, develop response procedures, test those procedures, and test decision-making. Participants discuss topics developed based on the scenario rather than acting them out. Such exercises include seminars, workshops, tabletop exercises, or games as described in [EO09] and [GR10] are as follows :

*Seminar.* Seminar provides an overview of new plans, strategies, concepts, ideas, instructions and discussion of plans and procedures, to instruct staff of new or changed procedures.

*Workshop.* In a workshop, experts and managers gather to engage in a constructive discussion of a theoretical scenario, considering implications, procedures, interdependencies, and decisions. This exercise is useful for jointly developing new procedures to cope with possible incidents.

*Tabletop.* In a tabletop exercise, participants work through a scenario and existing procedures. A facilitator will guide participants through the session, while participants describing

the procedures they would use and the decisions they would make as the scenario unfolds. This exercise is useful for preparedness and familiarity with procedures.

*Game.* A game is similar to a tabletop exercise except that participants are divided into two or more teams that work through the scenario separately in a competitive atmosphere. A game also used to explore decision making process and the consequences of these decisions.

**Operations-based.** Operations-based exercises enable the testing of procedures in practice. They are often narrow to focus on a specific operation or function, such as a drill to test a communications link, or they may involve a larger scale, involving the coordination of different departments or organisations. They can be much larger in scale, involving many organisations, many departments, and large numbers of people acting out their roles through a scenario.

**Table 2.2** Types of Cyber Exercises [GR10]

Discussion Based Cyber Exercise	Operation based Cyber Exercise
Tabletop Exercise (TTX)	Simulation
Seminar	Drill
Workshop	Functional Exercise
Game	Full Scale Exercise

The results of a survey reported in [PT12], as presented in Figure 2.2, showed that 43% of the exercises executed were distributed tabletop exercises, 19% were full-simulation exercises, and 5% were workshops. Types of exercises described in [PT12] :

*Desk check.* Use in early-stage of validation for a new plan or amendments to a plan. It involved one-to-one discussion with the author of the planned procedures against a simple scenario to demonstrate the stages that are in place and how they operate.

*Comm check.* Use to validate systems or infrastructures. A different form of initial activity used to validate communications methodologies or notification systems.

*Walk through.* The response team convenes to consider planned procedures and roles. The response team is convened in one room and a simple scenario is used to demonstrate the progression of the planned responses and what each responder should do.

*Command post.* Used to enable a team to test their response facilities. Usually involve management-level only. Response center based with role-play of players and the external environment.

*Full simulation.* Use to stress test the players with a real time environment that is close to reality. Players respond in real time, immediately as information is received, interacting with other teams and role players as the response requires.

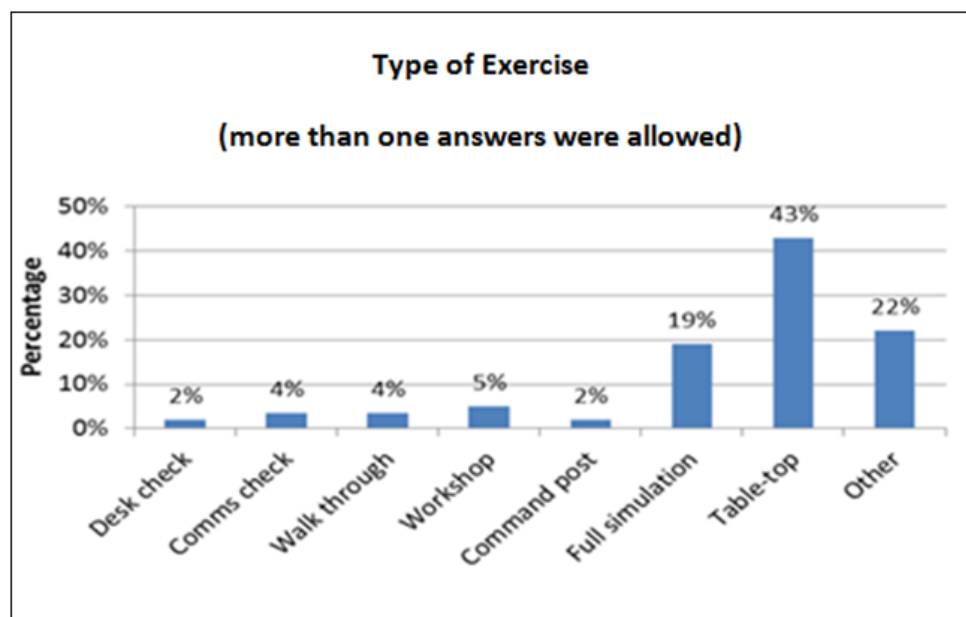


Figure 2.2: Type of cyber exercises [PT12] [Adapted from ENISA survey 2012]

### 2.5.2.3 Organising Collaborative Cyber Exercise

There are several guidelines provided by [PT12], [EO09] and [GR10] for organising a cyber exercise. These guidelines systematically examine the life cycle of a cyber exercise, which involves the following phases :

#### *Phase 1: Identifying the exercise*

In the first phase, the organiser must determine a need for an exercise, including the identification of procedures or measures that should be explored. Based on the need, organisers can select the type of exercise to be conducted and the organisations that need to participate.

#### *Phase 2: Planning the exercise*

In the second phase, the organiser engages in the planning process. This will involve recruiting the participants; acquiring financial resources for the exercise; selecting (and booking) the location; developing the scenario, rules, tools, and training materials for the exercise; selecting monitors and other role-players and specifying what and how they will perform their duties; and planning the evaluation process.

#### *Phase 3: Executing the exercise*

In this phase, the exercise is executed as specified in the planning process. Participants are involved either through discussion or simulation of the scenario and their response procedures and decisions. Monitors observe and note these actions and inject information into the scenario.

#### *Phase 4: Evaluating the exercise*

Finally, exercise evaluation is conducted after the exercise is completed. This process tends to include a final evaluation report or multiple reports tailored to different audiences. These reports review the exercise, identify weaknesses, and recommend improvements. Furthermore, this process may be followed by a forum to address identified weaknesses and recommendations.

#### **2.5.2.4 Monitoring and Evaluation Methodologies of Collaborative Cyber Exercises**

The findings of stocktaking survey in [PT12], as shown in Figure 2.3, defined the monitoring methodologies of cyber exercises as real-time monitoring, status report, the use of experts for monitoring, and other combined methodologies. The survey revealed that 31% of cyber exercises used real-time monitoring, 27% used experts for monitoring, 22% used periodic status reports, and 20% of used a combination of methodologies.

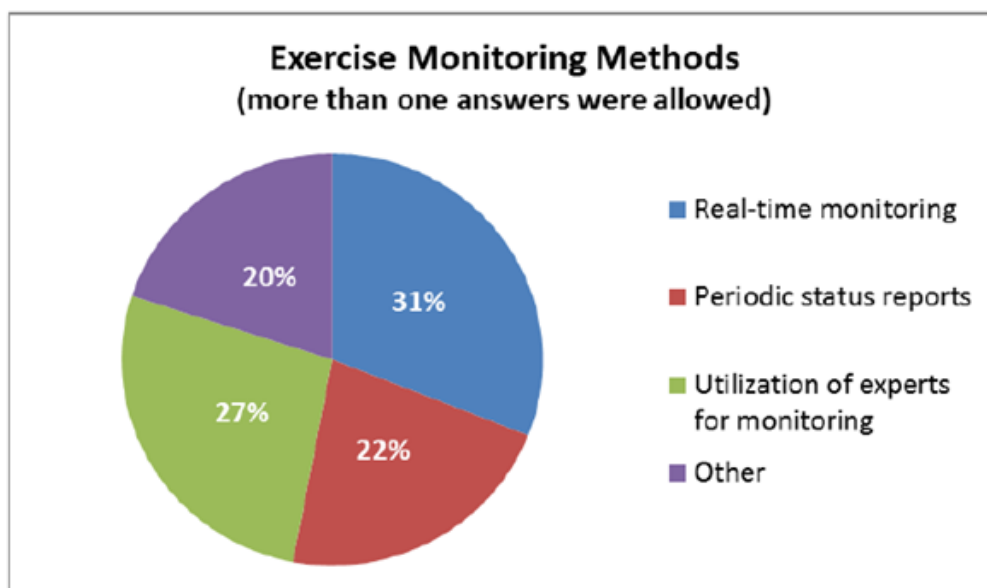


Figure 2.3: Cyber Exercises Monitoring Methodologies [PT12] [Adapted from ENISA survey 2012]

Figure 2.4 illustrates the survey findings in [PT12], showing the post evaluation methods used in collaborative cyber exercise. Reports were the most evaluation method used for post assessment (31 %), followed by Other (24%), Hot Washed session (17%), Debriefing Workshop (16%) and Self-evaluation (12%). These cyber exercise evaluation methodologies are explained as follows:

*Report.* The cyber exercise post evaluation report as described in [PT12] is a tool used to inform the organiser about the overall achievements and the results of the exercise.

*Debriefing.* Debriefing after the exercise when participants are brought together to describe what had occurred to account for the actions that had taken place and to develop new strategies as a result of experience. The purpose of the debriefing is to provide information to participants about what they have gone through rather to gather information from them [Led92].

*After Action Review (AAR).* AAR is an analytical review of training events that enables the training audience to examine actions and results during a training event through a facilitated professional discussion [Jas14].

*Hot Wash.* The *hot wash* session described as a discussions and evaluations of an agency's (or multiple agencies') performance following an exercise [RB13]. A hot wash discussion used to capture comments and suggestions while the exercise is still fresh in participants' minds [AS12]. The session should be led by a moderator and consist of a focused discussion on what worked well, what must improve, and what the organisation should consider for the next exercise [GR10],[AS12]. Further discussion on the limitation of collaborative cyber exercise evaluation methodologies are explained in Chapter 4.

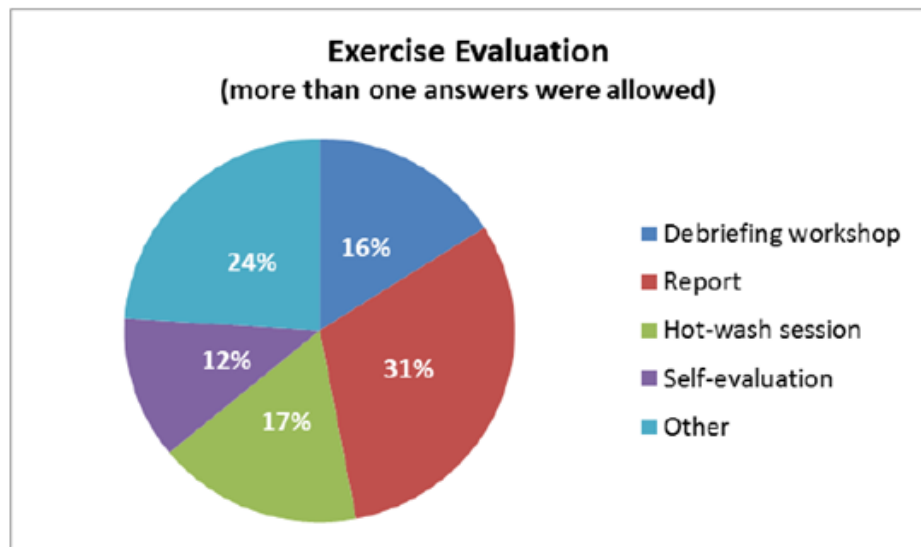


Figure 2.4: Evaluation Methodologies of Cyber Exercises [Adapted from [PT12]]

## 2.6 Summary of Research on Cyber Exercises

Figure 2.5 illustrates a summary of research on academic, competitive, and collaborative cyber exercises as described in previous sections. Academic cyber exercises highlight four main research topics: curriculum design and development, technical skills development and assessment, lab configurations for cyber exercise environments, and newly developed automation tools for practising cyber exercises. The focus of academic cyber exercises is on

developing individual skills needed for information security. The performance measurements are tightly based on the designed module and curriculum objectives.

The focus of competitive cyber exercises is on sharing experiences through participating and organising competitions with three different approaches, school exercises, the Collegiate Cyber Defense Competition (CDCC), and Capture the Flag (CTF), which are organised as annual events at the regional, national, and international levels. Most research on these competitions addressed the environment of the exercise, which can involve virtualisation and distributed settings. The competition infrastructures are supported by manual and automated tools. The focus of competitive exercises is on team performance. Participants are forced to apply their knowledge and skills to analyse and understand unfamiliar, complex sets of interdependent components that are similar to real-world networks and malware infrastructure. The competition simulated infrastructure is used to test participants ability to build and defend a network from attackers. For the performance measurement, several methodologies are used, either manual or automated, to score the competition and to determine the winner.

Collaborative cyber exercises are used to simulate operational cyber exercises to test community preparedness in emergency situations related to cyber incidents. Collaborative cyber exercises involve participants from industries, governments, and academia to test their awareness of current threats, interdependencies among sectors, and communication during the incidents. Collaborative cyber exercises are also used to test the policies and procedures of emergency preparedness at the organisational, national, and international levels. Collaborative cyber exercise performance evaluation uses the post-assessment methodologies of reports, debriefing, hot wash, and after-action review to review the overall exercise, identify weaknesses, and recommend improvements for the next exercise. As this chapter provides the research overview of collaborative cyber exercise, more implementations of collaborative cyber exercises in critical information infrastructure protection discussed in Chapter 3.



## 2.7 Chapter Contribution

This chapter provides a general overview of academic, competitive, and collaborative cyber exercises in terms of the purpose, scope, and research direction of the exercises.

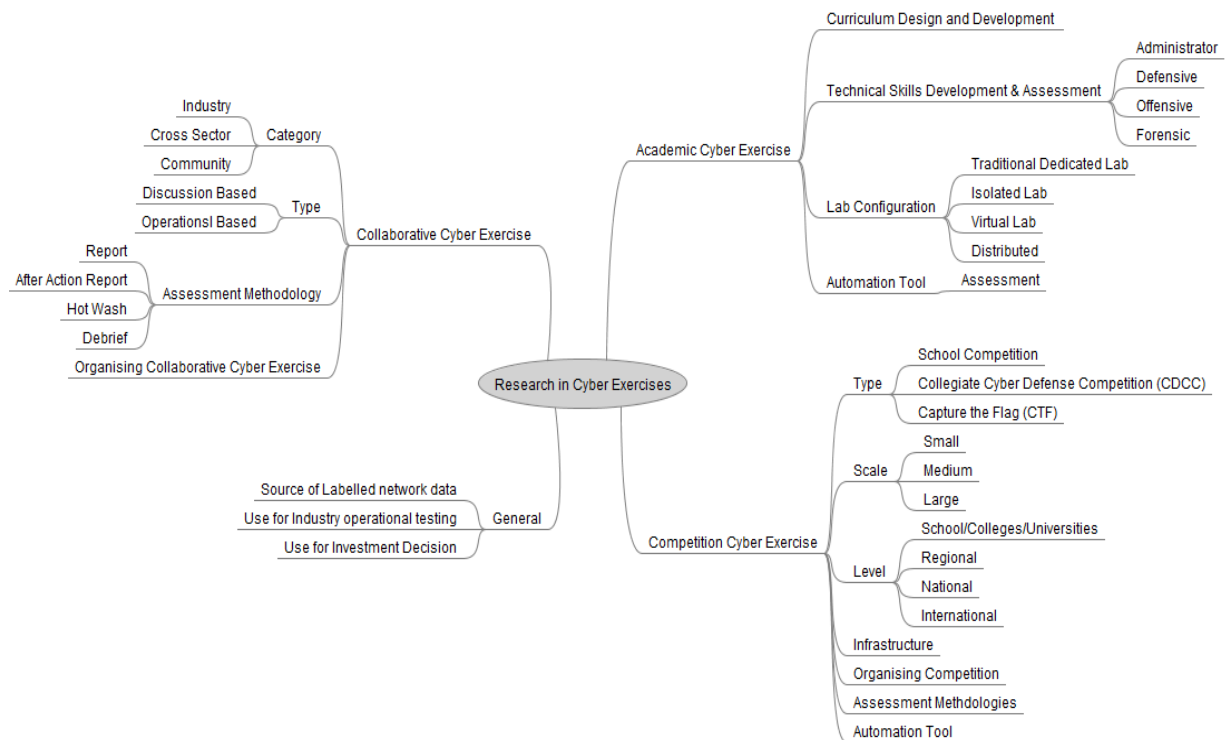


Figure 2.5: Research Overview on Cyber Exercises

### 2.7.1 Strength and Weaknesses of Cyber Exercises Category

This section provide a summary of strength and weaknesses of cyber exercises by category as describe in Table 2.3.

**Table 2.3** A Summary of Strength and Weaknesses of Cyber Exercises Categories

Cyber Exercise Category	Strength	Weaknesses
Academic Cyber Exercise	<p>1)Used to develop fundamental skills of information security personnel.</p> <p>2)Used in curriculum design for Information security courses</p> <p>3)Labs were provided for practising the knowledge.</p> <p>4)Student practise their skills in campus within control environment.</p>	<p>1)Curriculum oriented, might limit the important knowledge and skills needed.</p> <p>2)Assessments were individual based and rigidly following the curriculum.</p> <p>3)Limitation of skills can be practised because limitation in the curriculum designed which might not cover theories and skills needed</p>
Competitive Cyber Exercise	<p>1)Used to provide a platform for students to practise their security skills and knowledge in competition settings.</p> <p>2)Skills and knowledge can be practise in integrated manner, not limited to specific curriculum.</p> <p>3)Student team with highest point will be rewarded and win the competition.</p>	<p>1) Assessments have different criteria based on type and levels of the competition. Every type of competition has its own assessment methodology.</p> <p>2)Student needs to perform within limited time and resources.</p>
Collaborative Cyber Exercise	<p>1)Promote cooperation across multi sectors and cross borders.</p> <p>2)Provide platform for collaboration and knowledge sharing.</p> <p>3)Global coverage of cyber crisis.</p>	<p>1)The cyber exercise involved many sectors and people with varies in background and skills.</p> <p>2)Varieties in background cause difficulties to assess the effectiveness of the exercise.</p>

## 2.8 Summary

This chapter provides a literature review of three types of academic, competitive and collaborative cyber exercises. Academic, cyber exercises have become an important tool to provide hands-on learning and assessment environments for information assurance students in college, universities, and the training industry. The advancement of networks, operating systems, and software has enhanced the cyber exercise environment into virtual, distributed, and remote access, which make learning easier to conduct on and off campus. Students are not limited to developing their security knowledge and skills in class and lab activities. They can further explore and apply their skills through competitive cyber exercises, which help them to strengthen their understanding and knowledge on how to monitor, maintain, and protect network operations. Simulated operations used in competitive cyber exercises were used in collaborative exercises to test the preparedness of communities against cyber crises, technology failures, and critical information infrastructure incidents at organisation, state, national and international levels.

## **Chapter 3**

# **Contributions of Cyber Exercises to Critical Information Infrastructure Protection (CIIP)**

### **3.1 Introduction**

Academic, competition-based and collaborative cyber exercises have been discussed in Chapter 2. The main purpose of academic and competition-based cyber exercises are developing participants' skills and knowledge, while collaborative cyber exercises differ in scope, which involved multiple organisations at national and international levels. Exercises simulate cyber operations across multiple organisation to highlight the awareness of interdependencies, to coordinate in cyber emergency situations, and to promote cooperation and communication during a cyber crisis. This chapter highlights the importance of cyber exercises by focusing on the contributions of these exercises to CIIP. This chapter continues to answer the second research question, of (RQ2): how do cyber exercises contribute to critical information infrastructure protection?.

This chapter is divided into ten sections, Section 3.2 identifies several definitions of critical infrastructure (CI) and explains issues related to CIIP, while Section 3.3 discusses the emerging cyber threats that target critical information infrastructure (CII) and the effect of cyber attacks on CI in some countries. Section 3.4 dicusses issues and challenges cyber security in CII. Section 3.5 highlights the importance of collaboration efforts for CIIP. Section 3.6 discusses the importance of cyber exercises through the incorporation of cyber exercises in cyber security strategies and Section 3.7 shares cyber exercises implementations in some countries. Section 3.8 shares the background of critical national information infrastructure (CNII) in Malaysia including the national cyber security policy (NCSP), cyber incidents that

happened in Malaysia, and national and international collaborative cyber exercises activities. Section 3.9 shares the contributions of this chapter, and Section 3.10 summaries the chapter.

## 3.2 Definitions of Critical Infrastructure (CI)

Definitions of CI are different between countries as highlighted in [Cho10]. Various definitions of CIs in some countries are reviewed here. The UK defines its critical national infrastructure (CNI) as *'critical certain elements of infrastructure, the loss or compromise of which would have a major, detrimental impact on the availability or integrity of essential services, leading to severe economic or social consequences or to loss of life'* [cpn09]. In the UK, infrastructure is divided into the nine sectors: food, energy, water, ICT, transport, health, emergency services, government, and finance. Assets within these that have been identified by the government to be of importance to basic service delivery and national security are collectively known as CNI [cpn09].

Critical Infrastructure, as defined in [Bal04], is as follows: *Systems and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters* .

The National Strategy for Homeland Security in the US has identified the following 14 areas of CI as: agriculture and food, water, public health, emergency services, government, defence industrial base, information and telecommunications, banking and finance, energy, transportation, chemical industry and hazardous materials, postal and shipping, national monuments and icons, and critical manufacturing [Bal04].

In Australia, is defined as *those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would adversely impact on the social or economic wellbeing of the nation or affect Australias ability to ensure national security*[CIP10]

In Germany, *critical infrastructures are organisations or institutions with major importance for the public good, whose failure or damage would lead to sustainable supply bottlenecks, considerable disturbance of public security or other dramatic consequences*[CIP09]. [CS12] argued that in various definitions of CI, the focus alternates between physical and virtual aspects of CI, because there are no official distinctions between CI and CII, and both terms were interchangeably used in some countries .

Current debates in critical infrastructure protection (CIP) and CIIP topics alternate between defending the physical aspect of CI and the protection of data and software residing on computer systems that operates these physical infrastructures [CS12]. According [CS12],

both CIP and CIIP terms should not be discussed as separate concepts. These concepts are shaped by three main components: CIP, CIIP and National Information Infrastructures (NII), as depicted in Figure 3.1. While CIP is more than CIIP, CIIP is an essential part of CIP [CS12]. However, there is at least one characteristic to differentiate between the two: While CIP comprises all critical sectors of a nation's infrastructure, CIIP is only a subset of a comprehensive protection effort, as it focuses on securing the critical information. The concept was addressed as [CS12]:

- The CIIP is only a subset of a broad Critical Infrastructure Protection (CIP) effort, which targets on Critical Information Infrastructure (CII).
- The CII defined as part of the global or NII that is essential for the continuity of critical infrastructure (CI) services.
- Cyber security is defined by International Telecommunication Union (ITU) as, '*the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets*'.

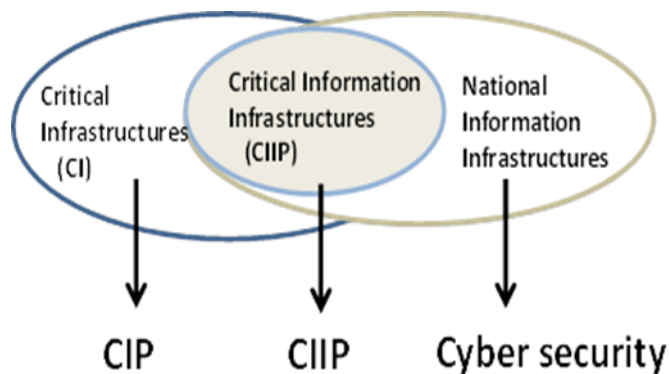


Figure 3.1: CIP, CIIP and Cyber security terminologies[CS12]

The importance of CII serves as a backbone of CIs that provide a continuous exchange of data, which is crucial to the operation of infrastructures and the services that they provide [Cav07]. Due to the role of CII in intertwining various other infrastructures, if not properly secured, this provides possibilities that they can be targeted as a source of attack [Bia06]. Thus, protection on CIs should strongly focus on the protection of specific information infrastructures rather than focus on all CI sectors and other aspects [CS12]. In conjunction to the importance of CIIs, in providing continuous support to the essential services, this study focuses on collaborative cyber exercises as collaborative protection efforts in CIIP, as shared in Section 3.6.

### 3.3 Emerging Cyber Threats Targeting Critical Information Infrastructure

The CII is a subset of CI, as described in Figure 3.1, which is composed of a vast range of components and systems, extending from hardware (satellites, routers), to software (operating systems, applications, databases), to data (database tables), and processes and operations [Hys07]. Moreover, CII are vulnerable to natural hazards, human errors and technical problems. In addition, they are also vulnerable to cybercrimes by hackers, criminals, state actors and terrorists.

The US National Infrastructure Protection Plan (NIPP) defines vulnerability as *the characteristics of an asset, system, or networks design, location, security posture, process, or operation that render it susceptible to destruction, incapacitation, or exploitation by mechanical failures, natural hazards, terrorist attacks or other malicious acts* [O'R07].

Normally, vulnerability assessments are conducted by private-sector infrastructure owners, stakeholders, and government agencies to identify asset, facility, system, and other vulnerabilities. Cyber-attacks have increased dramatically in sophistication and have been able to sabotage CIs, although the cyber defences are in place [Cav07]. Threats to CII involve various sectors and share cross-border vulnerabilities and interdependencies, which are explained as follows:

#### 3.3.1 Perpetrators Targeting CII

[Cav07] and [Nic06] described potential perpetrators targeting CII are ranging from teenagers, crackers, sophisticated expert hackers, criminal, terrorists and even nation as :

*Crackers, Malicious, Hackers and Script Kiddies.* Individuals, who have differing levels of technical expertise that break into systems by challenging security mechanisms. They launch attacks for thrill or for boasting rights in their communities.

*Insider Threats.* Disgruntled insider in an organisation is a major threat. An insider may not have a great deal of knowledge about computer intrusions, but his/her knowledge of and access to the targeted system enables the possibility of causing considerable damage.

*Malware Writers.* Malicious code writers produce software (viruses, worms or Trojan horses) designed specifically to damage or disrupt systems. This so-called malware can be specific (i.e., it targets particular systems or organisations), or it can be generic.

*Criminal Groups.* Criminal groups frequently attack systems for monetary gain. Their attempt to steal sensitive information for resale or for blackmail, extorting money by threaten-

ing to attack computing assets, and for committing various types of fraud (e.g., attempting to influence stocks) or forgery (e.g., changing payment information in invoices).

*Hactivist.* Hacktivism refers to politically-motivated attacks on computing assets. Hacktivists may overload e-mail servers or hack into websites to send political messages. Their actions against infrastructure assets are usually motivated by environmental, safety or nationalistic reasons.

*Terrorist Group.* Terrorism is the unlawful use of force or violence against persons or property in order to intimidate or coerce a government or civilian population to further certain political or social objectives.

*Information Warfare.* Several nations are aggressively developing information warfare doctrines, programs and capabilities. These capabilities can be used to disrupt the supply chain and cause considerable damage to the various infrastructure sectors, ultimately affecting the economy and the residents of the targeted region or country.

### 3.3.2 Availability of Tools for Cyber Attacks

Unlike natural disasters and man-made and many other areas of risk to human welfare, there is very limited organised historical data to estimate on cyber-attacks, successful attacks, and consequences of the attack. According to [Amo12], in all cases, cyber-attacks are less effective and less disruptive compared to physical attacks or natural disaster. The only advantage is that cyber-attacks are cheaper and easier to carry out compared to physical attacks.

However, as network performance and bandwidth have advanced, attack methods and attack tools have reached a maturity that could easily be used for cyber-attacks. With automated tools freely available on the Internet, cyber-attacks can be performed remotely within a few seconds, and the attacks easily launched and challenging to trace [Nic06]. Several attacks involving CII in some countries are presented in Section 3.3.3.

### 3.3.3 Cyber Attacks on Critical Infrastructures Sectors

The existence of cyber threats has been reported since 1980s and has been rapidly increasing. Beside the scope of attack that cross borders, threats has evolved from destructive threats to espionage mission, as described in Table 3.1



**Table 3.1** List of Cyber Attacks on Critical Sectors [MR12], [ISS14]

Year	Attack	Target	Sector	The Impacts of the Attack
2012	Gauss Malware	Iran, Lebanon, Syria, Sudan	Finance	The Gauss code includes commands to intercept data required to work with several Lebanese banks (e.g., Bank of Beirut, Byblos Bank, and Fransabank).
2011	Night Dragon	Five global energy and oil firms	Energy	SCADA systems werent directly attacked, but 5 global energy and oil firms companies that operate SCADA were attacked. Operational blueprints were reported stolen
2010	Stuxnet	Iranian nuclear facility at Natanz	Nuclear	Stuxnet altered the frequency of the electrical current to the drives causing them to switch between high and low speeds for which they were not designed. This switching caused the centrifuges to fail at a higher than normal rate [FR11].
2007-Now	Red October	Diplomatic and governmental, agencies, research institutions,energy, nuclear groups, trade and aerospace	ICT	Infiltrated over 1000 high level government computers around the world. There are sensitive geopolitical information being stolen, 7 terabytes stolen data and 55,000 connection targets within 250 different IP addresses, Switzerland, Kazakhstan and Greece.
2005	Daimler Chrysler	Manufacturing plants and business	Manufacturing	Infected business and industrial control network causing 13 manufacturing plants to shut down production lines costing 1.4 million Dollar
2000	Maroochy Water Systems	Maroochy Shire, Australia	Water	The Maroochy Shire attack was not one attack but a whole series of attacks over a prolonged period

As failure of CII considered being a significant risk in global society, securing CII security systems and their sub-systems is crucial. The overall CIIP requires broader community attention, including from academia, the private sectors, and government who must work together to understand emerging threats and to develop proactive security solutions to safeguard CIIs and their reliance [Hys07].

### 3.4 Issues and Challenges in Critical Information Infrastructure Protection

In the US, the Presidents 2013 Executive Order produced the National Institute of Standards and Technology (NIST) Cyber security Framework Version 1.0, of the voluntary standard, which is being implemented by individual companies to assess and improve cybersecurity, as well as to create a common language for discussion and collaboration on security intelligence and response tactics [LEP<sup>+</sup>13].

Moreover, the International Critical Information Infrastructure Protection (ICIIP) handbooks have included research reviews on 25 countries that shared the importance of CIIP through development of security strategies and collaboration efforts between public and private to better understand the vulnerabilities and threats to their CII [BS09]. Some possible solutions have also been drafted to protect their CII assets. Several cybersecurity issues that are discussed in the book also expressed demanding needs to effectively protect the CIIs from cyber threats. The effects of cyber threats that potentially disrupt CII operations and services to the nations are discussed next [PF07] :

#### 3.4.1 Nature of Cyberspace

In February 2003, the National Strategy to Secure Cyberspace (NSSC) specifically defines cyberspace as the hundreds of thousands of interconnected '*computers, servers, routers, switches and cyber optic cables that make ... critical infrastructures work*' [PF06]. To expand the complication of cyberspace, a new term, the Internet of Things (IoT) has been defined in [Wig14] as '*an environment in which objects, animals or people are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction*'. The IoT has evolved from the convergence of wireless technologies, micro-electromechanical systems (MEMS) and the Internet [Wig14].

It is well known that cyberspace is globally designed without a single owner or a controller and provides broad open access to anyone, anywhere in the world [PF07]. Although cyberspace is pervasive, CII components rely heavily on cyberspace resources for their operation [Hys07]. To emphasise this, Gartner, Inc. forecasts that 6.4 billion connected things

will be in use worldwide in 2016, up 30 percent from 2015, and will reach 20.8 billion by 2020 [vdM15]. In 2016, 5.5 million new things will get connected every day [vdM15]. The impact of the sudden expansion of the internet use will boost the economic effect of the IoT to consumers, businesses, city authorities, hospitals, and many other entities [vdM15]. Unfortunately, this also encouraged a growing number of adversaries looking to use cyberspace to steal, compromise or destroy critical data, which will increase the disruptive influence across all industries and all areas of society [Wig14]. Thus, protecting and controlling the cyberspace are overwhelming challenges.

### 3.4.2 Dependencies and Interdependencies

Identifying, understanding and analysing such dependencies and interdependencies of CIs are significant challenges due to the wideness and complexity of the CIIs as described in Section 3.4.1. These infrastructures, which affect all areas of daily life, include electric power, natural gas and petroleum production and distribution, telecommunications (information and communications), transportation, water supply, banking and finance, emergency and government services, agriculture, and other fundamental systems and services that are critical to the security, economic prosperity, and social wellbeing of nations [Hys07]. The CIs have a broader range, covering an economy branch or sector and are closely related to the CIs of other countries or even regions [O'R07]. There are several perspectives in envisioning the high level of CIs interdependencies. For these reasons, the 3.2 distinguishes CIs intra-dependencies and interdependencies as represented in a high level model with four layers [Bia06] as follows:

- *The physical infrastructure layer.* This layer consist of physical devices and infrastructures, such as building, an electric plant with power distribution lines, oil/gas pipelines and pumps, and telecommunications cables service provider that deliver essential services.
- *The cyber layer.* This layer contains computers, networks and data gathering sensors such as ICT systems, automation control (PLC and SCADA), and supervision systems, which are used to monitor and control the physical layer. Most SCADA systems are the main part of this layer.
- *The organizational layer.* This layer contains main business functions involving the whole organisation through communication and interaction of people, processes, and systems.
- *The strategic business layer.* This layer consists of top management, strategic management and policy makers of the CI stakeholder

Intra-dependencies exist between physical infrastructure, cyber layer, organisational layer, and strategic layer that contribute to CII of each sector. The interdependency between varying sectors of CI is one of the most essential relationships that shape the CII [Bia06]. Today, CI functions depend solely on an extensive network of infrastructures that are highly connected, forming a complex mesh of interdependencies which facilitate exchange of services of various forms.

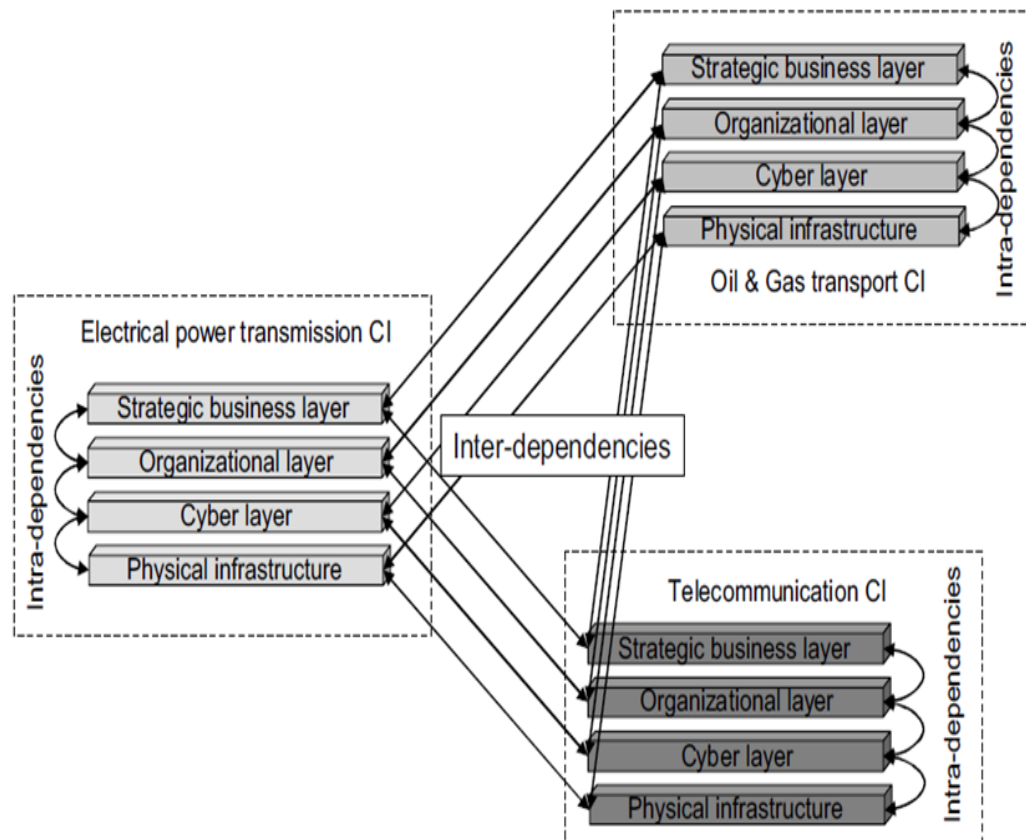


Figure 3.2: Dependencies and Interdependencies in Four Layers Model [Bia06]

In addition, [PDHP06] identified that interaction in CI can be through direct connectivity, policies and procedures, or geospatial proximity. These interactions often create complex relationships, dependencies, and interdependencies that cross infrastructure boundaries, rendering the entire system extremely complex and prone to domino failures [O'R07]. The effects of disruption involving interconnected systems are discussed in Section 3.4.3.

### 3.4.3 Consequences of Interdependencies

As explained in Sections 3.4.1 and 3.4.2, CIIs are complex system that interlink and demand high requirements in availability, resilience and security [Bia06]. It is important to raise awareness of these interdependencies among CI owners and operators [Bia06]. Any failures

affecting interdependent infrastructures can be described in terms of three general categories [PF07]:

*Cascading failure.* A disruption in one infrastructure causes a disruption in a second infrastructure. For example in 1998, the failure of the Galaxy IV satellite system degraded US telecommunications services, resulting in cascading effects in other infrastructures, causing 40 million pagers to fail to work [Amo11]. More than 20 United Airlines flights were delayed due to the lack of high altitude weather data [Amo11]. Consequently, the road transportation infrastructure was also affected because highway refuelling stations were unable to process credit cards, as their satellite links were down[Amo11].

*Escalating failure.* A disruption in one infrastructure exacerbates an independent disruption of a second infrastructure. In the event of electricity disruption in Manhattan in 2003, it immediately affected the telecommunications services. The global Internet was also immediately disrupted, and the effects were felt as far away as South Africa [Hys07].

*Common cause failure.* A disruption of two or more infrastructures at the same time is the result of a common cause. For instance, following the Hurricane Katrina, which struck the Gulf Coast of the United States in August 2005, simultaneously affected electric power, natural gas, petroleum, water supply, emergency services, telecommunications, and other infrastructures [PF07].

### 3.5 Importance of Collaboration Efforts

The security of cyberspace has become an important consideration in many countries. Moreover, the malicious actors have the ability to compromise and control millions of computers that belong to government, private enterprises, and ordinary citizens [Cho10] as shared in Section 3.3.3. These cybercrimes might affect society as a whole, not only threatening individual privacy but also potentially compromising a countrys CI and its ability to provide essential services to its citizens [Cav07]. Consequently, governments, international organisations, the private sectors, and civil society are required to work together in strengthening collaboration and escalating cybersecurity as a shared responsibility [Rid11].

Traditionally, the public-private collaboration has been viewed as a partnership or as contractual interaction between government agencies and private sector companies [KB04]. The public-private interface offers opportunities for decision makers at all levels of government and privates entities to build resilience by proactively coordinating and positioning the capabilities of stakeholders to collaboratively manage disaster consequences, especially involved cyber incidents [Lin03]. The impact of cyber-attack on CI sectors, as addressed in Section 3.3.3 involves cross-border vulnerabilities and geographic interdependency. Strong

international partnerships between governments and CI owners and operators are becoming essential.

In addition, [Lin03] wrote the following: *Collaboration is about co-labour, about joint effort and ownership. The end results is not mine or yours, it is ours. Collaboration occurs when people from different organizations produce something together through joint effort, resources, and decision making and share ownership of the final product or service. The focus is often on producing or implementing something* . Inter-organisational collaboration is an interesting concept, as it represents the paradox of hierarchical boundaries and cooperation, of autonomy and interdependence, as multiple organisations come together to approach a common issues [SB09].

Collaboration is especially important in complex, dynamic situations that effect community public security and safety [SB09]. Many cyber threats are difficult to detect and identify by a single organisation. Collaborative information sharing among different sectors is necessary and important to community cyber security and was implemented in collaborative cyber exercises shared in the next section.

## 3.6 Cyber Exercise in Cyber Security Strategy

Cyber exercises are an important tool to assess the preparedness of a community against cyber crises, technology failures and CII incidents [PT12]. Some countries, like the US, the UK, Australia and Canada have incorporated collaborative cyber exercises in their cyber security strategy as shared in Table 3.2.

[WDG04] suggested that exercises that are required that test not only an individual organisations ability to respond to cyber security events, but also the ability of related external entities, such as cities and states or other industry sector members, to respond in a coordinated manner. Besides, exercises enable competent authorities to test existing emergency plans, target specific weaknesses, increase cooperation between different sectors, identify interdependencies, stimulate improvements in continuity planning, and generate a culture of cooperative effort to boost resilience [PT12].

**Table 3.2** Incorporation of Cyber Exercise in Cyber Security Strategy

Year	Country	Cyber Security Strategy	Cyber Exercise in Cyber Security Strategy
2009	Australia	Australia Government Cyber Security Strategy	Highlights priorities under Threat Awareness and Response: to improve the detection, analysis, mitigation, and response to sophisticated cyber threats with a focus on government CI and other systems of national interest; conduct a programme of cyber security exercises to test and refine event response arrangements, including the Cyber Storm series of exercises coordinated by the US.
2010	Canada	Canada Cyber Security Strategy	Highlights priorities under Partnering with the Private Sector and CI Sectors: Collective cyber security efforts will be refined through training and exercise programmes. The result of these exercises, some of which are already underway, will be improved understanding of the dynamics among partners in cyber security. Participation in these exercises will also support the improvement of procedures to prevent cyber security failures.
2011	US	International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World	Highlights priorities under Protecting Our Networks: enhancing security, reliability, and resiliency; ensuring robust incident management, resiliency, and recovery capabilities for information infrastructure. The US will also work to engage international participation in cyber security exercises to elevate and strengthen established operating procedures with our partners.
2011	UK	The UK Cyber Security Strategy	In Objective 2: Making the UK more resilient to cyber-attack and better able to protect interests in cyberspace; defending national infrastructure from cyber-attacks by ensuring new national procedures for responding to cyber incidents (ensuring key services can be maintained or restored quickly) are fully tested, within the UK and in exercises with international partners. This includes a programme countering terrorist use of the Internet and exercises and plans for an EU-wide event in 2012. This builds on a minister-led incident management/response exercise (July 2011) and the governments on-going exercise programme.

## 3.7 Cyber Exercises Implementation

The broad spectrum of global economies indicates that cyber threats can occur at an international level [Rid11]. This highlights the need for CII protection action at four different levels: international, national, private sector, and individual [Cav07]. This means that governments must work closely with those infrastructure operators to ensure continuity of service by building resilient infrastructures [Hys07]. This section shares the implementation and contribution of collaborative cyber exercises involved various methods, such as large-scale and cross-boundary implementations, as summarised in Table 3.3 and Table 3.4

**Table 3.3** Collaborative Cyber Exercise Implementations -Part I

Cyber /Year	Exercise /Partici-pants	Cyber Exercise Objectives	Cyber Exercise Methods
Cyber Europe (2010)	30 EU and EFTA (22 player with 8 observer)	1) To trigger communication and collaboration between countries in Europe. 2) To try to respond to large-scale attacks.	Distributed table-top exercise, with players participating from their office locations and as part of their daily routine.
Cyber Europe (2012)	29 EU and EFTA(25 player and observer) 339 organizations, 571 individuals	1)To test the effectiveness and scalability of mechanisms, procedures and information flow for public authorities' cooperation in Europe. 2) To explore the cooperation between public and private stakeholders in Europe. 3) To identify gaps and challenges on how large-scale cyber-incidents could be handled more effectively in Europe.	Scenario based exercise using -Fictional adversaries joined forces in a massive cyber-attack against Europe, mainly through Distributed Denial of Service (DDoS) attacks against public electronic services.
Cyber Storm I (2006)	100(public and private agencies, associations, corporations) (60 locations and 5 countries)	1) To exercise communication, incident response policies, and operational procedures in response to various cyber incidents. 2) To identify future planning and process improvements.	Scenario based simulation on a large-scale cyber campaign affecting or disrupting multiple critical infrastructure elements primarily within the energy, information technology, transportation, and telecommunications sectors.



**Table 3.4** Collaborative Cyber Exercise Implementations (Continue Part II)

Cyber Exercise /Year /Partici- pants	Cyber Exercise Objectives	Cyber Exercise Meth- ods
Cyber Storm II (2008) Private sector, federal, state, and interna- tional governments (Australia, Canada, New Zealand, and the UK)	1. To examine the capabilities of partici- pating organisations to prepare for, protect from, and respond to the effects of cyber- attacks. 2. To exercise senior leadership de- cision making and interagency coordination of incident responses in accordance with na- tional policies and procedures. 3. To val- idate information-sharing relationships and communication paths for the collection and dissemination of cyber-incident situational awareness, response, and recovery informa- tion. 4. To examine the means and processes to share sensitive and classified information across standard boundaries in safe and se- cure ways without compromising proprietary or national security interests.	Scenario-based cyber- attacks focused on CI in the IT, communications, chemical, and transporta- tion (specifically rail and pipe) sectors, requiring action from foreign and domestic partners in the cyber response community.
Cyber Storm III (2010) 8 Cabinet- level departments, 13 states, 12 inter- national partners, and 60 private- sector companies and coordination bodies	1. To identify and exercise the processes, pro- cedures, relationships, and mechanisms that address a cyber incident. 2. To examine the role of DHS and its evolving National Cyber Incident Response Plan (NCIRP). 3. To as- sess information sharing issues. 4. To exam- ine coordination and decision-making mech- anisms. 5. To practically apply elements of on-going cyber initiatives, such as the Cy- berspace Policy Review and findings from past exercises.	Distributed exercise allowing players to par- ticipate from their office locations worldwide. The exercise control centre was located at a DHS fa- cility in Washington, D.C. The scenario progressed as players received 'in- jects' via e-mail, phone, fax, in person, and the Web. Exercise play simulated adverse effects through which the partici- pants executed their cyber crisis response systems, policies, and procedures

## 3.8 Cyber Exercise in Malaysia

### 3.8.1 National Cyber Security Policy (NCSP) in Malaysia

In advance of the emergent and sophisticated cyber threats growing and threatening the Malaysian nation, the Malaysia Ministry of Science, Technology and Innovation (MOSTI) conducted a study to develop policies and processes to address cyber security issues in the country since 2005 [bH11]. The study was conducted by consultants and relevant ministries and government agencies. The objectives of the study as highlighted in [DSZ09] as follows:

- To assess the current situation of cyber security risks within the CNII sectors;
- To ensure that the critical infrastructures are protected to a level that commensurate the risks faced; and
- To develop and establish a comprehensive road map and action plans for the implementation of a Cyber Security Framework.

On 7th April 2006, the result of the study was presented at the National IT Council (NITC). Consequently, the NCSP was endorsed and accepted for implementation on 31 May 2006 [DSZ09]. The NCSP is a comprehensive cyber security approach that provides a perspective on how cyber security should be implemented in an integrated manner [Has11]. Furthermore, the Malaysian government has adopted the NSCP as a comprehensive cyber security approach to increase the resiliency of the CNII [bH11].

In addition, NCSP states that objective that Malaysias CNII must be secure and resilient, which means immune against threats and attacks to its systems [bH11]. For an effective NCSP and policy implementation and to support all possible cyber security cooperation, this demands public-private partnership to bring together various cyber security experts from the government, industry, academia and individual experts to share, elaborate and debate various relevant cyber security issues and challenges [Has11].

As mentioned in [Has11] in his paper on Malaysia's NCSP, the NCSP is divided into seven areas as shown in Table 3.5, which are referred as the policy thrusts. While thrust drivers are the ministries that have the authority of their respective thrust areas, leading the thrusts with the assistance of their respective working group. The policy thrusts include effective governance, legislative and regulatory frameworks, which are are governed by the Attorney General's Chambers. The MOSTI is the thrust driver of the cyber security technology framework; culture of security and capacity building; research and development towards self-reliance; and compliance and enforcement.

A major initiative was to recommend that Malaysia's CNII organisations implement and adopt the MS ISO/IEC 27001-2007 as a security baseline and obtain a certification [DSZ09]. This will ensure that these organisations are implementing the required security measures on their SCADA systems. CNII organisations are instructed to follow this since 2013 [bH11].

**Table 3.5** Policy Thrust and Thrust Driver in NCSP Malaysia [Has11]

Policy Thrust	Thrust Driver
Effective Governance	National Security Council
Legislative and Regulatory Framework	Attorney General Chambers
Cyber Security Technology Framework	Ministry of Science, Technology and Innovation (MOSTI)
Culture of Security and Capacity Building	Ministry of Science, Technology and Innovation (MOSTI)
Research and Development Towards Self-Reliance	Ministry of Science, Technology and Innovation (MOSTI)
Compliance and Enforcement	Ministry of Science, Technology and Innovation (MOSTI)
Cyber Security Emergency Readiness	National Security Council

### 3.8.2 Critical National Information Infrastructure (CNII) in Malaysia

Malaysia's CNII defined as: '*Assets (physical and virtual), systems and functions that are vital to the nation that their incapacity or destruction would have a devastating impact on the; National economic strength; National image; National defence and security; Government capabilities to function; and Public health and safety*' [Has11].

National cyber security policies (NCSP) are designed based on a national security framework that includes legislation and regulatory, technology, public and private cooperation, institutional and international aspects (NICT, 2000) [bH11]. The policy is created to focus on the CNII, which comprises of 10 sectors of banking and finance, information and communications, energy and gas, transportation, water, health services, and food and agriculture, government, emergency services, and national defence and security [Has11]. Moreover, the NCSP vision is to ensure that the CNIIs are secure, resilient and self-reliant to consider the critical and interdependent nature of the CIs.

### 3.8.3 Cyber Incidents in Malaysia

Growing dependency on digital information systems has increased vulnerabilities and cyber risks, especially to the CNII in Malaysia. Several attacks have occurred on CIs in Malaysia, which affect public facilities and critical sectors, such as railway operation, stock exchange, and the postal system as well as government agencies as discussed as follows [AMZJ12]:

*Defacement Attacks on Malaysia Websites.* Malaysia experienced cyber-attacks codenamed 'Operation Malaysia' in 2010. The attacks appeared in the headlines of the mainstream media in Malaysia. The attack were prolonged attack from 15th to 19th June in 2010 by a hacktivism group known as 'Anonymous'. During the five-day period of attack, 210 Malaysian websites were defaced by the 'Anonymous' group which are recognised as high profile, sophisticated and politically-motivated [cyb11].

*Technical failure involved the railway services.* As reported by *The Star* on 25th July in 2006, during busy hours, the state-linked Light Railway Transit (LRT) system experienced a computer glitch that resulted in the lost of train tracking on the monitor screen in the control centre. The situation that followed was a service disruption every five minutes, and the trains were running at a much slower pace. Due to a failure of backup system, the situation become worse and caused a thousand passengers to be stranded hours in the trains and at the stations. Management quoted unexpected technical failure as the cause of disruption.

*System malfunction occurred at the national stock exchange.* Another incident reported by *The Star* on 4th July in 2008 involved a computer system malfunction at Bursa Malaysia, the national stock exchange, suspending a whole-day trading. According to the president of the Malaysian Investors Association, the interruption to the stock trading caused a government loss estimated of RM 1 million, which involved stamp duty of contracts, while brokers' loss RM 5 million during the non-trading day. The significant effects were not on the monetary losses to the stock exchange and Malaysian economy but also from the credibility losses.

*Malicious attack have occurred on government websites.* Among the latest incident was a series of unauthorised access and modifications by anonymous hackers against several government websites by *The Star* on 17th June 2011. The attacks were series of revenge to the government's latest decision to crackdown websites that are allegedly conduct activities in violation of copyright law. Although the damage was considered minor, the series of intended attack against government websites but it indicated that the national reputation was at risk.

### 3.8.4 National Cyber Exercises in Malaysia

In order to increase the awareness on cyber threats to organisations categorised under CNII, the Malaysia National Security Council with the support of Cyber Security Malaysia (CSM) has organised the collaborative National Cyber Crisis Exercise since 2008. The collaborative cyber exercises, known as X-MAYA [Ahm14], have involved the ten CNII sectors, as described in Section 4.2. The collaborative cyber exercises are conducted to assess the capabilities of CNII agencies to deal with cyber incidents [Ahm14]. As shown in Table 3.6, the first cyber exercise started in 2008 was X-Maya 1. Then, a series of X Maya exercises were conducted until the fifth exercise, which took place in 2013. The cyber exercises have been accepted by the community with an increasing number of participants of 11 agencies in 2008 to 28 agencies in 2009, 34 agencies in 2010, 51 agencies in 2011 and the largest number at 96 agencies in 2013, as shown in Table 3.6. This study involved participants of X-Maya 5, which are further discussed in studies in Chapter 5 and 6.

**Table 3.6** Collaborative Cyber Exercises in Malaysia

Cyber Exercise	Date	Participants
X Maya 1	24 July 2008	11 Agencies
X Maya 2	10 December 2009	28 Agencies
X Maya 3	4 August 2010	34 Agencies
X Maya 4	15 November 2011	51 Agencies
X Maya 5	25 November 2013	96 Agencies

### 3.8.5 International Cyber Exercises in Malaysia

**Organisation of the Islamic Cooperation - Computer Emergency Response Teams (OIC-CERT).** At the international level, Malaysia has participated in an annual cyber drill that involves the Computer Security Incidents Response Teams (CSIRT) from Asia Pacific economies and the OIC groups. The theme of the drill was countering cyber-ops with regional coordination. This exercise exposed real incidents and problems that exist on the Internet, in which every team performed tracing elements of cyber-op stages. These stages concluded to a point where CSIRTs/CERTs had to break up the infrastructure that was set up by the hackers, before a denial of service attack unfolds a government service [AH11].

**Asia Pacific Computer Emergency Response Team (APCERT).** Malaysia is on the steering committee of APCERT, which provides a network of security experts in the Asia Pacific region to improve awareness and competency regarding computer security incidents. This includes enhancing regional and international cooperation, joint measures to deal with security incidents, information-sharing, collaborative research and development, and assistance

and helps to address legal issues related to information security across boundaries. Today, APCERT consists of 26 member teams across 19 economies [APc15].

## **3.9 Chapter Contribution**

This chapter highlights the importance of collaborative cyber exercises contributions to CIIP and cyber security strategy implementations. It also shares some collaborative cyber exercise implementations in other countries.

## **3.10 Summary**

This chapter reviews the definitions of CI and CII in some countries. The importance of CIIP was highlighted due to emerging cyber threats that target CII and due to implications of cyber incidents on critical sectors involving stability of the economy and society. The importance of collaborative cyber exercise was highlighted through public-private commitments and the incorporation of collaborative cyber exercises into national cyber security strategies and implementation of cyber exercises in some countries. This chapter also shared the background of the CNII definitions and sectors in Malaysia, the NCSP, and collaborative cyber exercises at national and international levels.

## Chapter 4

# A Cyber Exercise Post Assessment Framework

### 4.1 Introduction

Cyber exercise was initiated to simulate a cyber environment used to develop and assess the knowledge and skills of information security personnel, which is discussed in Section 2.4.2. The importance of cyber exercise has been expounded as a platform used to assess the preparedness of a community against cyber incidents. Furthermore, cyber exercises implemented in some countries involving different communities backgrounds and services in public and private efforts to support cyber security.

Cyber exercises, such as the Blue Cascade exercise conducted in 2010, involve people from various sectors, including military, finance, telecommunications, and governments, each of whom had diverse backgrounds, skills, and experiences in cyber incidents [Mar09]. The exercises incorporating more than one sector are particularly challenging to conduct [WDG04]. To have an effective cyber exercise, a cyber exercise planning team must give careful consideration to the diversity of participants [RMM10].

[MFS<sup>+</sup>11] argues the simulation environment for cyber exercises often does not perfectly mirror participants working environments. Meanwhile, post assessment methodologies focus on organisation and management of the exercise rather than participants outcomes [BVH02]. Thus, how well the lessons are learned from cyber exercises and how they can be transferred to the participant organisations are still looming questions [MFS<sup>+</sup>11]. In order to understand the implications of cyber exercises on participants and the benefit to the participants' organisations, this chapter contributes to the development of a cyber exercise post assessment (CEPA) framework. This framework proposed to answer the third research question (RQ3), 'how can cyber exercise involved various sectors be beneficial to participants and

their organisations?’.

This chapter elaborates on the theories related to the post assessment framework in nine sections. The first three sections explain the first part of the framework, the participant assessment component, which focuses on what benefits participants gain from the cyber exercise and how they transfer the benefits to their organisations. Section 4.2 addresses the process of organising cyber exercises. Section 4.3 highlights the limitations of the CEPA methodologies. Section 4.4 presents the four-level Kirkpatrick model and compare it with other training models. Section 4.5 explains the adoption of the four-level Kirkpatrick model in the CEPA framework. Section 4.6 describes the second component of the post assessment framework. Two main tools suggested to evaluate at organisation level are organisation resilience and organisation cyber resilience. Section 4.7 provides research designs and implementations of studies using the proposed post assessment framework. Section 4.8 highlights the chapter’s contributions, and Section 4.9 summarises the chapter.

## 4.2 Organising A Cyber Exercise

According to [WDG04], creating and conducting a cyber exercise is a valuable experience for all participants but can be a major undertaking . A cyber exercise planning team must give careful consideration to the diversity of participants’ backgrounds [Jas14]. This involves different IT assets, network monitoring methods, and cyber incident response policies in participants’ organisations [Mar09]. The exercise master scenario events list (MSEL) must presents a reasonable scenario to all participants [Jas14]. So that, each event can easily be mapped back to exercise objectives [RMM10]. The MSEL defined in [Jas14] is a collection of pre-scripted events intended to guide an exercise towards specific outcomes [Jas14].

The process of organising a cyber exercise involves structured 1) planning, 2) designing, 3) conducting, and 4) evaluating processes as described in Table 4.1. Some guidelines have been developed for these processes, as discussed in [GR10] and [EO09]. A major concern is in the evaluation phase, as shown in Table 4.1. The cyber exercise evaluation phase of [EO09] focuses on the improvement of one cyber exercise to the next. Meanwhile, the evaluation phase of [GR10] has no direction on how the improvement action should be applied in participants’ environments. Further, limitations of the post assessment methodologies are discussed in the next section.



**Table 4.1** Comparison of Cyber Exercises Guides

Methods for Enhanced Cyber Exercises: Homeland Security Exercise and Evaluation Program (HSEEP) Volume I [GR10]	Good Practice Guide on National Exercises [EO09]
<u>Foundation</u> : To provide the foundation for an effective exercise: create a base of support (i.e., establish buy-in from the appropriate entities and/or senior officials); develop a project management timeline and establish milestones; identify an exercise planning team; and schedule planning conferences	<u>Identifying the exercise</u> : In this segment, the organizer must identify the need for an exercise. This need will include identification of procedures or measures that require practice or improvement and should be exercised. Based on this need, organizers can then select the type of exercise to conduct, and which organizations should participate
<u>Design and Development</u> : Building on the exercise foundation, the design and development process focuses on identifying objectives, designing the scenario, creating documentation, coordinating logistics, planning exercise conduct, and selecting an evaluation and improvement methodology.	<u>Planning the exercise</u> : In this segment, the organizer will drive the planning process. This process will involve recruiting the participants; acquiring financial resources for the exercise; selecting (and booking) the location, developing the scenario, rules, tools, and training materials for the exercise; selecting monitors and other role-players, and specifying what and how they will perform their duties; and planning the evaluation process.
<u>Conduct</u> : After the design and development steps are complete, the exercise takes place. Exercise conduct steps include set up, briefings, facilitation/control/evaluation, and wrap-up activities	<u>Executing the exercise</u> : In this segment, the exercise itself takes place. As specified in the planning process, participants go through (by discussing or actually acting out) the scenario and their response procedures and decisions. Monitors observe and note these actions, and inject information into the scenario.
<u>Evaluation</u> : The evaluation phase for all exercises includes a formal exercise evaluation, an integrated analysis, and an After-action Report (AAR)/Improvement Plan (IP) that identifies strengths and areas for improvement in an entity's preparedness. Recommendations are identified to help develop corrective actions to be tracked throughout the improvement planning phase.	<u>Evaluating the exercise</u> : Finally, after the exercise itself, the evaluation process takes place. This process tends to include a final evaluation report, or multiple reports tailored for different audiences. These reports review the exercise, identifying weaknesses, and recommending improvements. Furthermore, this process may include an ongoing process or forum by which to continue to address the weaknesses and recommendations identified.
<u>Improvement Planning</u> : During improvement planning, the corrective actions identified in the evaluation phase are assigned, with due dates, to responsible parties; tracked to implementation; and then validated during subsequent exercises.	

## 4.3 Limitations of Cyber Exercises Post Assessment Methodologies

Post assessment methodologies used for cyber exercises are AAR report, debriefing and hot wash, were mentioned in Section 2.5.2.2 of Chapter 2. The ENISA survey result in the section showed that reports were common post assessment methods used to evaluate the exercise. However, their scope is often limited to management and the organisation of the exercise.

A limitation of these post assessment methodologies is that they only focus on the event performance for the exercise designer, facilitators, and consultants (observers) [BVH02]. The learning outcomes for 'players' are difficult to define and measure [BVH02]. [PT12] further suggested that the monitoring and evaluation process will be more efficient if good practices are shared among several exercise organisers.

Limited evidence exists for monitoring and evaluation methods to further help exercise organisers to structure feedback from participating organisations in the implementation of lessons learned from cyber exercises [PT12]. Consequently, the study in this chapter proposed a post assessment framework to explore the impacts of the exercise on participants and their organisations.

## 4.4 Cyber Exercise Post Assessment Framework

The proposed CEPA framework consists of two main components for participants and organisations, as shown in Figure 4.1. Participants assessment adopted the four-level Kirkpatrick training model that analyses the participants' learning outcomes as reactions, learning, behaviour, and results. These are explained in Section 4.5.

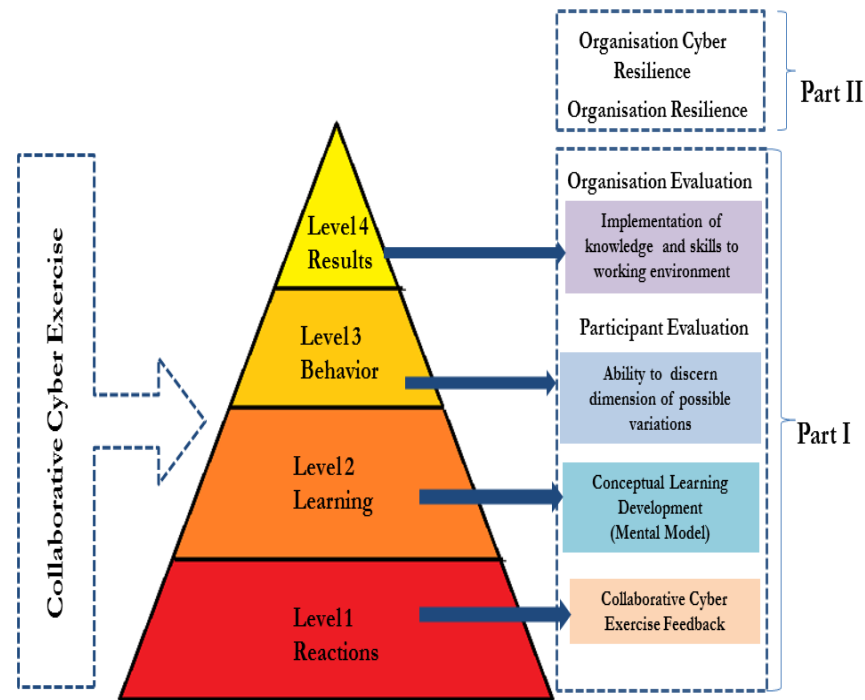


Figure 4.1: A Cyber Exercise Post Assessment Framework

#### 4.4.1 Kirkpatrick Training Model

In 1954, Don Kirkpatrick was at the University of Wisconsin working on his PhD dissertation on evaluating the effectiveness of a supervisory management programme, which he developed on four simple words: reaction, learning, behaviour, and results. In 1959, Bob Craig asked him to write an article for the American Society for Training and Development (ASTD) journal. Instead of one article, he wrote four articles that summarised of the Kirkpatrick four levels. In the 1970s, the use of the model grew worldwide as a standard for training evaluation [Kir09b]. Since then, the Kirkpatrick model of training evaluation criteria has had widespread and enduring popularity as described in [Bat04] and [Kir75].

The Kirkpatrick four levels: reactions, learning, behaviour, and results as elaborated in [MA12] and [Bat04]:

*Level 1: Reaction:* The first level is called reactions; most of this stage involves gathering feedback from participants regarding the training contents, training facilitators, training environments, and how much the training relates to the participants' job functions. If the participants showed a positive reaction after the training, this indicates that the participants were satisfied with the training programme and applied the skills and knowledge in their workplaces.

*Level 2: Learning.* Learning is defined as new knowledge and skills gained, which are shown through changes in participants' behaviours and attitudes.

*Level 3: Behaviour.* Behaviour measures whether the new knowledge, new skills, and developed attitudes are transferred to the workplace to reflect positive changes in behaviour and job performance. As Kirkpatrick highlighted, if learning is not transferred to the job, then it cannot have any effect on the job and the organisation [Kir09a].

*Level 4: Results.* The last level is the results. Results are the effects on the organisation's business or environment, resulting from the improved performance of the participants.

#### 4.4.1.1 Comparison on Training Models

The Kirkpatrick training model has served as a tool for training evaluators and has led to a number of other evaluation models [SA93]. This section provides a comparison of training models. The early Kirkpatrick model was developed in 1959 and updated in 1975, while other models, such as Tannebum's, was expanded from Kirkpatrick. [ASG04] provides a comparison of the four training models as:

*Kirkpatrick (1959a, 1959b, 1960a, 1960b):* The Kirkpatrick model four dimensional measurement levels: reactions, learning, behaviour, and results. It is the most frequently cited technique. Learning is measured during training and refers to attitudinal, cognitive, and behavioural learning. Behaviour refers to on-the-job performance and is measured after training. Additionally, reactions to training are related to learning, as learning is related to behaviour, and behaviour is related to results.

*Tannebum et al. (1993):* This is an expansion of the Kirkpatrick model by adding post training attitudes and dividing behaviour into two outcomes for evaluation: training performance and transfer performance. However, reactions to training and post training attitudes are not related to evaluation. Learning is related to training performance, while training performance is related to transfer performance, and transfer performance is related to results.

*Holton (1996):* This model includes three evaluation targets: learning, transfer, and results. Reactions are not a part of Holton's model because reactions are not considered a primary outcome of training; rather, reactions are defined as a mediating and/or moderating variables between trainees motivation to learn and actual learning. Learning is related to transfer, and transfer is related to results.

*Kraiger (2002):* This model emphasises three multidimensional target areas for evaluation: training content and design, changes in learners, and organisational payoffs. Reactions are considered a measurement technique for determining how effective the training content and design were for the tasks to be learned. Kraiger asserted that reaction measures are not

related to changes in learners or organisational payoffs but that changes in learners are related to organisational payoffs.

The Kirkpatrick model was selected for its popularity. Discussions on the popularity of the Kirkpatrick model are explained in the next section.

#### 4.4.1.2 Popularity of the Kirkpatrick Training Model

The Kirkpatrick model has made valuable contributions to training evaluation thinking and practice by focusing only on training evaluation outcomes [Bat04]. Furthermore, the distinction between learning (level two) and behaviour (level three) has drawn increased attention to the importance of the learning transfer process [SA93]. There are other factors that make the Kirkpatrick training model a popular choice [Bat04]:

*Systematic evaluation.* The four-level Kirkpatrick model helps to understand training evaluation in a systematic way. It offers a straightforward system, taxonomy, or language that describes training outcomes. This information can be used to assess the achievements of a programs objectives.

*Simple.* The four-level model simplifies the complex process of training evaluation. The model performs this in several ways: First, the model shows a straightforward guide for questions that should be asked and the appropriate criteria to be used. Second, the model reduces the complexity of measurement demands for training evaluation.

*Eliminate pre assessment.* As the model evaluation process only focuses on four-level outcome data that are collected after the training has been completed, this eliminates the need for pre-course measures (pre-evaluation) of learning or job performance measures, which are not essential to determining the programme effectiveness.

*Focus on outcome.* Training effectiveness is based solely on outcome. The model greatly reduces the number of variables that training evaluators need to consider. In effect, the model eliminates measurements on the surrounding factors that interact with the training process.

This model helps collect outcomes straight from post assessment without a need for pre-assessment. This was the strongest point supporting the adoption of the model into the post assessment framework as described in Section 4.5

#### 4.4.1.3 Kirkpatrick Training Model in Other Research

This section describes the use of the Kirkpatrick training model to evaluate several exercises in banking, education and university training:

*Evaluation on learning outcome of a course.* [Bas01], conducted research that examined two cohorts of students that engaged in the same course of study using different means of en-

agement. One cohort of 90 students completed a real-time learning programme integrating group dynamics. A second cohort of 171 students completed the same course in an online environment. The study examined the learning outcomes of the online cohort using level two, level three, and level four of the Kirkpatrick model .

*Evaluation on a training program in banking sectors.* [MA12] used the four levels of the Kirkpatrick model to examine the effectiveness of the Intermediate Central Banking Course in Malaysia. The study examined 1) the reactions of the employees to the training programmes, 2) the level of employee learning, and 3) the employees transfer of training. They used training feedback questionnaires, pre- and post-tests, face-to-face interviews, learner development plan reports, and behavioural surveys. The overall result of the study showed that the effectiveness of the bank training only supported evidence up to level three of the Kirkpatrick model. The findings of the study contributed to the decision of the policy maker in the Central Bank of Malaysia justifying the return on investment of the training.

## 4.5 Adoption of the Kirkpatrick Training Model

### 4.5.1 Participant Evaluation

The adoption of the four-level Kirkpatrick model to the CEPA is to evaluate the participants' learning outcomes from their participation in cyber crisis exercise involved multisectors to test national cyber incidents handling policies and procedures, as depicted in Figure 4.1. This section explains Part I of the framework, which consists of evaluation of participants based on the four levels of the Kirkpatrick training model:

#### Level 1 : Reactions

At the reactions level, we examine participants' perception about the exercise in terms of:

1. Objective of the exercise,
2. Scenario created for the exercise,
3. Environment setting for the exercise,
4. Participants' expectation of the exercise, and
5. Result at the end of the exercise,

This feedback contributes to the participants' perceptions based on what they have experienced during the exercise.

**Level 2: Learning**

The knowledge development of individuals is related to a mental model [BP97]. Mental models are built and developed during a lifetime and are shaped by social and cultural background, education, and experience [BP97]. Mental models change as people gain experience and learn from it [ML15]. From a cognitive perspective, people learn as they change their perceptions after surveying and evaluating the outcomes of their actions [Onw12].

In Chapter 2, the security knowledge and technical skills of information security employees are developed through continuous learning experiences in their educational life at college until their working life at their organisations. The knowledge and skills were continuously developed as participants were involved with more security training and cyber exercises. Cyber crisis exercises has two categories, first category used to test the cyber incident response procedures and policies designed in an organisation or at national level. Second exercise normally to increase information security employee knowledge and skills of new cyber threats that might have potential to affect their organisation as described in Section 2.5.1. Through these exercises, it is intended to give a hands-on, technical experience to participants. However as suggested in [AD<sup>+</sup>06] that these exercises can also be used to further demonstrate the importance of non-technical plans and policies. At this learning level, new conceptual learning models and new technical skills developed from variants of cyber incident scenarios as a result of participants' experiences during cyber exercises. Cyber exercises help to develop operational capability that support the types of skills and knowledge that lead to cyber situational awareness (CSA) [ML15].

**Level 3 : Behaviour**

New knowledge and skills developed during the exercise become a benefit to participants performing new actions at the behaviour level. These new capabilities of participants include how to detect relevant situational aspects or new threats and how participants can act upon them [SPGM11]. As a key challenge for cyber security operators is to develop an understanding of what is happening within and outside of their networks [TGM12]. This understanding or CSA provides the cognitive basis for human operators to take appropriate actions within their environments [TGM12]. Furthermore, defending a valuable digital infrastructure requires pursuing two interrelated goals: to maintain the production and at the same time prevent hackers from gaining access and acting on the network (e.g., stealing or corrupting data or interfering with process production) [Mar09]. For more effective detection and prevention of cyber threats, the security analyst requirements are an up-to-date knowledge of cyber threats and how to mitigate the threats.

**Level 4 : Results**

At the result level, results are the implementation of decisions and actions of the cognitive processes at the learning stage and the actions performed at the behaviour stage that directly affect the organisational environment.

## **4.6 Organisation Evaluation**

Part II involves assessment of organisation resilience (OR) and organisation cyber resilience (OCR) of the participated organisation in collaborative cyber exercises. The OR used a benchmark resilience tool (BRT-53) developed by University of Canterbury in New Zealand. This tool assess OR perceptions in three dimensions of Situation Awareness (SA), Management of Keystone Vulnerabilities (KV), and Adaptive Capacity with 15 indicators developed by Resilient Organisations Research at the University of Canterbury [Ste10]. This tool has been chosen because it has an indicator that assess perception on 'Participation in Exercises'. Furthermore it has been tested to assess ORs of critical sectors in Auckland [Ste10]. Details of the BRT-53 was presented in Chapter 6.

The assessment on OCR used the C-Suite Executive checklist developed by the World Economic Forum in 2012. The tool based has three main components of governance, programme and network. It was developed based on 4 core principles of 1) recognition of interdependence, 2) role of leadership, 3) integrated risk management and 4) promote uptake. Details of the tool was elaborated in Chapter 7.

## **4.7 Chapter Contribution**

This chapter proposed a CEPA framework. The framework adopted the Kirkpatrick training model to assess the participants outcomes and how it benefits their organisations, while the organisational resilience assessments used surveys developed from organisational cyber resilience research.

## **4.8 Summary**

This chapter provides the theories used to propose the CEPA Framework. The framework consists of two main assessment components: participants and participants organisations. The participant evaluation component adopted the four-level Kirkpatrick training model for CEPA outcomes: reaction, learning, behaviour, and results.



## **Chapter 5**

# **An Investigation into the Impacts of a Cyber Exercise in Malaysia**

### **5.1 Introduction**

The limitations of the current cyber exercise post assessment methodologies were addressed in Section 4.3. These tend to focus on the participants' performance during the exercise in organising and managing the event. As a result, a cyber exercise post assessment framework was proposed in Section 4.4 to assess the outcome of the cyber exercise, especially the benefits to the participants and their organisations. This chapter describes an investigation that used the framework.

The investigation involved a cyber exercise called X-Maya 5. The X Maya was organised to test a new national policy and procedures on cyber crisis in Malaysia which involved 10 CNII sectors as explained in Section 3.8.4. The main objective of the exercise is to test the communication between 10 CNII sectors during cyber incidents. The X Maya provide a platform for effective communication and knowledge sharing for incidents handling. The exercise tests the participants ability to identify threats targeting their cyber environment and how they handle and solve the incident. For a particular attack, how they can categorised the attack into a certain level of crisis and how they can response to the attack. The exercise also provide a platform for knowledge sharing in terms of defend and recovery with other sectors. Data collected through interviews with X-Maya 5 participants were coded and categorised according to the four-level Kirkpatrick training model.

This chapter presents the investigation in 11 sections. Section 5.2 explains the purpose of this study. Section 5.3 describes the semi-structured interviews. Section 5.4 elaborates on two pilot studies conducted to test the research instrument. Section 5.5 describes data collection for this study. Section 5.6 provides information on the demographic data of the respondents.

Section 5.7 provides a data analysis for the study. Section 5.8 presents the finalised categories according to the four-level Kirkpatrick training model. Section 5.9 discusses the results of the study, and Section 5.10 addresses the contributions of this chapter. Section 5.11 summarises the chapter.

## **5.2 An Investigation into impacts of the X Maya Cyber Exercise**

### **5.2.1 Purpose of the Study**

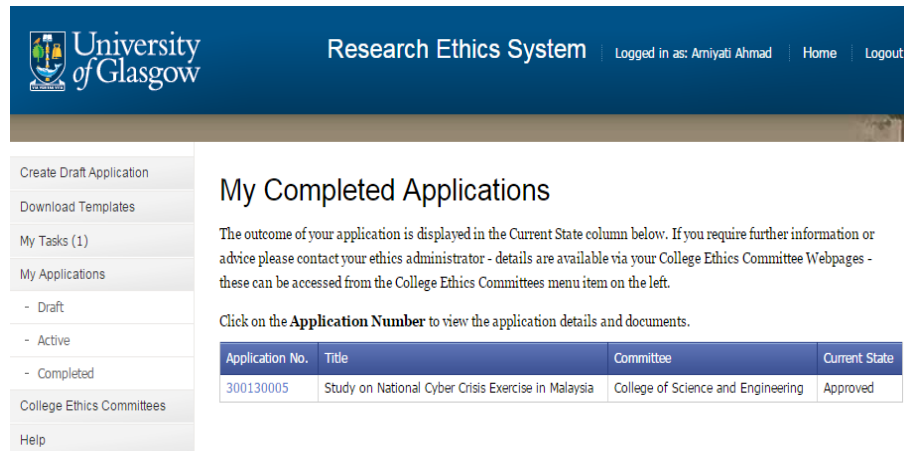
This study aims to answer research question three (RQ3): How do cyber exercises benefit participants and their organisations? This investigates the effects of the X-Maya exercise on participants reactions, learning, behaviours, and results, proposed in the post assessment framework in Section 4.5. The focus of this study is on people who were involved in collaborative cyber exercises. Post assessment was used because:

1. The X-Maya cyber exercise involved different participants from 10 different sectors, which have different working environments and various cyber incident handling policies and procedures.
2. The X-Maya exercise is a national series organised once a year.
3. Participation was voluntary and on an invitation basis. Thus, no pre-assessment was involved in the selection process.
4. The people involved with the exercise have different backgrounds in working experiences, skills, and expertise.
5. The participation experiences in X-Maya differ from one participant to another.
6. Data in this study was collected seven months after the exercise event.

### **5.2.2 Ethical Approval**

As this study focusses on human participants, this study complies with the British Psychological Society (BPS) ethical guidelines of the University of Glasgow. The ethics application proposed using interview questions; organisational resilience and organisational cyber resilience surveys for the research were applied for in 16 May 2014. The application was approved by the FIMS ethics committee of the University of Glasgow in June 2014.

The application approval information is displayed in Figure 5.1, with the application no. of 300130005.



The screenshot shows the 'Research Ethics System' interface of the University of Glasgow. The user is logged in as 'Amiyati Ahmad'. The main section is titled 'My Completed Applications'. It contains a table with one application entry.

Application No.	Title	Committee	Current State
300130005	Study on National Cyber Crisis Exercise in Malaysia	College of Science and Engineering	Approved

Figure 5.1: Ethical Approval for Data Collection on X Maya Participants

## 5.3 Research Methodology

An interview is designed to elicit the knowledge and beliefs of individuals [Bur94]. The use of an interview methodology, as recommended in [Bur94], offers one way of collecting data about peoples subjective experiences, views, and perceptions.

### 5.3.1 Semi Structured Interview

This study used a semi-structured interview because of the following advantages [LBW94]:

1. It is well suited for the exploration of the perceptions and opinions on specific issues. It enables probing for more information and clarification on a respondents answer.
2. Semi-structured interviews can provide reliable and comparable qualitative data. It can facilitate comparability by ensuring that all questions are answered by each respondent.
3. The wording and sequence of all questions are standardised for all respondents. Therefore, the differences in the respondents answers are due to differences among them rather than in the questions asked.
4. The analysis process of a semi-structured interview is relatively straightforward. All responses to a question from each of the respondents can be grouped together, and various themes can easily be identified [Bur94].

Semi-structured interviews are suitable for data collection from X-Maya participants from multiple sectors with different security backgrounds and experiences. Differences exist in participation experience in X-Maya exercises. Some of the participants had been involved with cyber exercises for several years, while some had just joined for the first time. The respondents experience with X-Maya is shown in Table 5.4.

The Kirkpatrick model normally uses to assess individual performance in training. As this study aims to assess the impact of X Maya on individual and their organisation using this model. The development of the interview questions in Table 5.1 were based on the four-level Kirkpatrick model, guiding the interview topics to be discussed.

**Table 5.1** Interview Questions Involved X Maya Respondents

No	Interview Questions
1	When did you start getting involved with cyber exercise?
2	How many times have you been involved with cyber exercise, including X-Maya?
3	Would you like to share your experience in X-Maya in terms of its objectives, the scenario, setting environment, and facilitator? What was the scenario used in the X Maya 5 exercise? Do you think it was easy to understand?
4	What have you learnt from the X-Maya 5 exercise and other cyber exercises in which you have been involved?
5	How did X-Maya 5 help you to contribute to cyber security in your organisation?
6	Did you revise the existing security standards, policies, and guidelines after attending the X-Maya exercise?
7	Has there been any improvement on standards, policies, and guidelines that you have proposed after attending the X-Maya exercise?
8	Do you think the scenario and infrastructure used in X-Maya should be implemented in your organisation?
9	Do you plan to run your own cyber exercise in your organisation?

## 5.4 Pilot Study

The interview questions in Table 5.1 were initially tested on two security experts. The first test was on the confidentiality of interview items. A set of interview questions was sent to an officer from Malaysia National Security (MSN). The officer was involved in the X-Maya exercises. The test was to ensure the confidentiality and suitability of the interview questions to be used to collect data from X-Maya participants. The officer agreed that the interview

questions have not asked any confidential information about X-Maya. He also agreed that the questions could be used to collect data. Based on his agreement, emails were sent to 10 CNII sector leaders involved in the X-Maya 5 exercise to recruit respondents for the interview.

The second test was on the suitability of interview items. An interview was conducted with an officer who was involved as a sector leader in a participating sector in the interview. The test found that people who were not directly involved with the exercise had limited information to answer Questions 3, 4, and 5, which related to operational and technical aspects of the exercise. Based on this situation, one of the requirements for the participants for the study is that they were fully involved in the exercise, as described in Section 5.5.1.

## 5.5 Data Collection

According to [CH96], it can be impractical to obtain measures from a total population due to accessibility, expense, and time. Because of these limitations, data collection for this research involved a smaller group or subset of the population with an assumption that the information generated will represent the population under study. This smaller group or subset is called the sample. This study used a sample from X-Maya 5 participants to investigate the impact of national cyber exercises called X-Maya in Malaysia.

### 5.5.1 Sampling Strategy

Details information on X Maya has been asked during the interview with the X Maya organiser (Malaysia National Security), but limited information were revealed by the officer because of confidentiality issues. However, we have tried to gather as much information regarding X Maya through, X Maya video [Ahm14], participants and Cyber Security Malaysia. Information on X-Maya 5 participants was from a public source [Ahm14]. This sampling technique was recognised as a convenience sampling technique. Two characteristics of participants were required:

1. The participants must be representatives of the 10 CNII sectors identified by the Malaysian National Cyber Security Policy as defence and security, banking and finance, information and communications, energy, transportation, water, health services, government, emergency services, and food and agriculture.
2. The participants must have been fully involved as players in the X-Maya 5 exercise.

From all the sector leaders contacted, only 15 participants replied and agreed to be interviewed: five from government agencies, three from the military sector, and seven from

telecommunication sectors. Each sector represented by one organisation except government which involved two different agencies. All participants are players during the X Maya exercise. Most of them have well technical background and skills. They also involved with system and network administrations at their organisation.

**Table 5.2** Interview Participants

Sector	No of Participants
Government	5
Military	3
Telecommunication	7

X Maya involved a group of players that performed in the cyber crisis to represent their organisation and sector. So the post assessment interviews were conducted in groups interviews as displayed in Table 5.2. Interviews were conducted in July 2014. All interviews were conducted at the participants offices, and all conversations were recorded in mp3 format. The interviews lasted for 60 to 130 minutes. Details of the interview activities are listed in Table 5.3.

**Table 5.3** Information on Interview Activities

Interview Date	Number of Participants	Audio File	Audio File Size (Kilo-byte)
16 July 2014	7	MCMC.mp3,	10554KB
17 July 2014	3	KML.mp3	13475KB
18 July 2014	2	SPPM.mp3	10554KB
25 July 2014	3	AF.mp3	21624KB

## 5.6 Demographic Data

Before each interview started, some background data of participants were collected, including their experience with the X-Maya exercise, as shown in Table 5.4; their working experience with the organisation, as shown in Table 5.5; and their experience with the industry sector, as shown in Table 5.6. Other information on their participation in preparation training organised by Cyber Security Malaysia is illustrated in Table 5.7.

### 5.6.1 Experience in X Maya Exercises

The participation in the X-Maya exercise is on an invitation and voluntary basis. Most participants from the public sector and government agencies received orders from their respective ministries to get involved with the exercise. All the respondents of the interview were participants of X-Maya 5, which was conducted in November 2013. Some had participated since the first X-Maya exercise in 2008.

**Table 5.4** Experience in X Maya Exercises

X Maya (Exercise Series)	1	2	3	4	5
Experience in X Maya (No of People)	5	6	9	12	15

### 5.6.2 Response on Working Experience in Organisation

As described in Table 5.5, three respondents have more than 20 years of working experience. There are five respondents in each category of four to 10 years and 11 to 20 years of working experience. Two respondents have less than three years of working experience.

**Table 5.5** Response on Work Experience in Organisation

Working Experience in Organisation	Frequency
1 to 3 years	2
4 to 10 years	5
11-20 years	5
>21	3

### 5.6.3 Response on Working Experience in Industry Sector

Table 5.6 shows that three respondents have more than 20 years of working experience. Seven respondents have working experiences between 11 to 20 years. Five respondents have four to 10 years of working experience.

**Table 5.6** Response on Work Experience in Industry Sector

Working Experience in Industry Sector	Frequency
4 to 10 years	5
11 to 20 years	7
>21	3

### 5.6.4 Participation in Security Training

Cyber Security Malaysia has organised training for X-Maya participants. Before the exercise started, participants were invited to attend this training. However, according to the respondents, seats for the training were limited, and the cost of the training was paid by their organisations. Data regarding involvement in the training is shown in Table 5.7.

**Table 5.7** Response on Cyber Security Training

Cyber Security Training	Frequency
YES	10
NO	5
Total	15

## 5.7 Data Analysis

Data analysis for this study used a deductive approach based on the proposed collaborative cyber exercise post assessment framework. As referred to [BGS<sup>+</sup>08], there are two fundamental approaches to analyse qualitative data, each of which can be handled in a variety of different ways :

*Deductive Approach.* This approach involves a structure or predetermined framework to analyse the data. Normally, the researcher imposes a structure or set of theories on the data. They used the theories to analyse the interview transcripts.

*Inductive Approach.* This approach analyses data with little or no predetermined theory, structure, or framework and uses the data to derive the structure of the analysis. The approach is comprehensive and time consuming. It is most suitable where little or no information is known about the subject.

Although coding an interview is widely recognised as a common step in the analysis process, many researchers do not fully explain how this process is done [DGMM11]. One qualitative interview data analysis method in [Bur91] involved 14 stages. Interview data analysis for this study involved six stages as depicted in Figure 5.2



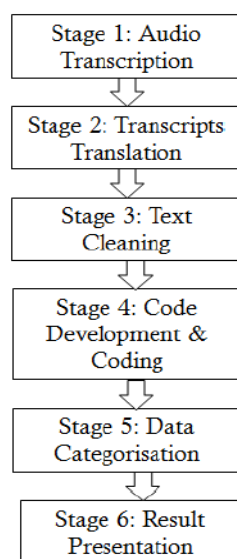


Figure 5.2: Data Analysis Process

**Stage 1: Audio Transcription:**

Data analysis for this study started with transcribing audio interview data in mixed Malay and English in its original format. During the interview, the participants were encouraged to speak any language with which they were comfortable. In the first round of the interviews, the interviewer found limited responses from the interviewee if they were asked in English; therefore, in order to eliminate any language barriers, the interviews were conducted in English and Malay. The interview audio was played repeatedly, and the interview data were transcribed into six individual documents, one for each interview. Transcribed data was also sent to participants to get more clarification and agreement from participants. Samples of the transcripts are displayed in Figures 5.3 and 5.4.

**Stage 2: Transcripts Translation:**

The original transcripts in Malay and English were read through, translated, and documented in English. The aim was to standardise the text used in the coding processes. Two colleagues were invited to validate the translation transcripts. Figure 5.4 shows a sample of the transcript in English.

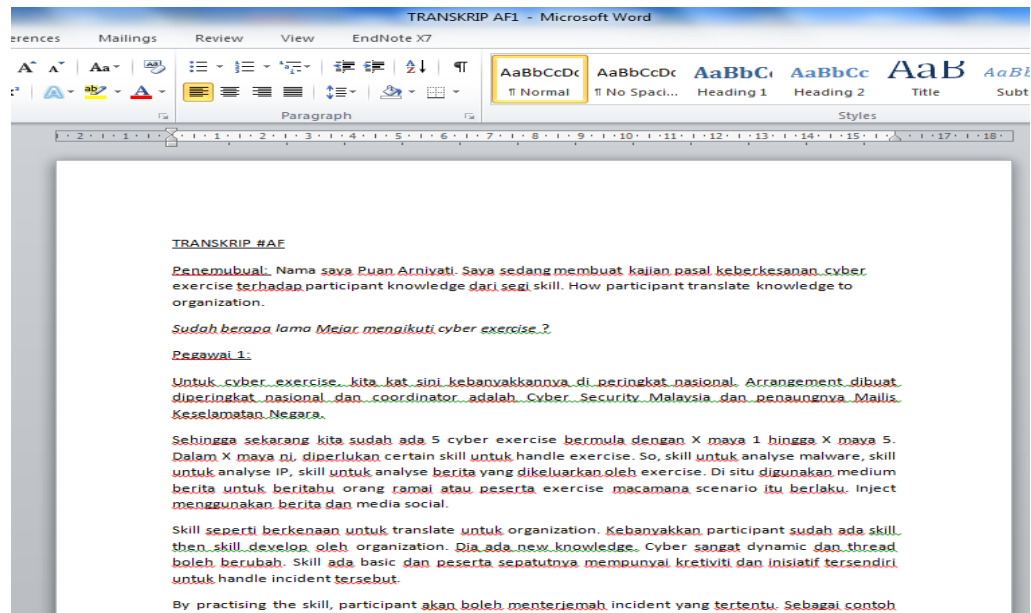


Figure 5.3: A Sample of Interview Transcript in Original Form

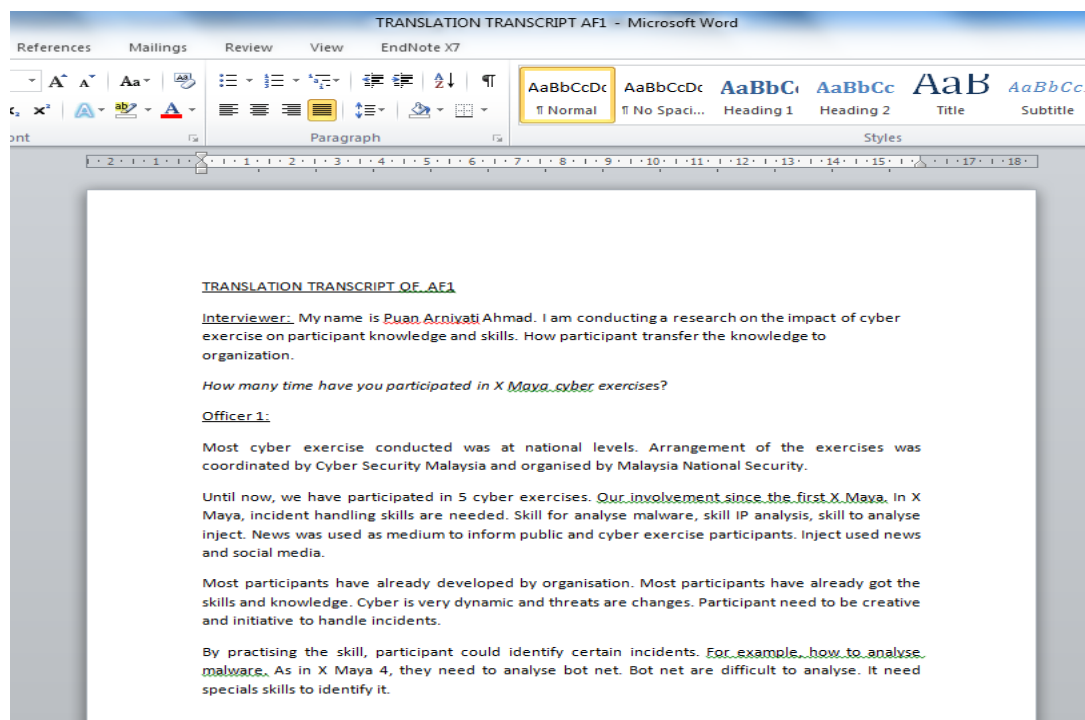


Figure 5.4: A Sample of Interview Transcript in English

### Stage 3: Text Cleaning:

For each translated transcript, interview Questions 3, 4, 5, 6, and 7 and their answers were extracted from the script and transferred into a table shown in Appendix G. These questions provide questions and participant's answer at each of Kirkpatrick level. At this stage, only text that specifically answered the interview questions was transferred into the table, while

dross remained in the original transcripts. [Mos85] defined dross as text that occurs in the transcripts that is not related to the interview topic. Extracted scripts are ready for coding in the next stage, while the remained scripts kept in original format and will be used in a future project.

#### **Stage 4 : Code Development and Coding:**

This stage involved two important processes 1) code development and 2) coding.

*Code development:* [MHS13] described a code as a label that assigns symbolic meaning or inferential information, which is compiled during a study. Codes are usually attached to data chunks of varying size and can be in the form of a straightforward, descriptive label or more evocative and complex labels . The code for a chunk of data is determined by carefully reading and reflecting on its core content or meaning [MHS13]. For this study, transcripts were read through and code themes generated according to the four-level Kirkpatrick model, as in Table 5.8. Code generation was done iteratively to ensure that all data was coded against the right themes.

*Coding:* According to [MHS13] coding is a heuristic method of discovery. Coding is a data condensation task that enables analysts to retrieve the most meaningful material and to assemble the chunks of data together [MHS13]. At this stage, clean transcripts are read through. Codes and code themes are generated.

Some code themes developed according to the four-level Kirkpatrick model of reaction, learning, behaviour, and results, as described in Table 5.8. As proposed in Section 4.5.1, the four code themes defined at the reaction level were 1) objective, 2) scenario, 3) environment, and 4) expectation. At the learning level, the three code themes generated from the scripts were 1) new skills, 2) experience, and 3) communication. At the behaviour level, two code themes were generated 1) situation awareness and 2) safeguard environment. At the results level, four code themes were generated: 1) new policy, 2) new procedure, 3) revised policy, and 4) revised procedures. Every code theme has its own code. These codes were used to annotate the transcripts on a line-by-line basis, this process is called coding. The sample of the coded transcripts is shown in Appendix G.

**Table 5.8** Code Themes for Coding and Categories Interview Data

Interview Questions	Kirkpatrick Levels	Themes Code
Question 3: What are participants' reactions regarding the cyber exercise objective, scenario, environment setting, and facilitator?	Level 1: Reaction(RE)	1) OBJECTIVE (RE:OBJ), 2) SCENARIO (RE:SC), 3)ENVIRONMENT(RE:ENV), 4) EXPECTATION(RE:EXP)
Question 4: What did the participant learn during the cyber exercise? (new skills, policy, communication, procedure, etc.)	Level 2: Learning(LE)	1) NEW SKILL(LE:SK), 2)EXPERIENCE (LE:EX), 5) COMMUNICATION(LE:COMM),
Question 5: What are the effects of changes in behaviour due to the cyber exercise experience?	Level 3: Behaviour(BE)	1) SITUATION AWARENESS(BE:SA), 2) SAFEGUARD ENVIRONMENT(BE:SE)
Questions 6 & 7: Any new implementation in the organisation after participating in cyber exercise?	Level 4: Result(RS)	1) NEW POLICY (RS:NEW PS), 2)NEW PROCEDURES(RS: NEW PRO), 3)REVISED PROCEDURES(RS:RE PRO),4)REVISED POLICY(RS: RE POL)

**Stage 5: Data Categorisation:**

At this stage, all text with the same code is combined into categories. The categories represented by the four-level Kirkpatrick model were reaction, learning, behaviour, and results. This stage finalised the coded text. Repeated data were removed from the lists. Table 5.9 provides definitions of the final code themes and their categories.

Two people were invited to match the generated category system. One of them are participant of the X Maya. Themes code description are presented in Table 5.9 and a list of text with 48 items were given to them. They have to match the code with the items. Forty-eight categorised items were analysed using SPSS. Every item which matched correctly with the code theme will given a score of one and labeled as similar, while false item were score as zero and labeled as different. The aim of this stage is to enhance the validity of the categorisation method and to avoid researcher bias. Kappa metrics were then used to measure the differences in categorising the text.

**Table 5.9** Description of Themes Code

<b>Kirkpatrick Levels or Category</b>	<b>Themes Code</b>	<b>Code &amp; Code Description</b>
Level 1: (RE)	1)OBJECTIVE  2)SCENARIO  3)ENVIRONMENT  4)EXPECTATION	RE:OBJ-1) To describe the participant' reactions towards the objective of the exercise. RE:SC-2) To describe the participants' reactions towards the scenario of the exercise. RE:ENV-3) To describe the participants' reactions towards the environment of the exercise. RE:EXP-4) To describe the participants' reactions regarding their expectations towards the exercise.
Level 2: (LE)	1)NEW SKILL  2)EXPERIENCE  3)COMMUNICATION	LE:NS-1)To describe the participants' perceptions of new skills developed from the exercise. LE:EX-2) To describe the participants' perceptions in experiencing the exercise situation. LE:COMM-4)To describe the participants' perceptions in communicating solutions during the exercise.
Level 3: (BE)	1)SITUATION AWARE- NESS  2)SAFEGUARD ENVI- RONMENT	BE:SA-1)To describe the participants' perceptions of the increment of their situation awareness by changes in their monitoring behaviour towards the cyber environment in their organisations. BE:SE-2) To describe the participants' perceptions of behaviour towards the cyber environment in their organisations.
Level 4: (RS)	1)NEW POLICY  2)NEW PROCEDURES  3)REVISED PROCE- DURES  4)REVISED POLICY	RS:NEW PS-1)To describe the participants' perceptions of changes to the current policy in their working environments. RS:NEW PRO-2) To describe the participants' perceptions in implementing new incident handling procedures in their organisational environments. RS:RE PRO-3)To describe the participants' perceptions of the revision of current incident handling procedures in their organisational environments. RS:RE POL-4) To describe the participants' perceptions of the revision of current incident handling policies in their organisational environments.

Inter-rater reliability was checked for each item. Table 5.10 illustrates the Kappa value for the categorisation results, which was 0.833. As suggested in [Fle81], the interpretation of the Kappa value is shown in Table 5.11. Values exceeding 0.75 suggest strong agreement above chance, and values in the range of 0.40 to 0.75 indicate fair levels of agreement above chance, while values below 0.40 indicate poor levels of agreement above chance. The Kappa agreement shows that the two research assistants (RAs) have achieved almost perfect categorisation on the list of text, according to the code themes, and the results are statistically significant ( $<0.0005$ ).

**Table 5.10** Inter-rater reliability for text categorisation

	Value	Asymp. Std Error	Approx. T	Approx Sig
Measure of Agreement Kappa	0.833	0.114	5.855	0.000
N of Valid Cases	48			

**Table 5.11** Kappa Coefficient Values and Interpretation

Kappa Value	Interpretation
Below 0.00	Poor
0.00-0.20	Slight
0.21-0.40	Fair
0.41-0.60	Moderate
0.61-0.80	Substantial
0.81-1.00	Almost perfect

### Stage 6: Results Presentation:

Final results presented in form of individual comments and group merged results. The individual data extracted from the translated transcripts presented as participants' comments at each Kirkpatrick level. While the merged results were the final categorised system which provide a group outcome as presented in Section 5.8 in form of a tabular table. The group outcome will be used to develop a quantitative survey for the X Maya assessment in the future study as proposed in Section 8.4.

**Table 5.12** Final Category and Number of Items

Category	Frequency
Reactions	Objective (5), Scenario (10), Environment (3), Expectation (3)
Learning	New Skills(9), Experience(2), Communication(3)
Behaviour	Situation Awareness (2), Safeguard Environment (3)
Results	New Policy(3), New Procedure (1), Revised Policy (1), Revised Procedure(3)

## 5.8 Categorical Results

This section presents the findings of participants' perceptions on how the X-Maya national collaborative cyber exercise benefits participants and their organisations. This section presents the participants' individual comments and group merged views for each theme and category as follows.

### 5.8.1 Level 1: Reactions

Level one presents the participants' reactions concerning the cyber exercise, which fall under four categories:

1. objective of the exercise,
2. scenario,
3. environment, and
4. expectations.

Regarding the objective, all participants have agreed that the objectives of the X-Maya exercise are 1) sharing information on cyber threats, 2) sharing solutions among collaborator sectors and agencies, 3) promoting interdependency awareness among sectors, and 4) establishing communication among sectors during a cyber crisis. These were supported by participants' response as follows:

*"Technical skills is not their main aims. Previously, in the first X Maya, they announced the winner at the end of the event. Usually people from ISPs won, because they got the right skills.... what they really want us to achieve is not the technical skills but the effective communication. Awareness to participants, where to communicate when incidents happened." (Military Officer 1, Male).*

*"Whatever things happened, all the agencies should have the incidents response teams response to the incidents, this is what we are tested, in how we tackle the issues and how we resolve the issues." (Telecommunication Officer 1, Male).*

*"Every team got different attack, we need to share how to solve and mitigate the attack. If real incidents happened we will help each other. Establish communication and sharing the knowledge among us." (Government Agency 1, Officer 2, Male).*

*"One of the X Maya objectives is to coordinate the government and private organisations in incidents handling and reporting." (Military Officer 2, Male).*

*"X Maya is more on management in how to manage incidents." (Government Agency 2, Officer 1, Female).*

Participants' perceptions on the scenario are categorised into a simulated scenario used in X Maya, types of attacks used in the X-Maya scenario (i.e., Trojan, Distributed Denial-of-service ( DDoS ) , etc.) and levels of attacks (i.e., web, sever, or application). Regarding the environment, participants specifically identified the setting of X-Maya exercise as 1) an isolated area 2) using virtualisation (i.e., virtual machine) and 3) using a virtual private network. Some positive and negative comments from X Maya participants as stated:

*"The attacks were on server....using virtual servers, they sent us a server with free BSD configured environment, which we have not familiar with. Our systems used Windows environment....We are not being train with free BSD and it has no realism." (Military Officer 3, Male).*

*"There are several attacks techniques....Malware, DDos, Trojan and Botnet." (Military Officer 1, Male).*

*"Each scenario is different, as in Apache, they changed the configuration and put a flag on the directory. DDos was the last scenario. Various scenario used as application, email, web, server dierctory." (Government Agency 1, Officer 2, Male).*

*"Scenario in X Maya 5 are similar with previous X Maya. In X Maya 1 and 2 they used attacks on Apache server and web defacement. In X Maya 5, it involved more technical, the DDos." (Government Agency 1, Officer 1, Male).*

*"..., the X Maya scenario is not helping much because the scenario is more suitable for an organisation and not for ISPs." (Telecommunication Officer 2, Male).*



*"...the differences between X Maya and our cyber drill..X Maya use more defacement, ISPs cyber drill used DDos high volume, X Maya test on 10 CNII sectors, the organiser has to cater all threats, Defacements, sql injection...." (Telecommunication Officer 3, Male).*

*"We can simulate the X Maya environment for our organisation exercise, we can create the worms and bugs. The only thing that a bit difficult is to fix the threats, it's really need knowledge and skills." (Government Agency 2, Officer 3, Male).*

*"...they provide us with a pen drive installed with VM with console. We need to install and activate a key to establish a communication to the host server, through a VPN tunnel, simultaneous attacks launch from the host server. We are in an isolated area in a cloud.." (Government Agency 1, Officer 1, Male).*

Participants' perceptions regarding expectations were gaining defensive skills as new capabilities that the organiser expects from the participants, improving participants' skills for the exercise, and solving the incidents within a set time frame. Some participants' comments as follows:

*"For the exercise....we need certain skills in incidents handling. For example analyse malware skills, analyse IP skills, tracing logs and how to analyse information from news, social network, they used news and social network as a medium." (Military Officer 2, Male).*

*"....in previous exercise, the expectation was to solve the issue. During X Maya 5 we were not just to resolve the issue but we have to trace and identify the attacker....try to attack back the attacker." (Military Officer 3, Male).*

Details of participants' merged and categorised results presents a level 1 of Kirkpatrick Model as showed in Table 5.13.

**Table 5.13** Results Categorised in Level 1: Reactions

Objective	Participants realised that the X-Maya exercise is not for competition. All participants agreed that X-Maya is not for testing the participants' skills but for assessing the incident handling reporting procedures and processes. All participants agreed that the X-Maya exercise is a platform to provide knowledge sharing in solving incidents and sharing solutions between agencies. The participants comprehended that the exercises test the communications between sectors during an emergency or crisis. Participants understood that the cyber exercise objective was to achieve effective communication. The participants also understood that the exercise was used to develop awareness of interdependencies and proper communication during a crisis.
Scenario	Participants perceived that each scenario has a different purpose. They also found that the simulation scenario lacked realism. While from ISP perspectives, the scenario created was insufficient for the ISP sector because the scenario was too general, which was suitable for other sectors but not for ISPs. The participants agreed that the cyber exercise scenario could easily be implemented in their organisations, but the methods to fix vulnerabilities are a bit difficult. The threats used in the X-Maya scenario are quite general and of multiple types, including threats on web, file, network, and server (apache). Some ISP participants felt that the exercise should focus more at the network level, which suits their business. The organiser purposefully used different attacks launched simultaneously to different agencies. Some attacks were sent by email. Trojan attacks were also used in the exercise scenario.
Environment	The participants noticed that the environment setup used in X-Maya 5 was similar to previous exercise setups. The simulation operated on a virtual machine (VM) environment with a virtual private network connection. Copies of VM were distributed to participants and operated at their isolated area within the cloud.
Expectation	The organisers were expecting more defensive action from the participants, including fighting back against the attacker. Participants believe that certain skills are needed for the exercise, importantly analysing network traffic and incident handling skills. The participants agreed that time is an important element because they needed to solve every incident within an allocated time.

### 5.8.2 Level 2 :Learning

At level two, learning developed as the participants agreed that they developed new technical skills during the exercise, especially skills related to cyber incident handling. They learnt new procedures to determine cyber threats according to national cyber threat levels, and they learnt how to address incidents and coordinate through communication between agencies as described by participants:

*"We work in a close system, we are less likely to see a real incidents. What we got only a theory....In X Maya we can see how attacks happen. We need to work in team and discuss in how to mitigate the attacks. We learnt new skills and procedure..." (Military Officer 2, Male).*

*"All agencies under Sector Lead share their solutions. They followed steps by steps. It was not for race, they want to see how we handle the situations...using different methodologies...either fast or slow response...how long we used to solve the issues" (Government Agency 2, Officer 1, Female).*

*"At the beginning of the exercise, we were confused..all participants were also confused...we try to understand the scenario ...we discuss among agencies....we try to get a clear picture of the attack" (Government Agency 1, Officer 1, Male).*

*"There were limited seat for X Maya training. We have to pay for the training...." (Government Agency 2, Officer 1, Female).*

*"Skills to handle incidents has already been developed in organisation..but because of cyber is very dynamic, we need creativity to solve the incidents" (Military Officer 2, Male).*

*"..we can see which technical part we need to improve. In one exercise expose us that our technical experience and skills are not up to the national level...In some cyber drill expose us that our SOP was not good enough" (Telecommunication Officer 1, Male).*

The merged participants' outcome on level 2 of Kirkpatrick Model described in Table 5.14.

**Table 5.14** Results Categorical in Level 2: Learning

New Skill	All cyber exercise participants agreed that they have learnt new technical skills during the exercise, specifically, in how to identify an attack when it occurs. Participants learnt how to handle incidents and how to share their problem if they cannot solve them. Some participants have not had opportunities to be involved in the training provided before the X-Maya because the seats for the course were limited. Some participants have already acquired skills from previous government training. The participants could identify the use of latest trends of DDoS attacks and knew how to mitigate risks. Participants learnt how to recognise and classify cyber threats based on national threat levels as low, moderate, high, and crucial. General rules should be applied during a crisis. Organisations need to define crisis stages, and business must run as usual.
Communication	Participants knew how to establish communication during incidents. If an incident happened, they knew how to share solutions between agencies in handling the issues because they understood how to coordinate communication between the sector leader and other agencies.
Experience	Participants felt confused at the beginning of the exercise and not noticed of any attack scenario used in the exercise. Some participants felt that they did not have enough experience in Linux, while some participants agreed that their skills have already been developed in their organisation. They just practised their skills and gained experience, which required more creativity in using the skills.

### 5.8.3 Level 3 : Behaviours

At level three, the X-Maya helped develop the cyber exercise situation awareness by increased network monitoring activities and develop an enthusiasm to safeguard their working environments.

*"The X Maya help us to increase our monitoring activities in our agency." (Government Agency 2, Officer 1, Female).*

*"After attending the X Maya exercise, we become aware on our cyber environment. We updated the anti virus, patches everything to ensure that our environment secure from attacks...we try to safeguard everything in our environment." (Government Agency 1, Officer 1, Male).*

*"...We advise our system administrator to upgrade the systems..." (Military Officer 2, Male).*

The merged outcome on level 3 of Kirkpatrick Model are displayed in 5.15.

**Table 5.15** Results Categorical in Level 3: Behaviour

Situation Awareness	All participants agreed that the X-Maya exercises have improved their situation awareness, especially in network monitoring. Furthermore, with X-Maya experience, the participants have increased their monitoring activities in the agency.
Safeguard	Participants have started asking the system administrator in the organisation to regularly update and patch their computers. They have to ensure that the working environment is secured. They took full responsibility to safeguard all the facilities in their work environments.

#### 5.8.4 Level 4 : Results

At level four, the coding results showed how their organisations benefited from the cyber exercise were through reviewing the existing organisation policies in handling cyber incidents and through new procedures to report incidents.

Some response from the participants' as the following:

*"We reviewed our incidents handling procedures...Previously we report all incidents to the Malaysian Administrative Modernization and Management Planning Unit (MAMPU)...Now the direction of reporting incidents change to Sector Leads." (Military Officer 2, Male).*

*"As awareness to system administrator..anything happened we have to report to the sector lead first before escalates the incidents to other agencies" (Military Officer 3, Male).*

*"The sector leads need to update the incidents following the National track levels of low, medium, high and crucial...based on colours...For low level, business has to operate as usual" (Military Officer 1, Male).*

*"The lead sector will lead to update the NC4. The NC4 belongs to MKN. Whatever direction or instructions given by the NC4 will be channel only to the lead sector. Lead sectors then need to communicate to their agencies." (Telecommunication Officer 2, Male).*

*"We tested our SOP during the X Maya especially on the network communication." (Telecommunication Officer 1, Male).*

Participants' outcome for Level 4 of Kirkpatrick Model merged and presented in Table 5.16.

**Table 5.16** Results Categorised in Level 4 : Results

New Policy	Participants ensured the system administrator in their organisation upgraded and patched the entire server on a periodic basis. At the national level, the lead sector needs to update the NC4 policy. The lead sector then escalates the report to the agencies.
Revised Policy	Participants were involved in creating new organisational incident procedures that suit the agencies.
Revised Procedures	Participants have revised their organisational cyber incident handling procedures and improved the procedure. The previous procedure stated to report any incidents to MAMPU. Now, it has changed the report direction to the sector lead. Reports must be based on flag level. Every level involved different working groups.
New Procedures	Participants were involved in creating new organisational incident procedures that suit the agencies.

## 5.9 Discussion

This section discussed the categorised results according to the four-level Kirkpatrick model of reactions, learning, behaviour, and results. At level one, it presents the participants reactions about the cyber exercise, including the objectives of the exercise, the scenario, the environment, and expectation. At this level, three main purposes of the X-Maya objectives addressed are 1) to provide knowledge sharing on cyber threats, 2) to provide knowledge sharing in solving incidents between agencies, 3) to increase awareness of interdependencies between sectors, and 4) to develop proper communication during a cyber crisis. These findings support the objectives of X-Maya as presented in [Ahm14], which focussed on assessing the effectiveness of action, communications, and national security coordination in dealing with existing cyber crises. The X Maya objectives also match the general purposes of collaborative cyber exercises as presented in Section 2.5.1 and are similar to other collaborative cyber exercise implementations in other countries, as described in Section 3.6. This indicated that Malaysia has awareness regarding the importance of protecting the CNII from cyber threats and developing strategies and implementations as described in Section 3.8.1.

In terms of scenarios, it addressed 1) the simulated scenario used in the X-Maya, 2) types of attacks used in the X-Maya scenario, and 3) levels of attacks. The limitation of using a

virtualisation environment was less realism. Furthermore, the differences in business backgrounds of participants also affected the participants satisfaction in terms of attack types and levels used in the exercise, which may be suitable for other sectors, but not for ISPs, as their business mainly focusses on telecommunications and networks. Thus, they were not really satisfied with the scenario provided. The organiser purposely used several types of attacks (i.e., DDoS, Trojan, etc.) and several levels (web, application, server, etc.), which have different purposes to increase participants awareness of the possibility of sources of cyber-attacks at their organisations. In terms of environment, the participants claimed that the setting was quite similar to previous exercises that used a VM with a Linux environment, and some agencies felt unfamiliar with the environment. The differences in participants environments from the X-Maya exercise reduced the ability for lessons learnt from the exercise, as it could not be transferred to their organisations. To match participants expectations in terms of scenario and environment, the organiser should involve the participants at the planning stages of the exercise, as suggested in [GR10]. Participants perceptions of expectations were 1) gaining defensive skills as new capabilities that the organiser expected from the participants, 2) improving participants skills for the exercise, and 3) solving the incidents within a set time frame. In terms of expectations, they were expecting to solve every incident within the time given and to see how they could communicate to solve the crisis. The communication process and procedures were tested during the exercise. This is to increase the participants awareness of interdependencies and consequences of the crisis if they failed to solve it.

Level two shows how participants benefited from the X-Maya exercise. Learning developed, as the participants agreed that they developed new technical skills during the exercise, especially skills related to cyber incident handling. They learnt new procedures to determine the cyber threats according to national cyber threat levels. They learnt how to address the incidents and coordinate them through communication between agencies. However according to organiser, most participants defence capabilities are still lacking because they were only manage to recover from attacks but not able to respond to the attacker (attack against the attacker).The defending skills are still lacking and need to be increased through future training and practices.

At level three, the behaviour that developed during the cyber exercise was situation awareness that increased their network monitoring activities. It also developed enthusiasm to safeguard their working environments. These individual behaviours contribute to situation awareness of the organisation towards cyber threats. The result at level four showed how their organisations benefited from the cyber exercise through their actions on creating new policies and procedures on cyber incident reporting, which increased coordination and cooperation during cyber crises.

## 5.10 Chapter Contribution

This chapter contributes to the use of the first part of the post assessment of cyber exercise framework to investigate the effect of the exercise on the participants. This chapter also shares the data analysis process for the interview data, including the code generation and the validation of the categories for the interview data. The inter-rater reliability results for categorised items showed the Kappa agreement for the two research assistants (RAs) have achieved almost perfect categorisation on the list of text, according to the code themes.

## 5.11 Summary

This chapter explained the investigation on the effect of the cyber exercise on participants and their organisations using the cyber exercise post assessment framework. The study uses an interview as a methodology to collect data on participants perceptions on the collaborative cyber exercise called X-Maya in Malaysia. Interview data were coded and categorised according to the four-level Kirkpatrick training model for levels of reactions, learning, behaviour, and results, as adopted in the collaborative cyber exercise post assessment framework.



## Chapter 6

# A Preliminary Investigation on Organisation Resilience

### 6.1 Introduction

Many cyber threats are difficult to detect and identify by a single organisation. Collaborative cyber exercises use scenarios to help collaborators practise their crisis management within an interconnected network of the participants [WG04]. In general, a Scenario-Based Exercise (SBE) is defined as *a methodology for an organisation to understand its business environment during a disruption, and to put in place efficient and effective plans for surviving the damage caused by those events* [PCC03].

Through SBEs, participants can simulate cyber risks that could affect their business operations. They provide the opportunity to validate policies, plans and procedures, and processes in their organisations [BP97], [MCD08]. This can enhance their capabilities in the preparation, prevention, response, recovery and continuity operations which contribute to resilience [PCC03].

However, collaborative cyber exercise scenario development is challenging due to the diversity of participants, as well as their different information assets and cyber incidents response policies [WG04]. This causes difficulty for cyber exercise planning teams in building exercise scenarios across-sectors, which challenge participants and, at the same time, satisfy exercise objectives [PCC03].

The objective of cyber crisis management through SBEs is to transfer useful learning outcomes for future and unexpected cyber crisis situations to participants' organisations, and to promote resilience in critical information infrastructures [MCD08],[Wyb08]. Measuring the effectiveness of SBEs in supporting resilience is still subject of research [MCD08]. This preliminary study investigates the suitability of existing organisation resilience tools to as-

sess organisations participating in scenario based cyber exercises. Subsequently, this study investigates the relationship between SBE and organisation resilience (OR). The suitable OR tool, will be used as a second components of the post assessment framework proposed in Section 4.4.

This chapter is organised into nine sections: Section 6.2 provides a background study on SBE. Section 6.3 shares information on organisation resilience and organisation resilience benchmarking tools. Section 6.4 explains details of the investigation. Section 6.5 describes the research methodology and the research instruments used in the study. Section 6.6 shares data collection of the study. Section 6.7 focuses on data analysis, including the reliability, the one-way ANOVA and the correlation tests. Section 6.8 discusses the results of the study. Finally, Section 6.9 summarises the chapter.

## 6.2 Scenario and Scenario-Based Exercise (SBE)

Scenarios were initially pioneered by Herbert Kahn in response to the difficulty of creating accurate forecasts [12]. Scenarios help organisations to deal with uncertainty [MCD08]. A scenario consists of descriptions or narratives of possible future situations that might impact upon the organisation and its environment. They are often used for strategic planning purposes [PCC03].

Today, scenarios are largely used in scenario planning (SP), scenario-based training (SBT) and scenario-based exercises (SBE). In [MCD08] suggested SP and SBT as two cutting-edge methods for organisational leaders to better understand their business environments. These methods allow disaster and crisis response to evaluate numerous outcomes from crisis scenarios [12]. Furthermore, a successful scenario planning effort should enhance the ability of people to cope with future change [PCC03]. Decisions can be made, policies changed, and management plans implemented to direct the system towards a more desirable future [PCC03].

In contrast to SP, SBT and SBE provide learners with opportunities to interact with a possible future [MCD08]. SBT presents participants with an interactive story and places them in a specific environment in which the problem would be encountered [MCD08]. [WG04] explored the use of SBEs in various sectors. Such exercises are used to identify and test the resources and capabilities necessary for preventing, detecting, and responding to cyber security incidents. The authors mentioned three purposes of SBE: 1) to conduct an exercise for awareness, 2) to use it for education and training, and 3) to test their ability to detect and respond in a coordinated manner to an attack or disruption [WG04]. The use of cyber exercise has been enhanced to simulate large-scale attacks in a collaborative manner across sectors, industries and governments [WG04].

## 6.3 Organisation Resilience

Organisational resilience can be defined as a sum of essential concepts. These essential concepts include enterprise risk management, governance, quality assurance, information security, physical security, business continuity, culture and values supported by adaptive leadership [BB10]. Horne and Orr defined resilience : *Resilience is a fundamental quality of individuals, groups, organisations, and systems as a whole to respond productively to significant change that disrupts the expected pattern of events without engaging in an extended period of regressive behaviour* [HO97]. Meanwhile, [PEF<sup>+</sup>12] defined three common characteristics of resilience as follows: 1) capacity to absorb a shock or a deformation, 2) capacity to restore the state of the system after a shock, and 3) capacity to operate correctly even if part of the system is degraded. An organisation with high resilience is able to quickly identify and respond to those situations that present potentially negative consequences, and find solutions to minimise these impacts .

While there is an increasing acceptance of organisational resilience within academic publications as in [McM08] and [Ste10], the concept and features of organisational resilience are still largely undefined and ambiguous [PEF<sup>+</sup>12]. The development of a resilience measurement methodology is also part of research in this area [McM08], [Ste10].

Recent work has developed tools for measuring organisational resilience described in [Ste10], [McM08] and [WKR<sup>+</sup>13]. The organisation resilience tool, BRT-53, was developed by the University of Canterbury in New Zealand in 2010. It was selected to be used in this study; because SBE is one of the indicator attributes under the BRT-53. Furthermore, the tool was used to measure OR in Auckland organisations in 2010. Section 6.3.1 provides the background of the tool.

### 6.3.1 Background of Organisation Resilience Benchmark Tool (BRT-53)

[McM08] used grounded theory to explore organisational resilience in New Zealand. She conducted a qualitative study using semi-structured interviews and a case study of 10 organisations . She provided a relative overall resilience (ROR) metrics which consists of three dimensions: situation awareness, management of keystone vulnerabilities, and adaptive capacity. she also proposed 15 indicators for each dimension [McM08]. [Ste10] enhanced the organisation resilience concept developed in McManus (2008) [Ste10]. She developed a survey-based online benchmark tool known as BRT-53 [WKR<sup>+</sup>13] , [Ste10].

BRT-53 is an organisation-level resilience quantification methodology that empirically assesses behaviour and perceptions connected to the organisation's ability to plan for, respond

to, and recover from emergencies and crises [Ste10]. Using the tool, organisations can review their scores for each of the indicators of organisational resilience, which addresses their organisation weaknesses [Ste10]. As a result, organisations can plan how to leverage their strengths in a crisis [Ste10]. The tool was tested on a random sample of Auckland organisations, and factor analysis was used to develop the instrument [SVS<sup>+</sup>10]. Table 6.1 shows the three dimensions : Situation Awareness (SA), Management of Keystone Vulnerabilities (KV), and Adaptive Capacity with 15 indicators developed by Resilient Organisations Research at the University of Canterbury [Ste10]. This tool was used to assess organisation resilience in this study. The researcher gained permission to use the tool from the University of Canterbury in New Zealand, as described in the email in Appendix B.

**Table 6.1** Organisation Resilience Benchmark Tool (BRT-53) [Ste10],[WKR<sup>+</sup>13]

<b>Code</b>	<b>OR Dimensions &amp; Indicators</b>
<b>SA</b>	<b><i>SITUATION AWARENESS</i></b>
SA1	Role and Responsibilities
SA2	Insurance Awareness
SA3	Connectivity Awareness
SA4	Recovery Priorities
SA5	Internal & External Situation Monitoring & Reporting
<b>KV</b>	<b><i>MANAGEMENT OF KEYSTONE VULNERABILITIES</i></b>
KV1	Planning Strategies
KV2	Participation in Exercises
KV3	Capability & Capacity in Internal Resources
KV4	Capability & Capacity of External Resources
KV5	Organisational Connectivity
<b>AC</b>	<b><i>ADAPTIVE CAPACITY</i></b>
AC1	Silo Mentality
AC2	Innovation & Creativity
AC3	Devolved & Responsive Decision Making
AC4	Information and Knowledge
AC5	Leadership, Management & Governance Structures

## 6.4 An Investigation into Organisation Resilience of CII sectors

### 6.4.1 Purpose of the Study

This study select the BRT-53 survey to assess OR of organisation participated in cyber crisis exercise because the previous study by [Ste10] has showed a correlation between OR and exercises. [Ste10] used the BRT-53 tool to assess OR in organisations in Auckland.

The purpose of the study is to investigate the relationship between SBE and organisation resilience in CII sectors using the BRT-53 Organisation Resilience (OR) benchmark tool, as follows:

#### 1. Experience in SBE:

This study investigates the correlation between OR and SBE across two groups of CII organisations with SBE experience and without SBE experience.

#### 2. Correlation between SBE experience and ORs dimensions:

The aim of the study is to investigates correlations between SBE experience and OR dimensions through the following hypotheses:

*H1: There is a relationship between SBE experience and OR*

*H2: There is a relationship between SBE experience and Adaptive Capacity (AC)*

*H3: There is a relationship between SBE experience and Management of Keystone Vulnerabilities (KV)*

*H4: There is a relationship between SBE experience and Situation Awareness (SA)*

## 6.5 Research Methodology

In order to investigate a relationship between SBE experiences and OR perspective, a preliminary study was conducted using the BRT-53 organisation resilience survey.

### 6.5.1 Research Instrument

BRT-53 uses a 5-point Likert scale ranging from Strongly Agree to Strongly Disagree [Ste10]. The online survey was developed using Qualtrics software and published online. It has a total of 82 questions divided by three sections which cover Background Information (10 questions), Leadership and Culture (24 questions), Network (17 questions), and Change Readiness (31 questions). Our version of the survey was published for two months (from September to November 2013). The online survey can be seen in Appendix J and accessed at <https://www.surveymonkey.com/r/OrganizationResilience>. It covered the three organisation categories from BRT-53: Situation Awareness, Management of Keystone Vulnerabilities and Adaptive Capacity [Ste10] as shows in Table 6.1

### 6.5.2 Ethical Approval

As this study focusing on human participants, this study complied to the BPS ethical guidelines of the University of Glasgow. The Ethics application proposed to use interview questions, organisation resilience and organisation cyber resilience surveys for the research were applied in 10 February 2014. The application was approved by the FIMS ethics committee of the University of Glasgow in June 2014. The approval information presented in Figure 6.1, with the reference no of CSE01346.

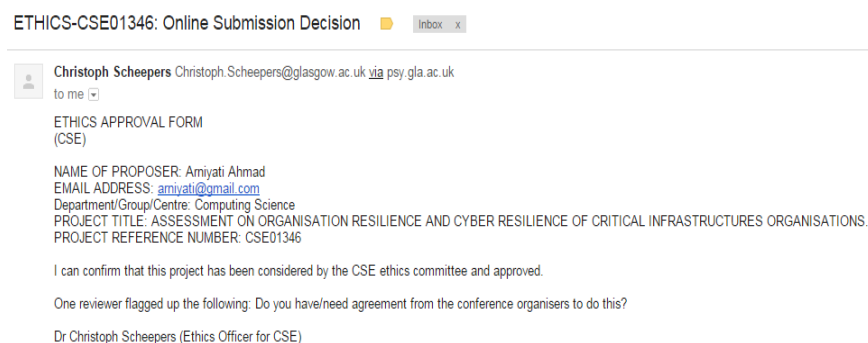


Figure 6.1: Ethical Approval for Data Collection on Organisation Resilience Study

## 6.6 Data Collection

A convenience sample was used. The LinkedIn social network was used to distribute the OR online survey through emails to people who work in information security in several critical infrastructure organisations. LinkedIn is a business-oriented social networking service. Founded in December 2002 and launched on May 5, 2003, it is mainly used for professional networking. As of October 2015, LinkedIn reports more than 400 million acquired users in more than 200 countries and territories [Lin15]. LinkedIn also supports the formation of interest groups, and as of March 29, 2012 there are 1,248,019 such groups whose membership varies from 1 to 744,662 [wik16]. The majority of the largest groups are employment-related, although a very wide range of topics cover mainly professional and career issues, and there are currently 128,000 groups for both academic and corporate alumni [wik16]. The survey was emailed to people in six LinkedIn discussion groups, as shown in Figure 6.2. The groups comprise:

1. Information Security Community
2. Malaysia Oil and Gas
3. ISTT - Information Security Think Tank
4. Critical Infrastructure Protection
5. International Association of Critical Infrastructure
6. Telecoms Professionals

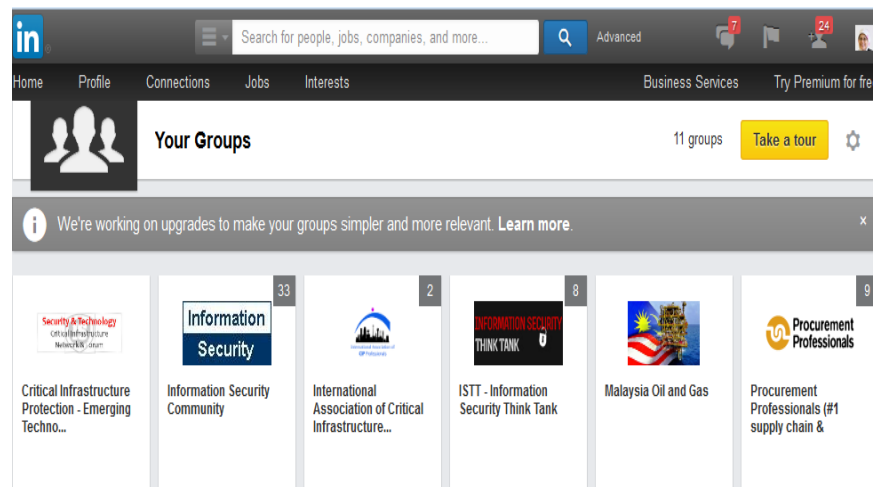


Figure 6.2: LinkedIn Groups

## 6.7 Data Analysis

### 6.7.1 Demographic Analysis

This study used a sample from 10 critical information infrastructures: Electricity/Power, Water Supply, Nuclear, Telecommunications, Internet Service Provider, Transport, Oil and Gas, Banking and Finance, Government Service, and Health. In total, there were 102 responses to the survey from 200 emails sent to people in the respective sectors. As shown in Table 6.2, the highest respondents were from Government Service (55%), followed by Oil and Gas (13%), Telecommunications (8%), Health (6%), and other (5%). While 4% were from Electricity/Power and Internet Service Provider, 3% were respondents from Banking and Finance. The lowest (1%) were respondents from Water Supply, Nuclear, and Transport. Unfortunately, there was no respondent from the Food Supply sector.

**Table 6.2** Participants' Response to Organisation Resilience Survey

Sector	Response	%
Electric/Power	4	4
Water Supply	1	1
Nuclear	1	1
Telecommunication	8	8
food Supply	0	0
Internet Service Provider	4	4
Transport	1	1
Oil and Gas	13	13
Banking and Finance	3	3
Governance Service	56	55
Health	6	6
Others	5	5
Total	102	100

#### 6.7.1.1 Response on Organisation Type

Table 6.3 shows 69 (68%) respondents of the survey, were from public organisations and 33 (32%) were from private organisations.



**Table 6.3** Participants' Response on Organisation Type

Sector	Frequency	%
Public	69	68
Private	33	32
Total	102	100

### 6.7.1.2 Response on Organisation Size

Table 6.4) shows the highest number of respondents 34 (33%) were from companies with 10-49 employees, 32 (31%) were from companies that have more than 500 employees, 22(22%) from companies with 250-499 employees, 10 (10%)from companies with 50-249 employees, and 4(4%) from the smallest scale company (fewer than 10 employees).

**Table 6.4** Participants' Response on Organisation Size

Organisation Size	Frequency	%
<10	4	4
10 to 49	34	33
50 to 249	10	10
250 to 499	22	22
>500	32	31
Total	102	100

### 6.7.1.3 Response on Participants' Role

Table 6.5 shows that the highest member of respondents 39(38%) were support staff, followed by 32 (31%) in management. Sixteen(16%) were engineers and five(5%) were in administration.

**Table 6.5** Participants' Response on Role in Organisation

Role	Frequency	%
Management	33	32
Administration	5	5
Engineer	16	16
Support	39	38
Other	33	32

#### 6.7.1.4 Response on Work Experiences in the organisation

Table 6.6 shows that the highest number of respondents 64 (63%) have less than 10 years of experience followed by 25 (25%) between 10 to 15 years and seven(7%) between 16 and 20 years. Six(6%) have more than 20 years of work experience.

**Table 6.6** Participants' Response on Work Experience in Organisation

Work Experience	Frequency	%
Below 10 Years	64	63
10 to 15 Years	25	25
16 to 20 Years	10	10
Above 20 Years	22	22
Total	102	100

#### 6.7.2 Reliability Analysis

A reliability test was conducted using Cronbach's alpha to assess the internal consistency of the benchmark tool [San99]. The reliability test was conducted on organisation resilience indicators to measure the internal consistency of the tool used. Cronbach's alpha coefficient is commonly used as an indicator of internal consistency and should have values of 0.7 or above to indicate strong item covariance [Pal13]. Table 6.13 shows that Cronbach's alpha coefficient for organisation resilience indicators ranged from 0.709 to 0.837. Thirty nine items that have Cronbach's alpha coefficient below 0.7 have been removed. Remains of thirty three items used in data analysis. The reliability test result was then used to calculate the Relative Overall Resilience (ROR) score.

**Table 6.7** Reliability of OR Dimensions and Indicators

<b>Dimension/Factor/ Indicator</b>	<b>Cronbach Alpha</b>	<b>Cronbach Alpha based on Standardised Items</b>	<b>No of items</b>
<b><i>Adaptive Capacity (AC)</i></b>			
Information & Knowledge	0.729	0.727	3
Leadership, Management & Governance Structures	0.724	0.716	5
Innovation & Creativity	0.729	0.738	3
Devolved & Responsive Decision Making	0.784	0.788	3
<b><i>Management of Keystone Vulnerabilities (KV)</i></b>			
Participation in Exercises	0.804	0.804	2
Capability & Capacity of Internal Resources	0.837	0.840	2
Capability & Capacity of External Resources	0.745	0.749	2
Organisational Connectivity	0.824	0.829	2
<b><i>Situation Awareness (SA)</i></b>			
Role & Responsibilities	0.707	0.713	3
Connectivity Awareness	0.709	0.709	2
Recovery Priorities	0.796	0.799	3
Internal & External Situation Monitoring & Reporting	0.734	0.733	3

### 6.7.3 Correlation Analysis

Pearsons correlation is a measure of the strength of association between two or more variables [Pal13]. The strength of the relationship between two variables was determined by the correlation coefficient and the significance [Pal13]. The correlation coefficient normally used is Pearsons  $r$ , which shows a strong positive or negative relationship between -1 and +1. It also provides the direction of a relationship between two variables [CH96]. Meanwhile, the significance (Sig.) shows confidence in the obtained results. This study investigates any relationship between SBE experience and OR, as explained in the next section.

### 6.7.3.1 Correlation Test between SBE Experience and OR Dimensions

To study the correlation between OR and two SBE groups, the data has been grouped into participants that have SBE experience and without SBE experience. Table 6.8 shows the distribution of the 39 (38%) participants with SBE experience and 61 (62%) participants without SBE experience.

**Table 6.8** Distribution of Respondents with SBE Experience

SBE Experience	Frequency
YES	39
NO	63
Total	102

Table 6.9 shows the results of Pearsons correlation  $r$  value of  $0.112$ , which indicates a weak relationship between SBE experience and OR. This relationship is also not statistically significant, with  $Sig. = 0.271$ , which falls outside  $0.05$ . This rejects the hypothesis which indicates that there is a relationship between SBE experience and OR.

**Table 6.9** Correlation between SBE and OR

SBE Experience	OR
Pearson Correlation ( $r$ )	0.112
Sig.(2-tailed)	0.271
N	102

### 6.7.3.2 Correlation Test between SBE Experience and OR Dimensions

This correlation test determine if there is any relationships between SBE Experience and organisation resilience dimensions including: Adaptive Capacity (AC), Management of Keystone Vulnerabilities (KV) and Situation Awareness (SA). Table 6.10 and Table 6.11 show the results of Pearsons correlation  $r$  value of  $0.03$  for AC and  $r$  value of  $0.100$  for KV, both of which indicate a weak relationship between SBE Experience and AC, and also a weak relationship between SBE Experience and KV. Both results were not statistically significant, with values of  $Sig=0.977$  for AC and  $Sig=0.325$  for KV, this rejects the H2 and H3 hypotheses. There is no relationship between SBE Experience with Adaptive Capacity and no relationship between SBE Experience with Keystone Vulnerabilities.

**Table 6.10** Correlation Test between SBE and Adaptive Capacity

SBE Experience	Adaptive Capacity (AC)
Pearson Correlation ( $r$ )	0.003
Sig.(2-tailed)	0.977
N	102

**Table 6.11** Correlation Test between SBE and Management Keystone Vulnerabilities

SBE Experience	Management Keystone Vulnerabilities (KV)
Pearson Correlation ( $r$ )	0.100
Sig.(2-tailed)	0.325
N	102

Table 6.12 shows the results of a Pearsons correlation  $r$  value of  $0.209$  for Situation Awareness (SA). Even though it shows a weak relationship between SBE Experience and SA, this result is statistically significant with  $Sig=0.038$  within  $0.05$ , so hypothesis H4 is accepted. This indicates that there is a relationship between SBE Experience and Situation Awareness.

**Table 6.12** Correlation between SBE Experience with OR Indicators

SBE Experience	Situation Awareness (SA)
Pearson Correlation ( $r$ )	0.209
Sig.(2-tailed)	0.038
N	102

### 6.7.3.3 Correlation Test between SBE Experience with OR Indicators

Table 6.13 shows the correlation test for organisation resilience indicators. The test on the 12 organisation resilience indicators showed that only three indicators have a relationship with SBE experience. Meanwhile, it shows weak relationships with Pearsons correlation  $r$  value of  $0.220$  for Capability and Capacity of External Resources, Pearsons correlation  $r$  value of  $0.250$  for Connectivity Awareness, and Pearsons correlation  $r$  value of  $0.201$  for Recovery Priorities. Moreover, the result showed a negative relationship between SBE and Devolved & Responsive Decision Making with  $r=-0.197$ , and a negative relationship between SBE and Capability & Capacity of Internal Resources with  $r=-0.116$ .

**Table 6.13** Pearson Correlation between SBE with OR Dimensions and Indicators

<b>Dimension/OR Indicator</b>	<b>Pearson Correlation</b>	<b>Sig.(2-tailed) n=102</b>
<b><i>Adaptive Capacity (AC)</i></b>		
Information & Knowledge	0.089	0.382
Leadership, Management & Governance Structure	0.153	0.132
Innovation & Creativity	0.028	0.782
Devolved & Responsive Decision Making	-0.197	0.051
<b><i>Management of Keystone Vulnerabilities (KV)</i></b>		
Participation in Exercises	0.147	0.148
Capability & Capacity of Internal Resources	-0.116	0.255
<i>*Capability &amp; Capacity of External Resources</i>	0.220	0.029
Organisational Connectivity	0.044	0.669
<b><i>Situation Awareness (SA)</i></b>		
Role & Responsibilities	0.140	0.167
<i>*Connectivity Awareness</i>	0.250*	0.013
<i>*Recovery Priorities</i>	0.201*	0.046
Internal & External Situation Monitoring & Reporting	0.088	0.386

#### 6.7.4 A OneWay ANOVA of OR Significant Test

##### 6.7.4.1 An Significant Test on OR between Two SBE Groups

A one-way ANOVA test was used to investigate whether there were statistically significantly different OR means between two groups with scenario-based exercise experiences and without scenario-based exercise experiences. The hypothesis is that there is no significant difference between groups with and without experience in scenario-based exercises in relation to organisational resilience.

*Ho: There are no statistically significant difference means between groups with Scenario-Based Exercise and without Scenario-Based Exercise*

*Ha: There is statistically significant difference between means groups with Scenario-Based Exercise and without Scenario-Based Exercise*

**Table 6.14** Descriptive Analysis of SBE Groups

OR			
SBE experience	N	Mean	df
YES	39	2.23	0.55
NO	63	2.24	0.43

**Table 6.15** ANOVA Tests on Scenario Based Exercise Experience Groups

Organisation Resilience					
SBE	Sum of Square	df	Mean Square	F	Sig
Between Groups	0.004	100	0.004	0.019	0.891
Within Groups	22.733	101	0.227		

The one-way ANOVA result in table 6.15 showed that the  $p$  value is 0.89. Furthermore, because  $0.891 > 0.05$ , there is no statistically significant difference between means of two groups with experience in scenario-based exercise ( $mean = 2.23$ ) and without experience in scenario-based exercise ( $mean = 2.24$ ) in relation to OR as in Table 6.14.

## 6.8 Result Discussion

Regarding the investigation on the relationship between SBE experiences and OR perspectives, the correlation test results indicate that there is not enough evidence to support our hypotheses. Meanwhile, the investigation between SBE experiences and organisation resilience indicators showed a weak relationship with Situation Awareness (SA). However, the result supports theories that SBE experiences contribute to Situation Awareness, as discussed in [BVH02] and [MFS<sup>+</sup>11]. Moreover, the qualitative study in Section 5.7.4 supported the contributions of SA to participants' behaviour after participating in collaborative cyber exercises.

Although Adaptive Capacity and Management of Keystone Vulnerabilities contribute to an organisations resilience in coping with disasters, as addressed in [BB11], there is a lack of evidence supporting the relationship between SBE experiences with both indicators. Other correlation results show relationships between SBE experience and organisation resilience

indicators Capability and Capacity of External Resources, Connectivity Awareness, and Recovery Priorities. Overall, the results of this study have not provided enough evidence to relate the relationship of SBE to organisation resilience.

The results of the one-way ANOVA tests for the OR mean difference between groups with scenario-based experiences and crisis experiences were not supported. Some other factors that influence the results and need further investigation are as follows: the role of respondents in the organisation and their experiences, which might have an influence on the results as shown in tables 6.5 and 6.6. The role of top management has significant direct and indirect influences on employees' attitudes towards, and the subjective norm of, perceived behaviour, as explained in [HO97]. Another factor that needs to be considered is the sample size. In order to achieve a representative sample, the sampling frame must be unbiased and complete; however, this is very difficult when surveying multiple organisations as no complete list is available [GRM03].

As a result of the study, due to limited evidence to support the relationship of SBE with OR, the BRT-53 tool will not be included in the proposed post assessment framework. Next study proposed in Chapter 7, is an investigation of organisation cyber resilience using C-Suite Executive tool developed by World Economic Forum and data collected from participants of the X Maya national collaborative cyber exercise in Malaysia. The tool used to investigate the Executive-level awareness and leadership of cyber risk management that contributes to organisational cyber resilience in CNII sectors participated in collaborative cyber exercise.

## 6.9 Summary

This chapter provides an investigation of the correlation between scenario-based exercises and organisation resilience perspectives. The preliminary investigation was conducted using a resilience benchmark tool developed by the University of Canterbury in New Zealand. A correlation test was conducted to see relationships between OR and SBE experiences. Other investigations were conducted, on correlations between SBE experiences with OR dimensions and indicators of Adaptive Capacity (AC), Management of Keystone Vulnerabilities (KV), and Situation Awareness (SA). Correlation test results indicate that there is not enough evidence to support the relationship between SBE experiences and OR perspectives, including the OR dimension, except for a weak relationship between SBE experiences with SA. Furthermore, the one-way ANOVA test of ORs significant difference between groups with SBE experiences and without SBE experiences showed no differences between them. This support our decision to use the organisation cyber resilience survey developed by the World Economic Forum in the next study.



## Chapter 7

# An Investigation on Organisation Cyber Resilience of Ten CNII Sectors

### 7.1 Introduction

The framework for collaborative cyber exercise proposed in Chapter 4 consists of participant and organisation components. The participant element was investigated in the qualitative study of Chapter 5. This chapter presents the second component of the framework on organisational cyber resilience (OCR). It focuses on research Question 5 (RQ5), 'how to assess organisation cyber resilience of CNII sectors involved in collaborative cyber exercises?'.

The resilience of critical infrastructure is usually examined within a technical setting [GMP11]. Critical infrastructure resilience has a broad impact because of its capacity to affect the operation of nations to shape public confidence [BG13]. When critical infrastructure is resilient, it continues to function even under challenging circumstances [LEP<sup>+</sup>13]. This is important to raise awareness on CI interdependencies among CIs stakeholders.

Collaborative cyber exercises implementations in Chapter 3 shares how the exercise can be used to promote interdependencies awareness of participated organisation. However as addressed in Section 1.3, the lack of interest of organisation to participate in a collaborative due to the difficulties of senior management to find suitable by emergency planning groups, which organisation could not easily commit resources to the activities that have a high social value, but no significant value in financial contributions in return [The13]. This study used the C-Suite Executive checklist to investigate the participants' perceptions on executive level awareness of interdependencies and their commitment to cyber risks management in their organisation. The checklist has three main components of governance, programme and network which contribute to organisation cyber resilience.

This chapter focuses on OCR perceptions of the 10 CNII sectors involved in the X-Maya exercise. This chapter explains the study in 13 sections. Section 7.2 defines the background of cyber resilience. Section 7.3 provides details of the investigation. Section 7.4 discusses the research methodology, research instruments, and pilot test. Data collection covered in Section 7.5. Section 7.6 elaborates on the data analysis. Section 7.7 provides details of a reliability test. Section 7.8 provides a Pearson correlation test also conducted to assess the consistency of items in the C-Suite Executive survey developed by the World Economic Forum. Section 7.9 describes the significance of the study on the OCR of 10 CNII sectors. Section 7.10 specifies the development of an OCR maturity model. Section 7.11 discusses the overall results of the study. Section 7.12 addresses contributions of the study. Finally, Section 7.13 summarises the chapter.

## 7.2 Cyber Resilience

Cyber resilience is defined in the literature in many different ways, such as the following: 1) the ability of systems and organisations to withstand cyber events, measured by the combination of a mean time to failure to a mean time to recovery [BG11], 2) the ability of systems to absorb external stress [LEP<sup>+</sup>13], and 3) the system capability to create foresight and to recognise, anticipate, and defend against risk before adverse consequences occur [BG11]. The literature on cyber resilience also has diverse focus:

The cyber resilience definitions in these literature are more focused on system resilience. Cyber resilience is multidisciplinary, which requires a different mindset than a traditional IT security and information security disciplines which more focuses on implementing security standards and security measures [HS14]. [Rid11] suggested that an organisation is resilient to cyberattacks when it adopts an intelligence-driven approach to cyber security and layers security controls.

This study focuses on OCR by building on an initiative developed by the World Economic Forum in 2012. The core principles of the World Economic Forums Partnering for Cyber Resilience initiative were established to raise awareness of cyber risk and to build commitment regarding the need for more rigorous approaches to cyber risk mitigation [Wor15]. This chapter describes the investigation of OCR perceptions in 10 CNII sectors involved in X-Maya. The World Economic Forum and its cyber activities are summarised in the next section.

**Table 7.1** Research on cyber resilience

<b>Cyber Resilience Topic</b>	<b>Research Focus on Cyber Resilience</b>
Vocabulary of cyber resilience techniques	[BG13] proposed a vocabulary to describe the effects of cyber adversary activities in the context of the cyberattack lifecycle, such as recon, weaponise, deliver, exploit, control, execute, and maintain. This vocabulary was mapped to cyber resilience techniques of adaptive response, analytic monitoring, coordinated defence, deception, diversity, dynamic positioning, dynamic representation, non-persistence, privilege restriction, realignment, redundancy, segmentation, substantiated integrity, and unpredictability.
Cyber resilience matrix for cyber systems	[LEP <sup>+</sup> 13] provided a cyber resilience matrix of four domains taken from the network centric warfare (NCW) doctrine of physical, information, cognitive, and social to four stages of the event management cycle: plan/prepare, absorb, recover, and adapt taken from the National Academy of Sciences (NAS).
Resiliency techniques	[GMP11] provided several classes of resiliency techniques in two approaches: 'proactive techniques' and 'reactive techniques'. Proactive techniques include data availability, data integrity, and segmentation. Reactive techniques apply the response to adversary activities through dynamic composition, diversity, dynamic reconstitution, dynamic reconfiguration, and deception.
CERT resilience management model (CERT RMM) [AD10]	The CERT resilience management model includes and integrates activities from security, business continuity, and aspects of IT operation management. The CERT RMM has 26 process areas (PAs). The CERT RMM PAs are organised into four high level operational resilience categories of engineering, enterprise, management, and operation and process management.

## 7.2.1 Organisation Cyber Resilience

## 7.2.2 World Economic Forum

The World Economic Forum was established in 1971 as a not-for-profit foundation and is head quartered in Geneva, Switzerland [Wor12b]. The Forum is an international institution committed to improve the state of the world through public-private cooperation. It is independent, impartial and not tied to any special interests. It builds, serves and sustains communities through an integrated concept of high level meetings, research networks, task forces and digital collaboration [Wor12b].

In 2012, a group of business leaders attended the World Economic Forums panel discussion on cyberattacks. This provided a strong indicator regarding the uncertainty of cyber security in the majority of businesses [Wor12a]. While there seemed to be growing sense of urgency and attention from business leaders, there also seemed to be a growing principle for cyber resilience derived from stakeholder dialogue across multiple regions and sectors [Wor15]. The core principles identified are [Wor12a]:

1. Recognition of interdependence: All parties have a shared interest in fostering a common, resilient digital ecosystem;
2. Role of leadership: Executive-level awareness and leadership of cyber risk management are encouraged.
3. Integrated risk management: A practical and effective implementation programme that aligns with existing frameworks should be developed.
4. Promote uptake: Suppliers and customers alike are encouraged to develop similar levels of awareness and commitment.

These core principles were used to formulate the C-suite executive checklist used for the study discussed in Section 6.4.1.

## **7.3 An Investigation on Organisation Cyber Resilience of Ten CNII Sectors in Malaysia**

The National Cyber Security Policy (NCSP) states that *Malaysias Critical National Information Infrastructure (CNII) must be secure and resilient, that is, immune against threats and attacks to its systems* [bH11]. As discussed in Section 3.8.1, in the Malaysia critical information infrastructure, as defined by the NCSP, 10 critical sectors:

1. National defence and security,
2. Banking/finance,
3. Information and communications,
4. Energy,
5. Transportation,
6. Water,
7. Health services,
8. Government,
9. Emergency services, and
10. Food and agriculture.

The Malaysia National Security Council with the support of Cyber Security Malaysia organised the national collaborative Cyber Crisis Exercise, known as X-MAYA [Ahm14] as discussed in Chapter 3. This program was conducted to assess the capabilities of CNII agencies to deal with cyber incidents [Ahm14].

### **7.3.1 Purpose of The Study**

The purpose of this study was as follows:

1. To ensure the suitability of the C-Suite Executive checklist to assess the OCR perceptions.
2. To assess the OCR perceptions of 10 CNII sectors involved in collaborative cyber exercise, X Maya in Malaysia, and
3. To develop the OCR perceptions Maturity Model of 10 CNII sectors involved in the exercise.

### 7.3.2 Ethical Approval

As this study focuses on human participants, it complies to BPS ethical guidelines of the University of Glasgow. The Ethics application proposed to use organisation cyber resilience surveys was submitted on 16 May 2014. The application was approved by the FIMS ethics committee of the University of Glasgow in June 2014. The approval is presented in Figure 5.1 of Section 5.2.2.

## 7.4 Research Methodology

This study used the C-Suite Executive checklist developed by the World Economic Forum in 2012 for data collection, as listed in Table 7.2. The researcher gained permission to use the C-Suite Executive checklist from the World Economic Forum committee, as presented in the email in Appendix A.

### 7.4.1 Research Instrument

We used an online version of the C-Suite Executive checklist in [Wor12a], which is attached in Appendix F. The questionnaire contains 19 questions that cover three main categories : Governance (eight questions), Programme (eight questions) and Network (three questions). Using a five-point Likert scale, defined from *1: does not describe my organisation at all* to *5: accurately describes my organisation*. The average score from all items provides the OCR result. In order to ensure the suitability of the tool used to measure the OCR, a reliability test on the C-suite executive items was conducted. The online survey can be accessed at [https://www.surveymonkey.com/r/Cyber\\_Resilience](https://www.surveymonkey.com/r/Cyber_Resilience).

### 7.4.2 Pilot Study

The term pilot study referred as a feasibility study involved small scale version or trial run of research instruments for a major study [BR94]. For this study, a pilot study was conducted from 12 to 13 February 2014 to test the C-Suite Executive Checklist. The pilot survey was distributed to 15 participants during the Critical Infrastructure Protection and Resilience Europe (2014) conference in London. This was attended by people from various critical infrastructure sectors based in Europe. The study used a printed version of the online survey, as shown in Appendix F. The pilot test was conducted to collect an expert perspective in terms of the survey format, confidentiality, structure, and the meaning. Participants' views were collected using the form attached with the survey, as displayed in Appendix E. The pilot test results are discussed next.

**Table 7.2** C-Suite Executive Checklist Survey Items [Wor12a]

<b>Item Code</b>	<b>Governance(GV)</b>
GV1	The chief executive and executive management team are responsible for overseeing the development and confirming the implementation of a programme of best practices for cyber risk management
GV2	The chief executive and executive management team ensure that the programme is reviewed for effectiveness and, when shortcomings are identified, corrective action is pursued
GV3	The chief executive and executive management team demonstrate visible and active commitment to implementation of the principles
GV4	Executives and managers are responsible for understanding at the appropriate level how cyber risks could impact and originate from their line of business
GV5	Senior leadership understands who is responsible for managing cyber risks when managing security incidents
GV6	The organisation has access to cyber expertise at its highest management levels
GV7	The organisation continuously improves the integration of its cyber risk management with its other risk management initiatives
GV8	The chief executive(or equivalent) has a clear decision path for action and communication in response to a significant security failure or accident
<b>Item Code</b>	<b>Programme (PRG)</b>
PRG1	The organisation conducts comprehensive assessments for its vulnerabilities to internal and external cyber risks that are appropriate for its industry and sector
PRG2	The organisation monitors the effectiveness of its cyber risk management strategy
PRG3	The organisation periodically internally verifies its compliance with rules and regulations
PRG4	The organisation's commitment to the programme is reflected in its policies and practices
PRG5	Managers, employees and agents receive specific training on the programme, tailored to relevant needs and circumstances
PRG6	The organisation has identified its data and information as vital assets and organise its programme around the recognition that data and information have value that can be separately and recognised and protected
PRG7	The risk management programme includes all material third party relationships and information flows
PRG8	The organisation conducts comprehensive internal short and long term cyber risks impact assessments
<b>Item Code</b>	<b>Network(NTW)</b>
NTW1	The organisation seeks to ensure that its suppliers and relevant third parties adhere to the organisation's specific cyber risk management standards or industry best practices, in line with the principles and formalises this requirements using contractual obligations
NTW2	The organisation has built relationships with its peers and partners to jointly manage cyber risks and more effectively deal with cyber incidents
NTW3	The risk management programme includes all material third party relationships and information flows

### 7.4.2.1 Demographic Analysis of Participants

The number of respondents involved in the pilot test by sectors, as displayed in Table 7.3, shows most participants were from the government and the information and communication sectors (four respondents from each sector), followed by the energy and the banking and finance sectors with two respondents from each. This was followed by representatives from the transportation, the emergency service, and the national defence and security sectors. There were no representatives from the water, the health services, or the food and agriculture sectors.

**Table 7.3** Demographic Analysis of Participants in the Pilot Study

Sector	Response Per cent	Response Count
National Defence and Security	6.7%	1
Energy	13.3%	2
Banking and Finance	13.3%	2
Information and Communication	26.7%	4
Transportation	6.7%	1
Water	0.0%	0
Health Services	0.0%	0
Government	26.7%	4
Emergency Service	6.7%	1
Food and Agriculture	0.0%	0
Total		15

### 7.4.2.2 Response on the Appropriateness Use of Language in the Survey Questions

As described in Table 7.4, in terms of appropriateness of the language used in developing the items of the survey, 10 people rated the governance items as good, three found it very good, and two rated it as fair. While for the second component, programme, 9 rated it as good, four rated it as fair, and two rated it as very good. The last component was network, seven respondents chose fair and good, while one rated it as very good.

**Table 7.4** Response on the Appropriateness of Language of the Survey

Answer Options	Poor	Fair	Good	Very Good	Excellent	Average
Language of governance questions	0	2	10	3	0	3.07
Language of programme questions	0	4	9	2	0	2.87
Language of network questions	0	7	7	1	0	2.60



### 7.4.2.3 Response on the Number of Questions of Each of Component

Table 7.5 describes the response on the number of questions in each component: governance, programme, and network. For governance, 12 people rated it as good, and three rated it as very good. For the number of items in the programme component, 11 respondents rated it as good, three rated it as very good, and one rated it as fair. For the number of questions in the network component, 11 rated it as good, three rated it as fair, and one rated it as very good.

**Table 7.5** Response on the Number of Question in Survey

Answer Options	Poor	Fair	Good	Very Good	Excellent	Average
No of questions of governance	0	1	12	3	0	3.20
No of questions of programme	0	1	11	3	0	3.13
No of questions of network	0	3	11	1	0	2.87

### 7.4.2.4 Response on the Content of Each Component

As referenced in Table 7.6, most participants (11 respondents) found the governance content of the survey was good, three found it very good, and one found it fair. While for programme, 10 found the content of the items was good, three found it very good, and two found it fair. Lastly, for network item content, 10 found it good, three found it fair, and two found it very good.

**Table 7.6** Response on OCR's Components

Answer Options	Poor	Fair	Good	Very Good	Excellent	Average
Rating content of the governance	0	1	11	3	0	3.13
Rating content of the programme	0	2	10	3	0	3.07
Rating content of the network	0	3	10	2	0	2.93

### 7.4.2.5 Response on the Confidentiality of the Survey Questions

Table 7.7 shows the responses on confidentiality of the survey items. For governance, 13 found the confidentiality of the survey good, and two found it very good. For the programme component, 12 people found the confidentiality good, two found it very good, and one found it fair. While for the network component, 12 found the confidentiality of the items good, two found it very good, and one found it fair.

**Table 7.7** Response on the Confidentiality of the Survey

Answer Options	Poor	Fair	Good	Very Good	Excellent	Average
Confidentiality in the governance	0	0	13	2	0	3.13
Confidentiality in the programme	0	1	12	2	0	3.07
Confidentiality in the network	0	2	12	1	0	2.93

Based on good responses on the OCR survey format including the appropriateness of the language, content and confidentiality in the pilot study, the survey was used to collect data from the participants that experienced the X-Maya exercise in Malaysia.

## 7.5 Data Collection

Data for this study was collected using an online version of the C-Suite Executive checklist in Appendix F. Participants were involved with the X Maya 5 exercise in November 2013. Five sector leaders were contacted to distribute the online survey to the ten CNII sectors. They were from Government, national defence and security, banking and finance, energy, information and communication. Sector leaders then forwarded the survey to all participants under their sector. The survey also being given to the interview respondents in Section 5.5.1.

## 7.6 Data Analysis

Data analysis involved the following two types of demographic analyses and three statistical analyses:

1. Demographic data on participants provide background information including sectors, size of their organisations, roles, and work experience in their sectors. It also included data on the cyber risk management programmes in participants' organisations, the date of the cyber security training attended, and the security certification.
2. Demographic data on cyber exercises, such as the types of cyber exercises that participants have attended and the level of the exercises.
3. Reliability test on the instrument used.
4. Correlation test between the components of OCR; governance, programme, and network.
5. Significance analysis on the OCR scores for each CNII sector.

Details of the analyses are provided in the following sections.

### 7.6.1 Demographic Analysis

A total of 83 participants answered the online survey. Figure 7.1 shows the number of respondents involved in this study. It showed a high frequency of respondents from information and communication (13), banking and finance (12) and the transportation (10) sectors. While the same number of respondents were from energy (6), Water (6), and the health (6) sectors.

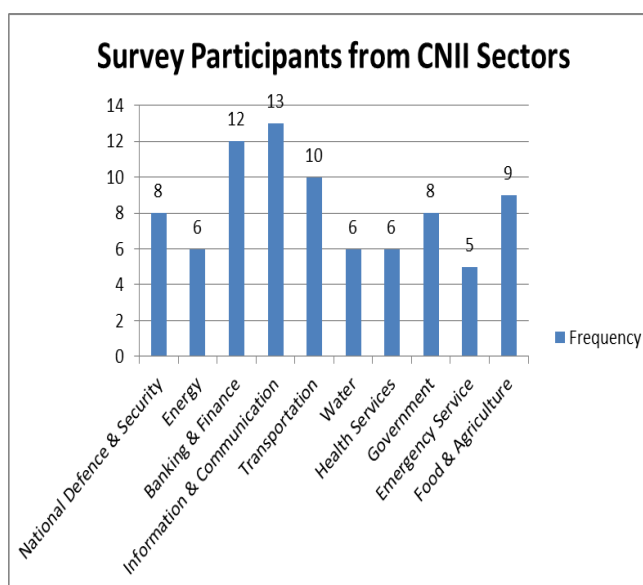


Figure 7.1: Number of Respondents

#### 7.6.1.1 Response on Organisation Size

Respondents were asked about the size of their respective organisations. The results in Table 8 indicate that the largest group of employees (73; 88%) were from large organisations that had 500 or more employees. The remaining four (5%) were from organisations with between 250 and 499 employees, three (4%) were from organisations with 50 to 249 employees, two (2%) were from organisations with 10 to 49 employees, and one (1%) was from a small organisation with less than 10 employees.

**Table 7.8** Response in Organisation Size

Number of Employee	Frequency	%
<10	1	1
10 to 49	2	2
50 to 249	3	4
250 to 499	4	5
>500	73	88
Total	83	100

### 7.6.1.2 Response on Participants' Roles

Data collected on participants' role in the organisations are presented in Table 7.9, which showed that 36 (43%) were technical advisor to their organisation, 18(22%) were in other role as asked in the survey, 17(21%) were decision makers, while the same number of people (6;7%) were policy maker and (6;7%) strategic planner.

**Table 7.9** Response on Role in Organisation

Role	Frequency	%
Decision Maker	17	21
Strategic Planner	6	7
Policy Maker	6	7
Technical Advisory	36	43
Other	18	22
Total	83	100

### 7.6.1.3 Response on Work Experience in the Organisation

In terms of respondents' work experience in organisations, Table 7.10 shows that 40 (48%) had 4 to 10years of experience with their organisation, 26(32%) had 11 to 20 years of experience, 14 (17%) had 1 to 3 year experience, and three(3%) had 21 or more years of experience in their respective organisations.

**Table 7.10** Response on Work Experience in Organisations

Working Experience in Organisation	Frequency	%
1 to 3 years	14	17
4 to 10 years	40	48
11-20 years	26	32
>21	3	3
Total	83	100

### 7.6.1.4 Response on Work Experience in Industry Sectors

In terms of respondents' work experience in their industry sectors, Table 7.11 shows that 46 (55%) had 4 to 10 years of experience, 34(41%) had 11 to 20 years of experience, and three(4%) had 21 or more years of experience in their respective work sectors.

**Table 7.11** Response on Work Experience in Respective Sectors

Working Experience in Industry Sector	Frequency	%
4 to 10 years	46	55
11 to 20 years	34	41
>21	3	4
Total	83	100

#### 7.6.1.5 Cyber Risk Management Programme

Data on Cyber Risk Management Programmes in the participants' organisations are based on multiple responses shown in Table 7.12 : 56 (67.5%) have risk management plans in their organisations, 51(67%) have business continuity plans, 51(61.4%) have crisis management plans, 45 (54.2%) have emergency plans, three (3.6%) have disaster recovery plans, four (4.8%) were still waiting for any approval of a plan, and five (6.0%) were not sure about any plan in their organisations, while 12 (14.5%) have different plans from those listed above.

**Table 7.12** Response on Cyber Risks Management Programme in Organisations

Cyber Risk Management Programme	Frequency	%
Business Continuity Plan	52	67
Emergency Plan	45	54.2
Crisis Management	51	61.4
Risk Management	56	67.5
Disaster Recovery	3	3.6
Waiting for Approval	5	6.0
Not Sure	5	6
Others	12	14.5

#### 7.6.1.6 Participants' Involvements in Cyber Risk Management Programmes

In terms of respondents' involvement in the cyber risk management programme in their organisations as showed in Table 7.13, 59(71.1%) were involved in risk management plans, and 46 (55.4%) were involved in business continuity plans. Emergency plans and crisis management plans have the same rates at 37 (44.6%) respondents, while 14 (16.9%) were involved with other types of plans. Two (2.4%) were involved in simulation, and one (1.3%) was involved in a disaster recovery plan.

**Table 7.13** Response on Involvement in Cyber Risks Management Programme

Cyber Risk Management Programme	Frequency	%
Business Continuity Plan	46	55.4
Emergency Plan	37	44.6
Crisis Management Plan	37	44.6
Risk Management	59	71.1
Disaster Recovery	1	1.3
Simulation	2	2.4
Others	14	16.9

### 7.6.1.7 Participation in Security Training

Data regarding involvement of the participants in cyber security training is shown in Table 7.14; 70 (84%) respondents have attended cyber security training, while 13(16%) have not attended any cyber security training.

**Table 7.14** Response on Cyber Security Training

Cyber Security Training	Frequency	%
YES	70	84
NO	13	16
Total	83	100

### 7.6.1.8 Participants with Security Certification

Responses on security certification that the participants had obtained is shown in Table 7.15. Only 25 (30%) have security certification, while the rest (58;70%) have no security certification. Certifications are provided by Cyber Security Malaysia for those who attended their collaboration programs and training which cover Computer Emergency Response Teams (CERTs), Information Security Management Systems (ISMS), Business Continuity Management (BCM), Wireless Technology, Penetration Testing, SCADA, and Digital Forensics

**Table 7.15** Response on Security Certification

Security Certification	Frequency	%
YES	25	30
NO	58	70
Total	83	100

## 7.6.2 Data on Cyber Exercise

### 7.6.2.1 Response on Level of Cyber Exercise

Data on cyber exercises experience was collected from respondents and categorised by level and type. In cyber exercise levels, as demonstrated in Table 7.16, 55% have cyber exercise experience at a national level, 28% have experience at an organisation level, 16% have experience at training level, and 1% have experience at the state level. None of the respondents have experienced any cyber exercises at the regional or international levels.

**Table 7.16** Response on Cyber Exercise Involvement by Cyber Exercise Levels

Level of Cyber Exercise	%
Organisation	28
Regional	0
State	1
National	55
International	0
Training	10

### 7.6.2.2 Response on Types of Cyber Exercise

In terms of cyber exercise types, Figure 7.2 shows that 65% of participants have experience with simulation cyber exercises, 34% of participants have attended seminars, 16% of participants have attended workshops, 9% of participants have attended conferences, 1% of participants have attended other types of cyber exercises, and 1% of participants have attended table-top cyber exercises.

## 7.7 A Reliability Test on C-Suite Executive Survey

This section focuses on validating the C-Suite Executive checklist survey items using a Cronbach's alpha reliability test to check the internal consistency of the items that will be used as tools to assess OCR. As emphasised in [Cro51], summated scales are often used in survey tools to inquire about underlying constructs that need to be measured. The tool contains a set of indexed responses, which are later summed to arrive at a subsequent score associated with a particular respondent [Pal13]. Usually, the development of such scales is not the only aim of the research but rather is a means to collect predictor variables to be used in an objective model [Cro51]. However, the question of reliability increases as the function of scales

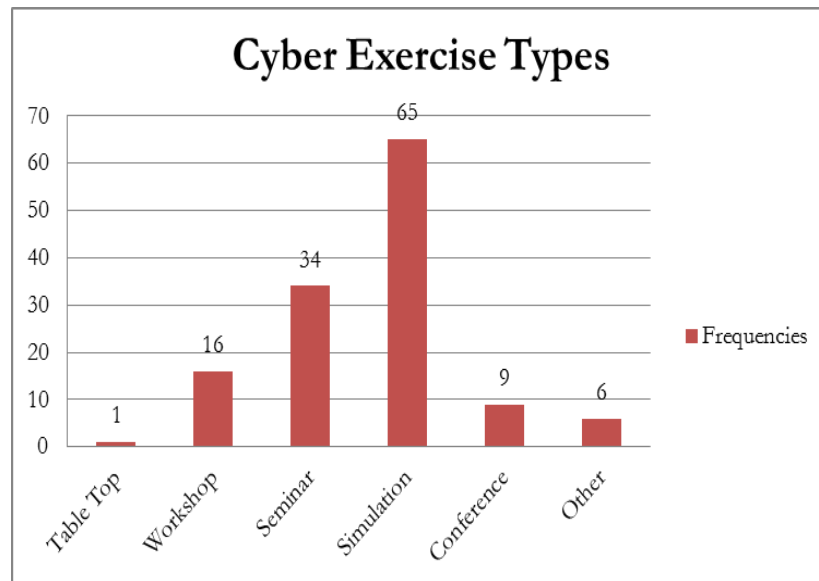


Figure 7.2: Response on Cyber Exercises Attended by Cyber Exercise Type

is strained to include prediction [Cro51]. One of the most popular reliability statistics used today is Cronbach's alpha [San99].

### 7.7.1 Cronbach's Alpha On C-Suite Executive Checklist Items

According to [San99] the OCR items in the C-Suite Executive checklist survey has good internal consistency if the Cronbach's alpha coefficient is more than 0.7. In this study, the reliability test was satisfied by Cronbach's alpha coefficient values of 0.974 and 0.975, as described in Table 7.17.

**Table 7.17** Cronbach's Alpha Analysis

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of items
0.974	0.976	19
0.975	0.977	17

All items achieved a corrected item-total correlation ranging from 0.682 to 0.906. As suggested by [San99], items that have a score less than 0.7 indicates that the items are measuring something different from the scale as a whole [Cro51]. As in Table 7.18, items PRG5 and PRG8 showed corrected item-total of 0.682 and 0.689, respectively, which are below 0.7. Removing the items from the set showed a small difference in score of 0.001(0.975-0.974), as shown in Table 7.18, with minimal effect. For this reason, both items will not be removed from the original set.



**Table 7.18** Item Total Statistics for C-suite Executive Checklist Survey

Item Code	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach Alpha if Item Deleted
GV1	69.5	256.4	0.865	0.972
GV2	69.5	252.45	0.870	0.972
GV3	69.9	250.91	0.778	0.973
GV4	69.6	253.68	0.846	0.972
GV5	69.6	252.54	0.888	0.972
GV6	69.8	254.11	0.807	0.973
GV7	69.5	257.33	0.823	0.973
GV8	69.5	252.06	0.906	0.972
PRG1	69.98	250.98	0.721	0.974
PRG2	69.94	250.98	0.767	0.973
PRG3	69.47	256.50	0.824	0.973
PRG4	69.53	252.64	0.897	0.972
<b>PRG5</b>	69.93	256.56	<b>0.682</b>	0.974
PRG6	69.73	253.72	0.905	0.972
PRG7	69.96	253.13	0.721	0.974
<b>PRG8</b>	69.96	253.91	<b>0.689</b>	0.974
NTW1	69.59	253.81	0.853	0.972
NTW2	69.63	256.60	0.811	0.973
NTW3	69.65	252.96	0.817	0.972

## 7.8 Pearson Correlation Test on Organisation Cyber Resilience Components

The Pearsons product moment coefficient of correlation is one of the best-known measures of association. It is a statistical value ranging from -1.0 to +1.0 to express the relationship in quantitative form [Pal13]. The coefficient is represented by the symbol  $r$ . The Pearson correlation test was conducted to determine the relationship between OCR variables of: governance (AvgGV), programme (AvgPRG), and network (AvgNTW). Table 7.19 shows the descriptive analysis of the three main components in the C-Suite Executive survey: governance, programme, and network.

**Table 7.19** Mean and Standard Deviation of OCR, AvgGV, AvgPRG, and AvgNTW

	Mean	Standard Deviation
OCR	3.88	0.88
AvgGV	3.96	0.92
AvgPRG	3.75	0.96
AvgNTW	3.94	0.96

Table 7.20 and correlation scatterplots in Figure 7.3 show the high positive correlation between AvgGV and OCR with  $r=0.97$ , AvgPRG and OCR with  $r=0.93$  and AvgNTW with OCR with  $r=0.90$ . This indicates that the increment of governance, programme, and network factors will strongly influence the OCR.

**Table 7.20** Pearson Correlation Results of OCR with of AvgGV, AvgPRG, and AvgNTW

OCR	AvgGV	AvgPRG	AvgNTW
Pearson Correlation ( $r$ )	0.965**	0.931**	0.895**
Sig.(2-tailed)	0.000	0.000	0.000
N	83	83	83

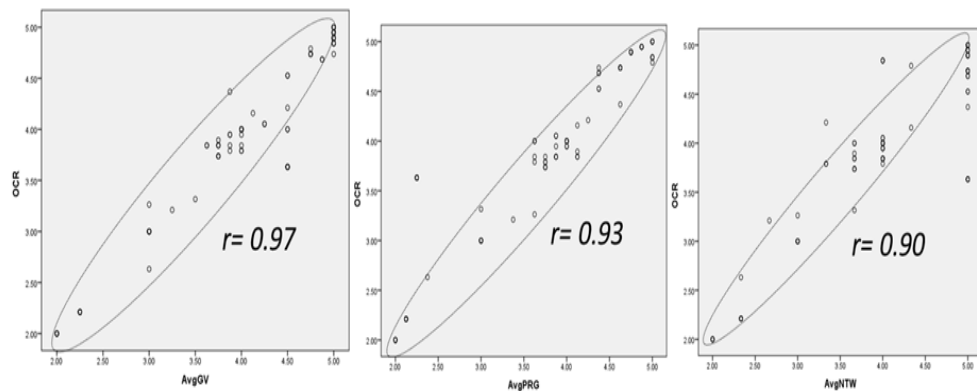


Figure 7.3: Correlation Scatterplots of AvgGV, AvgPRG, AvgNTW with OCR

## 7.9 Significant Study on Organisation Cyber Resilience of Ten CNII Sectors

Further investigations was conducted to test the differences of OCR perceptions for multiple sectors involved in the cyber exercise. A one-way between-group analysis of variance was conducted on OCR perceptions of the 10 CNII sectors to explore the hypothesis stated as following:

Hypothesis:

*H<sub>0</sub>: There is no statistically significant difference in OCR perceptions between CNII sectors that participated in the cyber crisis exercise.*

*H<sub>a</sub>: There is a statistically significant difference in OCR perceptions between CNII sectors that participated in the cyber crisis exercise.*

### 7.9.1 Data Analysis on Organisation Cyber Resilience (OCR)

As shown in Table 7.21, the OCR perceptions for the 10 CNII sectors is between 2.80 to 4.64. The OCR scores for the 10 CNII sectors were quite small except the slight deviation in the health service, the emergency service, and food and agriculture sectors from 0.88 to 0.94.

**Table 7.21** Descriptive Analysis of 10 CNII Sectors

CNII Sectors	N	Mean	%	Standard Deviation
National Defence and Security	8	4.06	81.2	0.61
Energy	6	4.51	90.2	0.55
Banking and Finance	12	4.64	92.8	0.36
Information and Communication	13	4.49	89.8	0.47
Transportation	10	3.32	66.4	0.53
Water	6	2.80	56	0.77
Health Services	6	3.15	63	0.88
Government	8	4.22	84.4	0.44
Emergency Services	5	3.12	62.4	0.94
Food and Agriculture	9	3.26	65.2	0.91
Total	83			

### 7.9.2 Results of A One-Way ANOVA Test

The one way between-group analysis of variance results showed that there were statistically significant differences in OCR perceptions between the 10 CNII sectors at the  $p < 0.05$  level as in Table 7.22. Multiple comparison between sectors are shown in Appendix G. The Post Hoc test results showed how one sector was difference from the other sector.

**Table 7.22** OCR One-Way ANOVA Results

Organisation Cyber Resilience					
10 CNII Sectors	Sum of Square	df	Mean Square	F	Sig
Between Groups	35.1	9	0.004	9.78	0.00
Within Groups	29.1	73			

## 7.10 Organisation Cyber Resilience Maturity Model

This section provides the OCR maturity model of the 10 CNII sectors based on their OCR perceptions. The OCR maturity model, developed by the World Economic Forum, suggested five stages of OCR maturity based on Table 7.23 : unaware for OCR scores between 0% to 20%, fragmented for OCR scores between 21% to 40%, top down for OCR scores between 41% to 60% , pervasive for OCR scores between 61% to 80% and networked for OCR scores between 81% to 100%.

**Table 7.23** Organisation Cyber Resilience Maturity Stages

OCR Stages and Stage Description
Stage 1: Unaware (0% - 20%)
The organisation sees cyber risks as largely irrelevant, and cyber risk does not form part of the organisations risk management processes. The organisation is not aware of its level of interconnectedness.
Stage 2 : Fragmented (21% - 40%)
The organisation recognises hyperconnectivity as a potential source of risk and has limited insight into its cyber risk management practices. The organisation has a silo approach to cyber risk, with fragmented or incident reporting.
Stage 3 : Top Down (41% - 60%)
The Chief Executive Officer has set the tone for cyber risk management, has initiated a top-down threat-risk-response programme but does not view cyber risk management as a competitive advantage.
Stage 4 : Pervasive (61% - 80%)
The organisations leadership takes full ownership of cyber risk management, has developed policies and frameworks, and has defined responsibilities and reporting mechanisms. It understands the organisations vulnerabilities, controls and interdependencies with third parties.
Stage 5: Networked (81% - 100%)
Organisations are highly connected to their peers and partners, sharing information and jointly mitigating cyber risk as part of their day-to-day operations. Its people show exceptional cyber awareness and the organisation is an industry leader in managing cyber risk management.

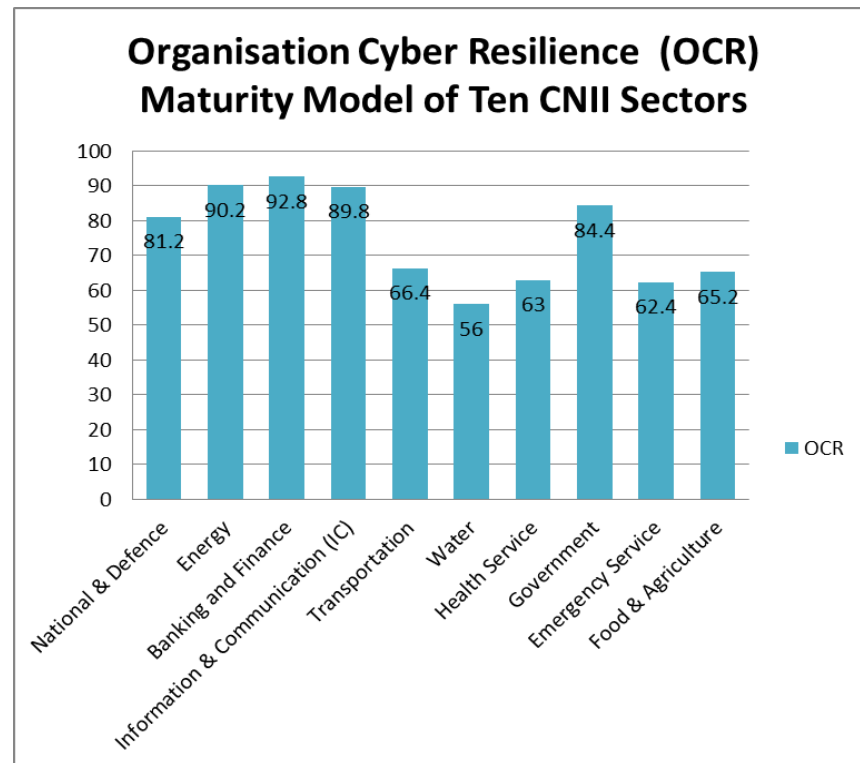


Figure 7.4: Organisation Cyber Resilience Maturity Model of the 10 CNII Sectors

The OCR maturity model results, as depicted in Figure 7.4, show that five sectors have the highest OCR score of 5 (Networked): energy, banking and finance, information & communication, the government and national defence and security sectors. The transportation, water, health services, food and agriculture, and emergency service sectors were in Stage 3 (Top Down). According to the maturity stage description, organisation at Stage 5 (Networked) are highly connected to their peers and partners. They are sharing information and jointly mitigating cyber risk as part of their day-to-day operations. Its people show exceptional cyber awareness, and the organization is an industry leader in managing cyber risk. Organisations at Stage 4 (Pervasive) have leadership that takes full ownership of cyber risk management, have developed policies and frameworks, and have defined responsibilities and reporting mechanisms. Leadership understands the organisations vulnerabilities, controls, and interdependencies with third parties. Finally, in organisations at Stage 3 (Top Down), the chief executive officer has set the tone for cyber risk management, and has initiated a top-down threat-risk-response programme, but does not view cyber risk management as a competitive advantage.

## 7.11 Result Discussion

The Cronbach's alpha test was conducted on 19 items of the C-Suite Executive checklist survey and showed a good internal consistency of 0.974. Moreover, the Pearson correlation test on OCR components showed a very high positive relationship between OCR with governance, programme, and network components. The Pearson coefficient values range from 0.90 to 0.97. This suggests that the increment of these components will increase the OCR of the participating sectors. This also indicated the appropriateness of the C-Suite Executive checklist survey to assess OCR of ten CNII sectors. The one-Way ANOVA test was conducted to compare OCR among participating CNII sectors and showed a statistically significant difference between sectors. Furthermore, the OCR maturity model for the 10 CNII sectors, developed based on their individual OCR scores, showed differences in OCR maturity stages in the 10 CNII sectors. Results of the study provides evidence of suitability of the C-Suite Executive checklist survey to assess OCR. This support the use of C-Suite Executive checklist survey as second component to assess organisation in the proposed framework.

## 7.12 Chapter Contribution

This chapter highlights three contributions of the study:

1. An assessment of the second component of the Post Assessment Framework for Collaborative Cyber Exercises, the OCR.
2. A validation on the reliability of the C-Suite Executive checklist survey to assess OCR.
3. The development of a sector OCR maturity model using OCR scores.

## 7.13 Summary

This chapter provides an investigation of OCR as the second component of the post assessment framework for collaborative cyber exercise. The assessment involved three tests, the reliability and Pearson correlation tests on the C-Suite Executive checklist survey and the OCR significant test of the 10 CNII sectors. The OCR scores were used to developed the maturity model of OCR of the 10 CNII sectors.

## Chapter 8

# Conclusion and Future Work

### 8.1 Conclusion

This research investigated the potential impact of cyber exercises on participants and their organisations. The study used a cyber exercise post assessment framework to answer five research questions. Research questions were answered through a literature review and several empirical studies.

#### 8.1.1 Findings to the Research Question 1

The first research question (RQ1) was 'what are focuses of cyber exercises research?' The question was answered in Chapter 2 as a result of a literature review. The study contributed to a general overview of cyber exercise research across three categories of academic, competitive, and collaborative cyber exercises:

The results revealed that academic cyber exercises mainly focus on individual skills and knowledge development in the information security domain. Academic cyber exercises involve curriculum design for teaching and learning and assessment of students involved in information security courses at universities, colleges, and in the training industry. The four main skills needed for information security are system administration, defensive, offensive, and forensic skills.

Competitive cyber exercises provide a platform to test participants knowledge and skills. The focus on teamwork and collaborative decision making contributes to a winning performance. Previous research covers two types of competitions: collegiate cyber defence competitions (CDCC) and capture the flag exercises that assess student skills and knowledge at school, college, and universities at national and international levels. Both academic and competitive

cyber exercises share a structure, including the process of organising the exercise, the environment setting, and the software to automate the management and assess the exercises.

Research in crisis cyber exercises involved multi sectors provides a platform to test cyber-crisis operations involving various organisations at state, national, and international levels. The cyber exercise supports cyber security strategy implementation as part of public-private cooperation in cyber security strategy and CII protection. Collaborative cyber exercises use scenarios that help organisations understand the effect of cyber incidents on their services, to coordinate the response to cyber crises, to share information on the latest cyber threats through effective communication, and to collaborate efforts in handling a cyber crisis at organisation, national, and international levels.

### 8.1.2 Findings to the Research Question 2

The second research question (RQ2) was 'how do cyber exercises contribute to critical information infrastructure protection? This question was answered in Chapter 3. It highlighted the contribution of cyber exercises to CIIP through joint collaborative exercises between public and private CII organisations across sectors and borders. Cyber exercises contribute to cooperation among collaborators in computer emergency response teams, increase awareness on interdependencies, sharing information on cyber threats, and mitigation efforts.

### 8.1.3 Findings to the Research Question 3

The third research question (RQ3) was 'how can cyber exercise be beneficial to participants and their organisations?' This was answered in Chapter 4. This chapter contributes to the development of a post assessment framework for cyber exercise that consists of two parts: the participants and the organisations assessment. The first part on participants assessment adopted the four Kirkpatrick training levels that evaluate the effect of collaborative cyber exercises on their reactions, learning, behaviour, and results.

The reaction level considers participants perceptions in terms of the exercise objectives, the participants experience with the scenarios used in the exercise, the environment setting that simulates the cyber operations, and the participants expectations throughout the exercise, The learning level assesses how new knowledge and skills are developed during the exercise, increasing participants cyber operation analysis capabilities on cyber-attacks. At the behaviour level, the actions and innovations show how participants responded to cyber threats after the exercise. The improvements of cyber analysis capabilities and cyber defence actions provide evidence of the effect of a cyber exercise.



The second part of the framework proposed two resilience tools to assess organisation's resilience; the organisation resilience benchmark tool of BRT-53 and C-Suite Executive checklist: The first tool, the BRT-53 developed by University of Canterbury in New Zealand use to assess behaviour and perceptions that linked to the organisation's ability to plan for, respond to, and recover from emergencies and crises. The tools provides three dimensions of situation awareness (SA), management of keystone vulnerabilities (KV) and adaptive capacity (AC). Every dimensions have five indicators that contribute to organisation resilience. The second tool, the C-Suite Executive checklist developed by the World Economic Forum. The tool provides perceptions on: recognition of interdependencies, executive level awareness of cyber risk management, and suppliers and customers awareness and commitments to cyber risks. This tool consists of three main components of governance, programme and network.

#### 8.1.4 Findings to the Research Question 4

The fourth research question (RQ4) was 'what are the impacts of collaborative cyber exercises to participants and their organisations?' This question was answered in Chapter 5. Findings were presented from post assessment interviews conducted with collaborative cyber exercise participants from the X-Maya 5 in Malaysia. Interview data was coded and categorised according to the four-level Kirkpatrick training model. At level one, participants reactions involved their perceptions of the objective of the exercise, the scenario, the environment, and their expectations towards the exercise. The study showed that participants had positive reactions to the X-Maya exercise.

At level one, most of the participants agreed on the X-Maya objectives 1) to develop communications during a cyber crisis, 2) to offer a knowledge-sharing platform in solving incidents between agencies, and 3) to assess the effectiveness of action, communication, and national security coordination in dealing with existing cyber crises. At level two, most participants agreed that they developed new technical skills during the exercise, especially skills relating to cyber incident handling of 1) knowledge to determine cyber threats according to national cyber threats levels, 2) how to address incidents, and 3) how to coordinate incident response through communication between agencies. At level three, participants improved their situation awareness, including 1) increment in network monitoring activities and 2) more enthusiasm in safeguarding their working environments. At the results stage, 1) revision of their organisations cyber incident response procedures and policies and 2) new directions to national cyber incident response policies and procedures occurred. Sector leaders were identified to coordinate cyber incident reporting.

### 8.1.5 Findings to the Research Question 5

The last research question (RQ5) was 'how to assess organisation cyber resilience of CNII sectors involved in collaborative cyber exercises?' This question was answered in Chapters 6 and 7. Two studies were designed to assess organisational resilience and organisational cyber resilience of CII sectors involved with collaborative cyber exercises. A preliminary study conducted in Chapter 6 was designed to determine the suitability of the organisational resilience tool, the BRT-53, used to assess organisational resilience of organisations in CII sectors involved in scenario-based cyber exercises. The tool has three main dimensions: situation awareness, management of keystone vulnerabilities, and adaptive capacity. The study involved participants from information security in several critical infrastructure organisations in six LinkedIn groups.

Several correlation tests were conducted. One correlation test was conducted to discover relationships between OR and SBE experiences. Other investigations were conducted on correlations between SBE experiences with OR dimensions and the indicators: AC, KV, and SA. Correlation test results indicate that there was not enough evidence to support the relationship between SBE experiences and OR perspectives, including the OR dimensions, except for a weak relationship between SBE experiences with SA. A one-way ANOVA test of ORs significant difference between groups with SBE experiences and without SBE experiences showed no differences between them. As a result of the preliminary study, due to the limited evidence to support the relationship of SBE with OR, the BRT-53 tool was excluded from the proposed post assessment framework.

In Chapter 7, the C-Suite Executive checklist was used to collect data from participants in the X-Maya exercise. This survey has three main components: governance, programme, and network. Several studies were conducted on the tool before it was used to assess the OCR and to develop the OCR maturity model. First, a reliability test was conducted on the C-Suite Executive checklist survey. Results showed a good internal consistency of 0.974. Second, the Pearson correlation test on OCR components showed a very high positive relationship between OCR with the governance, programme, and network components. This indicated the appropriateness of the C-Suite Executive checklist survey to assess OCR across 10 CNII sectors. Third, a one-Way ANOVA test was conducted to compare OCR among participating CNII sectors and showed a statistically significant difference between CNII sectors. Lastly, the OCR maturity model for the 10 CNII sectors based on their individual OCR scores showed differences in OCR maturity across the 10 CNII sectors in the X-Maya 5 exercise

## 8.2 Research Limitations

This study faced several limitations, which influenced the research design, data collection, data analysis, and research objectives.

*Differences of scope and objectives of collaborative cyber exercises.* It was difficult to use the collaborative post assessment framework to compare the effect of cyber exercises between countries since every country has their own cyber security context priority, scope, mission, and strategy as presented in Chapter 3. For this reason, Malaysia National collaborative cyber exercise X Maya was chosen for this research instead of a comparison between countries.

*Interview data analysis.* Codes were specifically generated based on the interview data. Because every cyber exercise has its own scope, objective, and setting, especially at the learning stage, code generated in terms of new skills and knowledge for one cyber exercise will not be the same for other exercises.

*Limitation of control on online surveys.* Online surveys were used in the OCR investigation because the researcher lacked direct access to other participants. We could not conducted detail checks through the participating agencies. Emails were sent through the Sector Leader only, we have no control if qualified participants actually participating in the survey.

*Limitation to access specific participants.* Investigation concerning OR used a sample from the LinkedIn social network. The difficulty using this sampling technique was to reach specific participants with cyber exercise experience. The participants' involvement in cyber exercises varies across the level and type of cyber exercises.

*Limitation using available survey.* This study use BRT-53 developed by University of Canterbury, New Zealand. This version has too many questions as commented by survey participants. The short version was produced by the institution later after this study completed. This new version will use in future study for a comparison.

*Limitation of online survey to trace user participation.* Another limitation of using LinkedIn is the participants profile can be checked during the invitation to answer the survey but not from survey data. The survey was developed using a survey monkey tool. The survey data only have the IP address of the participant which difficult to trace who was answering the survey.

*Government Staff Mentality and Perception.* In Malaysia most of public sectors like health, nuclear and transport are belong to government. Even though they are belong to any CII sectors, some participants are tending to select government sector rather than their own sector. This is a reason in most of the survey, the government sector has more respondents compared to other sectors.

## 8.3 Significant Contributions

The significant contributions of this research were mentioned in Section 1.7 of the introductory chapter, and we can also summarise contributions from each chapter as follows:

1. Contributions to knowledge relating to collaborative cyber exercises and interview data analysis.
  - Chapter 2 contributes findings on cyber exercise comparisons and research directions across academic, competitive, and collaborative cyber exercises.
  - Chapter 3 contributes findings on collaborative cyber exercises to critical information infrastructure protection.
  - Chapter 5 contributes to interview data analysis using a collaborative cyber exercise post assessment framework. The interview data analysis involved six phases of audio transcription, translation, text cleaning, code development, data categorisation, and result presentation. For the inter-rater reliability results on categorised items showed the Kappa agreement for the two research assistants (RAs) have achieved almost perfect categorisation on the list of text, according to the code themes.
2. Chapter 4 contributes to the development of a collaborative cyber exercise post assessment framework: This framework consists of two parts. The first part adopts the Kirkpatrick training model to evaluate how participants benefit from collaborative cyber exercises in four stages: reactions, learning, behaviour, and results. The second part assesses organisational cyber resilience for organisations participating in cyber exercises.
3. Chapter 7 contributions include:
  - Reliability test on the C-Suite Executive survey. The study validated the internal consistency of the C-Suite Executive survey. The reliability results showed a very high internal consistency of Cronbachs alpha values of 0.976, which supports the use of this survey for organisational cyber resilience assessment.
  - Organisational cyber resilience assessment and OCR maturity model development for 10 CNII critical sectors. This work provides an assessment of organisational cyber resilience for 10 CII sectors and developed an organisational cyber resilience maturity model for 10 CNII sectors that participated in X-Maya exercises.

- Chapter 6 provided evidence that the organisational resilience BRT-53 survey tool was not suitable to assess organisational resilience based on a limited convenience sample. The results of the study showed no correlation between organisational resilience with scenario-based experience. The ANOVA significance test showed no difference in organisational resilience between organisations with scenario-based experience and without scenario-based experience.

## 8.4 Future Works

This study can be enhanced for future work:

- *A post assessment metrics.* Future studies will focus on developing participants post assessment metrics for the four levels. New study will be designed to gather more collaborative outcomes of participants knowledge, skills and behaviour from other collaborative cyber exercises to identified the components of the metrics. These metrics can be used to objectively evaluate and compare the implications of participants post assessment from 10 CNII sectors for the next X-Maya exercise.
- *Correlation between OCR with Collaborative Cyber Exercise.* To investigate a correlation between X-Maya experience with organisational cyber resilience, a new study could be designed to involve CNII organisations with X-Maya experience and without X-Maya experience.
- *Correlation between Public and Private with Collaborative Cyber Exercise.* To investigate a correlation between X-Maya experience with organisational cyber resilience, a new study could be designed to involve public and private organisations with and without cyber exercises experiences.
- *Enhance the OCR tool.* For a holistic organisational cyber resilience assessment, the current cyber resilience survey could be enhanced to include items that evaluate technical, process, and operational resiliency.

## 8.5 Significant Usage of the Collaborative Cyber Exercise Post Assessment Framework

The collaborative cyber exercise post assessment framework developed in this research provides two important assessment components of participants and organisations that can be used as a whole or separately:

*Participant Assessment Component.* This component can be applied to assess investments in security personnel development. It serves as an important tool for human resource managers or senior managers to assess the benefits of security training. The performance of the trainee can be assessed by their reaction, learning, behaviours, and results in their organisations. The outcome of any training or exercise activities can be measured for performance evaluation and individual development.

*Organisation Assessment Component.* The OCR survey can also be used to assess OCR of CNII organisations that participated in cyber exercises, even non CNII organisations. The maturity model of OCR in these organisations could be developed using the survey. The OCR components of the OCR survey can also be used to independently investigate governance programmes and network perceptions of these organisations.

*Usage in Other Domain of Crisis Management.* This framework can be applied for any type of crisis exercise such as natural disaster, technical problem or man-made disasters. It can be used to collect the impact of these exercises on participants reactions, learning, behaviour and results.

# Appendix A

## Permission Application for C-Suite Executive Survey



Arniyati Ahmad <arniyati@gmail.com>

---

### C Suite Executive Checklist

3 messages

Arniyati Ahmad <arniyati@gmail.com>  
 To: derek.ohalloran@weforum.org  
 Cc: alex.deleeuw@weforum.org, elena.kvochko@weforum.org

Thu, Jan 23, 2014 at 2:10 PM

Dear Derek,

My name is Arniyati Ahmad, I am currently doing my postgraduate study in University of Glasgow, UK. My research area is in Cyber Security which focusing on Critical Infrastructure Protection. Currently I am gathering information on Cyber Resilience and I have just found that C Suite Executive Checklist in Partnering for Cyber Resilience white paper. As it mentioned that it can be used to check on Cyber Resilience, I would like to request for a permission to use this tool in my research.

If it is permissible, I will collect some data using this tools from critical infrastructure organisation in my country (Malaysia).

I am looking forward to hear from you.

regards,  
 Arniyati  
 Department of Computing Science  
 University of Glasgow  
 UK

---

Derek O'Halloran <Derek.OHalloran@weforum.org>  
 To: Arniyati Ahmad <arniyati@gmail.com>  
 Cc: "alex.deleeuw@weforum.org" <alex.deleeuw@weforum.org>, Elena Kvochko <Elena.Kvochko@weforum.org>

Tue, Feb 4, 2014 at 5:29 PM

Dear Arniyati,

Apologies for the delay – we just completed our Annual Meeting in Davos and was on vacation last week.

Yes, feel free to use the tool. The document has been published under a Creative Commons license 3.0, so you are free to use with attribution, just not for commercial gain.

Many thanks for your interest. We'd be interested to see the outcome of your research.

Best,  
 Derek

# Appendix B

## Permission Application for Organisation Resilience Survey

Gmail - Permission to use the Resilience Benchmark Tool

<https://mail.google.com/mail/u/0/?ui=2&ik=76258e022c&view=pt&q...>



Arniyati Ahmad <arniyati@gmail.com>

### Permission to use the Resilience Benchmark Tool

8 messages

Arniyati Ahmad <arniyati@gmail.com>

Mon, Sep 9, 2013 at 2:34 PM

To: erica.seville@rsrc.co.nz, john.vargo@canterbury.ac.nz

Dear Dr Erica and Dr John,

My name is Arniyati Ahmad, currently pursuing my PhD in University of Glasgow, UK.  
My research will be focusing on the effectiveness of National Cyber Crisis Exercise in cultivating Resilience Culture in Critical Infrastructure Organisations.

I am currently look at several Organisational Resilience Benchmark Tool to study the organisation resilience culture.I found that your Benchmark tool is the most suitable to be used in the study.  
I would like to request for a permission to use the tool in Malaysia environment.

I am really need you permission on this.

Thank you.

regards,  
Arniyati

John Vargo <john.vargo@canterbury.ac.nz>

Tue, Sep 10, 2013 at 2:15 AM

To: Arniyati Ahmad <arniyati@gmail.com>

Cc: "erica.seville@rsrc.co.nz" <erica.seville@rsrc.co.nz>

Hi Arniyati,

Very nice to hear from you and your interest in using our resilience benchmark tool in your research. We would be happy to have you use the ResOrgs benchmark tool on the following provisos:

- That you suitably acknowledge Resilient Organisations in any publications
- That you make available to us an anonymised copy of the data from your research so we can add it to our growing database of results to assist in our ongoing research, and
- That you provide us with a copy of your final results/PhD thesis for us to post on our website (at our discretion)

Are you agreeable to those provisos?

Erica, are there any other issues that we need to raise with Arniati regarding this request?

Best regards,

John

John Vargo, co-leader  
Resilient Organisations Research Programme  
University of Canterbury  
Private Bag 4800  
Christchurch  
P +643 364 2627  
M +6421 442 091

[Quoted text hidden]

This email may be confidential and subject to legal privilege, it may not reflect the views of the University of Canterbury, and it is not guaranteed to be virus free. If you are not an intended recipient,



## **Appendix C**

### **Interview Consent Form**

## **The Effectiveness of Cyber Exercise in Contributing Cyber Security to Organisation**

I want to thank you for taking the time to meet with me today.

My name is Arniyati Ahmad and I would like to talk to you about your experiences participating in the X Maya 5 exercise in November 2013. The objectives of this interview are to assess the effectiveness of cyber exercise in providing new knowledge on cyber threats and new cyber defence skills. It also to see how these knowledge and skills transferred to participants' organisation.

The interview should take less than an hour. The session will be taping because I don't want to miss any of your comments. Although I will be taking some notes during the session, I can't possibly write fast enough to get it all down. Because we're on tape, please be sure to speak up so that we don't miss your comments.

All responses will be kept confidential. This means that your interview responses will only be accessed by the researcher and I will ensure that any information include in my report does not identify you as the respondent.

Remember, you don't have to talk about anything you don't want to and you may end the interview at any time.

Are there any questions about what I have just explained?

Are you willing to participate in this interview?

---

Interviewee

---

Witness

---

Date

## **Interview Questions**

1. When do you start get involved with Cyber Exercise?
2. How many times have you involved with cyber exercise including X Maya?
3. What was the scenario used in X Maya 5 exercise? Was it easy to understand?
4. What have you learnt from X Maya 5 exercise and other cyber exercises that you have involved?
5. In your opinion, how X Maya 5 exercise has improved your situation assessment on cyber threats in your working environment?
6. How X Maya 5 help you to contribute to cyber security in your organisation?
7. Did you revise on standard, policy and guidelines after attending the X Maya exercise?
8. Is there any improvement on standard, policy and guidelines that you have proposed after attending the X Maya exercise?
9. Do you think the scenario and infrastructure used in X Maya can easily be implemented in your organisation?
10. Do you plan to run your own cyber exercise in your organisation?

Is there anything more you would like to add?

I will be analysing the information that you and others have provided and writing a report. If you are interested, I will send you a copy of the report.

Thank you for your time and your cooperation are really appreciated.

## Appendix D

### Sample of Interview Coding Script

Table D.1: Sample of Interview Coding Script

Begin of Audio Coding Text	
Interview Questions	Interviewee Answers
When do you start get involved with Cyber Exercise?	2010,2012, 2013
How many times have you involved with cyber exercise including X Maya?	3 times X maya 1, X maya 3 and X maya 5 2013
Would you like to share your experience in X Maya in terms of its objectives, the scenario, setting environment and scenario? What was the scenario used in X Maya 5 exercise? Do you think it was easy to understand?	[RE: SC ]The attack scenario created a little bit confuse to all the participants. [RE: SC ]Each scenario different. Scenario have multiple attacks of web, file, network and server (apache). [RE: SC ] Different attacks launch to different agencies. No similar attack launched between agencies at the same time.
What have you learnt from X Maya 5 exercise and other cyber exercises that you have involved?	[LE:SK ]If incident happened, we know how to establish the communication and sharing the knowledge between agencies in handling the issues. [LE:SK] We learnt how to handle incident and knowledge sharing.
How X Maya 5 help you to contribute to cyber security in your organisation?	[RS:REV PS] By check the existing procedure of incidents handling. [RS:REV PS] Improved the existing procedure.
<i>(Continue to the next Page)</i>	

Continuation of Table D.1	
Interview Questions	Interviewee Answers
Did you revise the existing security standard, policy and guidelines after attending the X Maya exercise?	[LE:PO ]National threat levels. Low, moderate, high, crucial. General rules. [LE:PO ]During crisis organisation have to define crisis stages and business must operates as usual even under low resources.
Is there any improvement on standard, policy and guidelines that you have proposed after attending the X Maya exercise?	[RS: NEW PS] sector need to update the NC4. NC4 belong to MKN. [RS:NEW PS ]Direction by NC4 will be channel to the lead sector and they will escalate the direction to the agencies.
Do you think the scenario and infrastructure used in X Maya can be implemented in your organisation?	[RE: SC ] The cyber exercise scenario can easily be implemented in the organization. Only the way to fix the vulnerabilities a bit difficult. [RE:ENV]Run on VM with VPN. Using VM copied in thumb drive and run in isolated area through the cloud.
Do you plan to run your own cyber exercise in your organisation?	No. [RS:LIMIT ] Not enough capability and competency of people to run the exercise.
End of Table	

## **Appendix E**

### **A Pilot Test Survey on C-Suite Executive Checklist**

# Pilot Test on Organisation Cyber Resilience Survey

This survey is to gather feedback on the operationalization of the Organisation Cyber Resilience Survey

## 1. Under which sector does your organisation belong?

☐ National Defence & Security

☐ Energy

☐ Banking & Finance

☐ Information & Communication

☐ Transportation

☐ Water

☐ Health Services

☐ Government

☐ Emergency Service

☐ Food & Agriculture

Other (please specify)

## 2. Evaluation on the appropriateness of the language used for every question

	Poor	Fair	Good	Very Good	Excellent
The language use for Governance questions	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The language use for Programme questions	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The language use for Network	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

## 3. Evaluation on number of questions for each components of the survey

	Poor	Fair	Good	Very Good	Excellent
Number of questions for Governance components	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Number of questions for Programme components	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Number of questions for Network components	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

**4. Evaluation on the content of all components in the survey**

	Poor	Fair	Good	Very Good	Excellent
What is your rate for the content of Governance questions	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
What is your rate for the content of Programme questions	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
What is your rate for the content of Network questions	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

**5. Evaluation on the confidentiality on the content of the survey**

	Poor	Fair	Good	Very Good	Excellent
Confidentiality on Governance questions	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Confidentiality on Programme questions	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Confidentiality on Network questions	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>



## **Appendix F**

### **Online Organisation Cyber Resilience Survey**

## Survey on Organisation Cyber Resilience

### INTRODUCTION

The openness of internet connection has provided a border less cyberspace that invited many threats to an organisation. Any vulnerability in the organisation system will lead to cyber attack. It is highly important to cultivate cyber resilience for the organisation that provides critical services to a community. Cyber resilience can be defined as a cyber-system's ability to function properly and securely regardless of any disruptions to the system. The disruptions can be caused by cyber or physical, intentionally or by accidental, or random.

### OBJECTIVE

The objective of this study is to investigate the correlation of Cyber Crisis Exercise experience with Organisation Cyber Resilience of critical infrastructure organisations. The cyber resilience tool is created by the World Economic Forum in 2011.

### REFERENCES

Partnering for Cyber Resilience, World Economic Forum, 2012.

[http://www3.weforum.org/docs/WEF\\_IT\\_PathwaysToGlobalCyberResilience\\_Report\\_2012.pdf](http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf)

### CONFIDENTIALITY

The information of this study including participant's response data will be kept confidential and can only be accessed by this research conductor. No reference will be made in any report, which may link the participants to the study.

### CONTACT:

If you have questions about the study, please contact:

Mrs Arniyati Ahmad, at Email: [a.ahmad.1@research.gla.ac.uk](mailto:a.ahmad.1@research.gla.ac.uk),

Prof Chris Johnson, at Email: [Christopher.Johnson@glasgow.ac.uk](mailto:Christopher.Johnson@glasgow.ac.uk),

School of Computing Science, University of Glasgow

Participation in this survey is entirely voluntary, meaning that you can withdraw at any time. However, we would be very grateful if you could attempt to answer all questions. All responses are anonymous.

**BY CLICKING NEXT YOU ARE AGREEING TO PARTICIPATE IN THIS SURVEY**

Thank you for participating in this survey.

Background Information

---

\* 1. In which country do you work?

Country

Other (please specify)

2. Under which category does your organisation belong?

☐ Public

☐ Private

\* 3. Under which sector does your organisation belong?

☐ National Defence & Security

☐ Transportation

☐ Emergency Service

☐ Energy

☐ Water

☐ Food & Agriculture

☐ Banking & Finance

☐ Health Services

☐ Other

☐ Information & Communication

☐ Government

Other (please specify)

\* 4. Number of employee in your organisation

☐ <10 ☐ 10-49 ☐ 50-249 ☐ 250-499 ☐ >500

\* 5. How long have you worked in your industry? (please tick one):

☐ Less than 1 year ☐ 1-3 years ☐ 4-10 years ☐ 11-20 years ☐ 21+ years

\* 6. How long have you worked at your organisation? (please tick one)

☐ Less than 1 year ☐ 1-3 years ☐ 4-10 years ☐ 11-20 years ☐ 21+ years

\* 7. Which role do you play in your organisation? (you can tick on more than one answer)

☐ Decision Maker ☐ Strategic Planner ☐ Policy Maker ☐ Technical Advisory ☐ Other

Other (please specify)

\* 8. Have you experienced Cyber incidents or cyber crisis in your organisation?

☐ Yes

☐ No

\* 9. Have you attended any Cyber Crisis Exercises in your organisation?

- ☐ Yes
- ☐ No
- ☐ Don't Know

\* 10. Have you attended any Cyber Crisis Exercises outside your organisation?

- ☐ Yes
- ☐ No
- ☐ Don't Know

\* 11. Which level of Cyber Crisis Exercises that you have attended?

- |                                       |                                   |                                        |
|---------------------------------------|-----------------------------------|----------------------------------------|
| <input type="checkbox"/> Training     | <input type="checkbox"/> Regional | <input type="checkbox"/> National      |
| <input type="checkbox"/> Organisation | <input type="checkbox"/> State    | <input type="checkbox"/> International |

Name of Cyber Crisis Exercise Attended:

\* 12. What type of Cyber Crisis Exercises have you experienced? (you can tick on more than one answer)

- |                                    |                                     |                                     |
|------------------------------------|-------------------------------------|-------------------------------------|
| <input type="checkbox"/> Table Top | <input type="checkbox"/> Seminar    | <input type="checkbox"/> Conference |
| <input type="checkbox"/> Workshop  | <input type="checkbox"/> Simulation | <input type="checkbox"/> Other      |

Other (please specify)

\* 13. Have you obtained any security certification?

- ☐ Yes
- ☐ No

\* 14. Have you attended any cyber security training?

- ☐ Yes
- ☐ No

\* 15. Is your organisation having any plan stated below? (tick all that apply)

☐ Business Continuity Plan ☐ Emergency Plan ☐ Crisis Management Plan ☐ Risk Management Plan

☐ Other

Other (please specify)

\* 16. Have you involved in the discussion of any plan stated below? (tick all that apply)

☐ Business Continuity Plan ☐ Emergency Plan ☐ Crisis Management Plan ☐ Risk Management Plan

☐ Other

Other (please specify)

## Governance

Please rate for each question in a scale of 1 to 5. If you are unable to answer the questions please choose 'Don't Know' Option.

1: Does not describe my organisation at all. 5: Accurately describes my organisation

\* 17. The chief executive and executive management team are responsible for overseeing the development and confirming the implementation of a Programme of best practices for cyber risk management

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ Don't Know

\* 18. The chief executive and executive management team ensure that the Programme is reviewed for effectiveness and, when shortcomings are identified, corrective action is pursued

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ Don't Know

\* 19. The chief executive and the executive management team demonstrate visible and active commitment to the implementation of the Principles

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ Don't Know

\* 20. Executives and managers are responsible for understanding at the appropriate level how cyber risks could impact and originate from their line of business

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ Don't Know

\* 21. Senior leadership understands who is responsible for managing cyber risk when managing security incidents

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ Don't Know

\* 22. The organization has access to cyber expertise at its highest management levels

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ Don't Know

\* 23. The organization undertakes to continuously improve the integration of its cyber risk management with its other risk management initiatives

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ Don't Know

\* 24. The chief executive (or equivalent) has a clear decision path for action and communication in response to a significant security failure or accident

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ Don't Know

### Programme

**Please rate for each question in a scale of 1 to 5. If you are unable to answer the questions please choose 'Don't Know' Option.**

**1: Does not describe my organisation at all. 5: Accurately describes my organisation**

\* 25. The organization conducts comprehensive assessments of its vulnerabilities to internal and external cyber risks appropriate for its industry and sector

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ Don't Know

\* 26. The organization monitors the effectiveness of its cyber risk management strategy

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ Don't Know

\* 27. The organization periodically internally verifies its compliance with rules and regulations

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ Don't Know

\* 28. The organization's commitment to the Programme is reflected in its policies and practices

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ Don't Know

\* 29. Managers, employees and agents receive specific training on the Programme, tailored to relevant needs and circumstances

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ Don't Know

\* 30. The organization has identified its data and information as vital assets, and organizes its Programme around the recognition that data and information have value that can be separately recognized and protected

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ Don't Know

\* 31. The risk management Programme includes all material third-party relationships and information flows

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ Don't Know

\* 32. The organization conducts comprehensive internal short- and long-term cyber risk impact assessments

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ Don't Know

## Network

**Please rate for each question in a scale of 1 to 5. If you are unable to answer the questions please choose 'Don't Know' Option.**

**1: Does not describe my organisation at all. 5: Accurately describes my organisation**

\* 33. The organization seeks to ensure that its suppliers and relevant third parties adhere to the organization's specific cyber risk management standards or industry best practices, in line with the Principles, and formalizes this requirement using contractual obligations

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ Don't Know

\* 34. The organization has built relationships with its peers and partners to jointly manage cyber risk and more effectively deal with cyber incidents

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ Don't Know

\* 35. The risk management Programme includes all material third-party relationships and information flows

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ Don't Know

36. Comments:

Thank you for your cooperation by filling up this survey, your participation is highly appreciated



## **Appendix G**

### **Post Hoc of Comparison Sectors Result**

Post hoc test results between the 10 CNII sectors

Comparison OCR Between Sectors		Mean Difference	Std. Error	Sig.	Hypothesis $p < 0.05$ <i>reject H0</i>
National Defence Security (Group 1)	Water	1.28728*	.34083	.011	<i>reject H0</i>
Energy (Group 2)	Transportation	1.18772*	.32590	.017	<i>reject H0</i>
	Water	1.71053*	.36437	.000	<i>reject H0</i>
	Health Services	1.35965*	.36437	.013	<i>reject H0</i>
	Emergency Service	1.39298*	.38215	.017	<i>reject H0</i>
	Food & Agriculture	1.24561*	.33262	.012	<i>reject H0</i>
Banking & Finance (Group 3)	Transportation	1.31930*	.27022	.000	<i>reject H0</i>
	Water	1.84211*	.31555	.000	<i>reject H0</i>
	Health Services	1.49123*	.31555	.000	<i>reject H0</i>
	Emergency Service	1.52456*	.33593	.001	<i>reject H0</i>
	Food & Agriculture	1.37719*	.27829	.000	<i>reject H0</i>
Information & Communication (Group 4)	Transportation	1.16478*	.26545	.001	<i>reject H0</i>
	Water	1.68758*	.31148	.000	<i>reject H0</i>
	Health Services	1.33671*	.31148	.002	<i>reject H0</i>
	Emergency Service	1.37004*	.33211	.004	<i>reject H0</i>
	Food & Agriculture	1.22267*	.27366	.001	<i>reject H0</i>
Transportation (Group 5)	Energy	-1.18772*	.32590	.017	<i>reject H0</i>
	Banking & Finance	-1.31930*	.27022	.000	<i>reject H0</i>
	Information & Communication	-1.16478*	.26545	.001	<i>reject H0</i>
Water (Group 6)	National Defence & Security	-1.28728*	.34083	.011	<i>reject H0</i>
	Energy	-1.71053*	.36437	.000	<i>reject H0</i>
	Banking & Finance	-1.84211*	.31555	.000	<i>reject H0</i>
	Government	-1.42544*	.34083	.003	<i>reject H0</i>
Health Services (Group 7)	Energy	-1.35965*	.36437	.013	<i>reject H0</i>
	Banking & Finance	-1.49123*	.31555	.000	<i>reject H0</i>
	Information & Communication	-1.33671*	.31148	.002	<i>reject H0</i>
Government (Group 8)	Water	1.42544*	.34083	.003	<i>reject H0</i>
Emergency Service (Group 9)	Energy	-1.39298*	.38215	.017	<i>reject H0</i>
	Banking & Finance	-1.52456*	.33593	.001	<i>reject H0</i>
	Information & Communication	-1.37004*	.33211	.004	<i>reject H0</i>
Food & Agriculture (Group 10)	Energy	-1.24561*	.33262	.012	<i>reject H0</i>
	Banking & Finance	-1.37719*	.27829	.000	<i>reject H0</i>
	Information & Communication	-1.22267*	.27366	.001	<i>reject H0</i>

## **Appendix H**

### **Online Organisation Resilience Survey**

## Organisation Resilience Survey

### Organisation Resilience on Critical Infrastructures Organisations

#### INTRODUCTION:

Organisation resilience is the capability of an organisation to adapt from the consequences of a catastrophic failure caused by natural disaster, technical failure, man-made disaster or any cyber threats that potentially disrupt the organisation functions and operations.

#### OBJECTIVE:

This survey is aim to collect some data on organisation resilience and preparedness towards the unexpected events and how it can adapt to any changes, and rapidly bounce back from any disaster. This survey used Organisation Resilience Benchmark Tool, developed by Mc Manus (2008) and Stephenson (2010).

#### REFERENCES

1. Stephenson, A. V. (2010). Benchmarking the resilience of organisations.  
<http://www.ir.canterbury.ac.nz/handle/10092/5303>

2. McManus, S., Seville, E., Brunsdon, D., & Vargo, J. (2007). Resilience management: a framework for assessing and improving the resilience of organisations. Resilient organisations research report. <http://ir.canterbury.ac.nz/handle/10092/2810>

#### CONFIDENTIALITY :

The information of this study including participant's response data will be kept confidential and can only be accessed by this researcher. No reference will be made in any report, which may link the participants to the study.

#### CONTACT:

If you have questions about the study, please contact:

Mrs Arniyati Ahmad, at Email: [a.ahmad.1@research.gla.ac.uk](mailto:a.ahmad.1@research.gla.ac.uk),

Prof Chris Johnson, at Email: [Christopher.Johnson@glasgow.ac.uk](mailto:Christopher.Johnson@glasgow.ac.uk),

School of Computing Science, University of Glasgow

Participation in this survey is entirely voluntary, meaning that you can withdraw at any time.

However, we would be very grateful if you could attempt to answer all questions. All responses are anonymous.

**BY CLICKING NEXT YOU ARE AGREEING TO PARTICIPATE IN THIS SURVEY**

Thank you for participating in this survey.

# Organisation Resilience Survey

## Background Information

\* 1. In which country do you work?

Country

Other (please specify)

2. Under which category does your organisation belong?

☐ Public

☐ Private

\* 3. Under which sector that your organisation belong?

☐ National Defence & Security

☐ Energy

☐ Emergency Services

☐ Banking & Finance

☐ Transportation

☐ Food & Agriculture

☐ Water

☐ Health Services

☐ Other

☐ Information & Communication

☐ Government

Other (please specify)

4. Which of the following best describes the department or business unit you work in?

☐ Accounting & Payroll

☐ Support

☐ Marketing

☐ Administration

☐ Facilities & Maintenance

☐ Manufacturing

☐ Customer Services

☐ Finance & Insurance

☐ Media & Public Relations

☐ Design & Print Services

☐ Health & Safety

☐ Procurement

☐ Engineering

☐ Human Resources

☐ Risk Management Sales

☐ Emergency Planning/Management

☐ ICT/Networking

☐ Other

☐ Information Security

☐ Logistics

Other (please specify)

5. Which of these levels best describes your position within your organisation?

- ☐ Senior Manager ☐ Technical ☐ Other
- ☐ Middle Manager ☐ Support
- ☐ Admin ☐ Staff

Other (please specify)

## Organisation Resilience Survey

\* 6. Which role do you play in your organisation? (you can tick on more than one answer)

- ☐ Decision Maker ☐ Technical Advisory
- ☐ Strategic Planner ☐ Other
- ☐ Policy Maker

Other (please specify)

\* 7. How long have you worked in your industry? (please tick one):

- ☐ Less than 1 year ☐ 1-3 years ☐ 4-10 years ☐ 11-20 years ☐ 21+ years

\* 8. How long have you worked at your organisation? (please tick one)

- ☐ Less than 1 year ☐ 1-3 years ☐ 4-10 years ☐ 11-20 years ☐ 21+ years

\* 9. Has your organisation experienced a crisis or emergency in the last 5 years? (please tick one)

- ☐ Yes ☐ No ☐ Don't Know

\* 10. Why type of Disaster/Crisis that your organisation experienced? (You can tick more than one)

- ☐ Natural ☐ Man made ☐ Technical Failure ☐ Cyber Attack
- ☐ Other

Other (please specify)

## Crisis Management

\* 11. Think of the highest risk will be facing by your organisation; which of the categories does it fit into?

- |                                                                     |                                            |                                                    |
|---------------------------------------------------------------------|--------------------------------------------|----------------------------------------------------|
| <input type="checkbox"/> Natural hazard                             | <input type="checkbox"/> Fire              | <input type="checkbox"/> Staffing issues           |
| <input type="checkbox"/> Financial crisis                           | <input type="checkbox"/> Reputation damage | <input type="checkbox"/> Failure of a key supplier |
| <input type="checkbox"/> Major accident                             | <input type="checkbox"/> Fraud             | <input type="checkbox"/> Failure of customer       |
| <input type="checkbox"/> Loss of critical services e.g. electricity | <input type="checkbox"/> Cyber Threats     |                                                    |
| <input type="checkbox"/> Pandemic                                   | <input type="checkbox"/> Regulatory issues |                                                    |

\* 12. Our organisation prepares for crisis through: (please tick one)

- ☐ Planning ☐ Insurance ☐ A combination of planning and insurance ☐ Don't know

## Resilience Ethos

\* 13. Please rate for each question in a scale of 1 to 10.

1=Does not describe my organisation at all. 10=Accurately describes my organisation

If you unable to answer the questions please choose 'Don't Know' Option.

	Don't Know	1	2	3	4	5	6	7	8	9	10
Our organisation is focused on being able to respond to the unexpected	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
In our organisation, there is an appropriate balance between short and long term priorities	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Our organisation is concerned with building people's ability to respond to unexpected challenges	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Our organisation actively participates in industry or sector groups	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Our organisation is able to collaborate with others in our industry to manage unexpected challenges	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Management see our organisation as having a leadership role in our industry	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

## Situation Awareness 1

\* 14. Please rate for each question in a scale of 1 to 10.

1=Does not describe my organisation at all. 10= Accurately describes my organisation

If you unable to answer the questions please choose 'Don't Know' Option.

[illegible]

\* 15. Please rate for each question in a scale of 1 to 10.

If you unable to answer the questions please choose 'Don't Know' Option



Our organisation is prepared to invest to ensure that decisions are made on the basis of the most up to date information

☐☐☐☐☐☐☐☐☐☐

In our organisation, it is generally easy to obtain expert assistance when something comes up that we don't know how to handle

☐☐☐☐☐☐☐☐☐☐

If something is not working well, I believe staff from any part of our organisation would feel able to raise the issues with senior management

☐☐☐☐☐☐☐☐☐☐

### Management of Keystone Vulnerabilities

\* 16. Please rate for each question in a scale of 1 to 10.

1= Does not describe my organisation at all. 10=Accurately describes my organisation

If you unable to answer the questions please choose 'Don't Know' Option.

Don't  
Know 1 2 3 4 5 6 7 8 9 10

Given our level of importance to our stakeholders I believe that the way we plan for the unexpected is appropriate

☐☐☐☐☐☐☐☐☐☐☐☐

Our organisation understands that having a plan for emergencies is not enough and that the plan must be practiced and tested to be effective

☐☐☐☐☐☐☐☐☐☐☐☐

People are generally able to take time off from their day-to-day roles to be involved in practicing how we respond in an emergency

☐☐☐☐☐☐☐☐☐☐☐☐

I believe our organisation invests sufficient resources in being ready to respond to an emergency of any kind

☐☐☐☐☐☐☐☐☐☐☐☐

I believe that our organisation has sufficient internal resources to operate successfully during business-as-usual

☐☐☐☐☐☐☐☐☐☐☐☐

During business as usual resources are managed so that we are always able to absorb a small amount of unexpected change

☐☐☐☐☐☐☐☐☐☐☐☐

When a problem occurs in our organisation, internal resources become more easily available at short notice and there is less red tape to deal with

☐☐☐☐☐☐☐☐☐☐☐☐

I am confident that our staff have enough contacts that we would be able to access external resources at short notice if we needed to

☐☐☐☐☐☐☐☐☐☐☐☐

Our organisation has agreements with other organisations to provide resources in an emergency

☐☐☐☐☐☐☐☐☐☐☐☐

\* 17. Please rate for each question in a scale of 1 to 10.

1= Does not describe my organisation at all. 10=Accurately describes my organisation

If you unable to answer the questions please choose 'Don't Know' Option.

	Don't Know	1	2	3	4	5	6	7	8	9	10
Our organisation has thought about and planned for support that it could provide to the community during an emergency	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
People in our organisation actively manage areas of their work that rely on other organisations	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Our organisation keeps in contact with organisations that it might have to work with in a crisis	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Our organisation understands how it is connected to other organisations in the same industry or location, and actively manages those links	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
People in our organisation understand how quickly we could be affected by unexpected and potentially negative events	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
People in our organisation report significant mistakes even if others do not notice that a mistake is made	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
People in our organisation are always rewarded if they spot potential trouble spots	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
People at all levels of the organisation often think about what could go wrong so that they can create ways to manage those challenges	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Most people in our organisation feel responsible for the organisations effectiveness	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
People in our organisation typically "own" a problem until it is resolved	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

## Crisis Management & Planning

\* 18. Our organisation currently employs people in the following areas (tick all that apply) :

- ☐ Risk management
 ☐ Crisis management
 ☐ Emergency management
 ☐ Business Continuity management
- ☐ Other

Other (please specify)

\* 19. Does your organisation have a formal written crisis/emergency or business continuity plan?

- ☐ Yes
 ☐ No
 ☐ Don't Know

☐ Yes ☐ No ☐ Don't Know

☐ Yes ☐ No ☐ Don't Know

<input type="checkbox"/> Natural hazard	<input type="checkbox"/> Fire	<input type="checkbox"/> Regulatory issues
<input type="checkbox"/> Financial crisis	<input type="checkbox"/> Fraud	<input type="checkbox"/> Loss of critical services e.g. electricity
<input type="checkbox"/> Major accident	<input type="checkbox"/> Cyber Threats	<input type="checkbox"/> Other

--

## Adaptive Capacity

1=Does not describe my organisation at all. 5=Accurately describes my organisation

[illegible]

## Adaptive Capacity 2

1=Does not describe my organisation at all. 5=Accurately describes my organisation

Don't Know 1 2 3 4 5 6 7 8 9 10

[illegible]

25. Comment

Thank you for your cooperation by fill up this survey, your participation is highly appreciated

## Bibliography

- [AD<sup>+</sup>06] Thomas Augustine, Ronald C Dodge, et al. Cyber defense exercise: meeting learning objectives thru competition. 2006.
- [AD10] Julia H Allen and Noopur Davis. Measuring operational resilience using the cert resilience management model. 2010.
- [ADMW10] Thomas A Augustine, Lori L DeLooze, Justin C Monroe, and Christopher G Wheeler. Cyber competitions as a computer science recruiting tool. *Journal of Computing Sciences in Colleges*, 26(2):14–21, 2010.
- [AGLL09] William J Adams, Efstratios Gavvas, Timothy H Lacey, and Sylvain P Leblanc. Collective views of the nsa/css cyber defense exercise on curricula and learning objectives. In *CSET*, 2009.
- [AH11] Rahayu Azlina Ahmad and Mohd Shamir Hashim. The organisation of islamic conferencecomputer emergency response team (oic-cert): Answering cross border cooperation. In *Cybersecurity Summit (WCS), 2011 Second Worldwide*, pages 1–5. IEEE, 2011.
- [Ahm14] Bob Mustaffa Ahmad. X maya 5 - the national cyber crisis exercise 2013, <https://www.youtube.com/watch?v=mt1neiedy4g>, 2014.
- [Amo11] Edward G Amoroso. Cyber attacks: awareness. *Network Security*, 2011(1):10–16, 2011.
- [Amo12] Edward G Amoroso. *Cyber attacks: protecting national infrastructure*. Elsevier, 2012.
- [AMZJ12] Abdul Ghani Azmi, Ida Madieha, Sonny Zulhuda, and Sigit Puspito Wigati Jarot. Data breach on the critical information infrastructures: Lessons from the wikileaks. In *Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on*, pages 306–311. IEEE, 2012.

- [APc15] Apcert embarks on cyber attacks beyond traditional sources. Technical report, Asia Pacific Computer Emergency Response Team (APCERT), 2015.
- [AS12] C Warren Axelrod and Robert Schmidt. A successful transaction-level simulation model of the us securities marketplace. In *Homeland Security (HST), 2012 IEEE Conference on Technologies for*, pages 529–534. IEEE, 2012.
- [ASG04] Kaye Alvarez, Eduardo Salas, and Christina M Garofano. An integrated model of training evaluation and effectiveness. *Human Resource Development Review*, 3(4):385–416, 2004.
- [Bal04] Howard Ball. *USA Patriot Act of 2001*. ABC-CLIO, 2004.
- [Bas01] Colin Baskin. Using kirkpatrick's four-level-evaluation model to explore the effectiveness of collaborative online group work. In *Proceedings of the Annual Conference of the Australasian Society for Computers in Learning in Tertiary Education*, pages 9–12, 2001.
- [Bat04] Reid Bates. A critical analysis of evaluation practice: the kirkpatrick model and the principle of beneficence. *Evaluation and program planning*, 27(3):341–347, 2004.
- [BB10] Bruce Braes and David Brooks. Organisational resilience: a propositional study to understand and identify the essential concepts. 2010.
- [BB11] Kevin Burnard and Ran Bhamra. Organisational resilience: development of a conceptual framework for organisational responses. *International Journal of Production Research*, 49(18):5581–5599, 2011.
- [BG11] Deborah Bodeau and Richard Graubart. Cyber resiliency engineering framework. The MITRE Corporation, 2011.
- [BG13] Deborah Bodeau and Richard Graubart. Intended effects of cyber resiliency techniques on adversary activities. In *Technologies for Homeland Security (HST), 2013 IEEE International Conference on*, pages 7–11. IEEE, 2013.
- [BGS<sup>+</sup>08] Philip Burnard, P Gill, K Stewart, E Treasure, and B Chadwick. Analysing and presenting qualitative data. *British dental journal*, 204(8):429–432, 2008.
- [bH11] Mohd Shamir b Hashim. Malaysia's national cyber security policy: The country's cyber defence initiatives. In *2011 Second Worldwide Cybersecurity Summit (WCS)*. 2011.

- [Bia06] Andrzej Bialas. Information security systems vs. critical information infrastructure protection systems-similarities and differences. In *Dependability of Computer Systems, 2006. DepCos-RELCOMEX'06. International Conference on*, pages 60–67. IEEE, 2006.
- [BKGT11] Yan Bei, Robert Kesterson, Kyle Gwinnup, and Carol Taylor. Cyber defense competition: a tale of two teams. *Journal of Computing Sciences in Colleges*, 27(1):171–177, 2011.
- [Blu02] Infrastructure interdependencies tabletop exercise: Blue cascades. Technical report, Pacific NorthWest Economic Region, 2002.
- [BP97] Robert Bood and Theo Postma. Strategic learning with scenarios. *European Management Journal*, 15(6):633–647, 1997.
- [BR94] Therese L Baker and Allen J Risley. Doing social research. 1994.
- [BS09] EM Brunner and M Suter. International critical information infrastructure protection handbook. *Center for Security Studies, ETH Zurich*, 2009.
- [Bur91] Philip Burnard. A method of analysing interview transcripts in qualitative research. *Nurse education today*, 11(6):461–466, 1991.
- [Bur94] Philip Burnard. Searching for meaning: a method of analysing interview transcripts with a personal computer. *Nurse Education Today*, 14(2):111–117, 1994.
- [BVH02] Edward Borodzicz and Kees Van Haperen. Individual and group learning in crisis simulations. *Journal of contingencies and crisis management*, 10(3):139–147, 2002.
- [BWS<sup>+</sup>14] Stefan Boesen, Richard Weiss, James Sullivan, M Locasto, Jens Mache, and Erik Nilsen. Edurange: meeting the pedagogical challenges of student participation in cybertraining environments. In *Proceedings of the 7th Workshop on Cybersecurity Experimentation and Test*, 2014.
- [CAB<sup>+</sup>07] Bei-Tseng Chu, Gail-Joon Ahn, Steven Blanchard, James Deese, Richard Kelly, Huiming Yu, and Ashika Young. Collegiate cyber game design criteria and participation. In *Computer and Information Science, 2007. ICIS 2007. 6th IEEE/ACIS International Conference on*, pages 1036–1041. IEEE, 2007.
- [Cav07] Myriam Dunn Cavelty. Critical information infrastructure: vulnerabilities, threats and responses. In *Disarmament Forum*, volume 3, pages 15–22, 2007.



- [CCHL] Jonathan Crawford, Kenneth Crowther, Barry Horowitz, and James Lambert. An example collaborative exercise for decision making in investment in cyber security.
- [CH96] Louis Cohen and Michael Holliday. *Practical statistics for students: An introductory text*. Sage, 1996.
- [Cho10] Kim-Kwang Raymond Choo. High tech criminal threats to the national information infrastructure. *Information security technical report*, 15(3):104–111, 2010.
- [CIP09] National strategy for critical infrastructure protection. Technical report, Federal Republic of Germany, 2009.
- [CIP10] Critical infrastructure resilience strategy. Technical report, Commonwealth of Australia, 2010.
- [CMZ10] Anna Carlin, Daniel Manson, and Jake Zhu. Developing the cyber defenders of tomorrow with regional collegiate cyber defense competitions (ccdc). *Information Systems Education Journal*, 8(14), 2010.
- [Con05] Art Conklin. The use of a collegiate cyber defense competition in information security education. In *Proceedings of the 2nd annual conference on Information security curriculum development*, pages 16–18. ACM, 2005.
- [Con06] Art Conklin. Cyber defense competitions and information security education: An active learning solution for a capstone course. In *System Sciences, 2006. HICSS'06. Proceedings of the 39th Annual Hawaii International Conference on*, volume 9, pages 220b–220b. IEEE, 2006.
- [COT13] Christian Czosseck, Rain Ottis, and Anna-Maria Talihärm. Estonia after the 2007 cyber attacks: Legal, strategic and organisational changes in cyber security. *Case Studies in Information Warfare and Security: For Researchers, Teachers and Students*, page 72, 2013.
- [CPH13] Kyle Cronin, Wayne Pauli, and Michael Ham. Creating a virtualized environment for large-scale hands-on ia education. In *Proceedings of the Information Systems Educators Conference ISSN*, volume 2167, page 1435, 2013.
- [cpn09] Cpni(centre for the protection of critical infrastructure, <http://www.cpni.gov.uk/>, 2009.

- [CRC<sup>+</sup>12] Michael Champion, Prashanth Rajivan, Nancy J Cooke, Shree Jariwala, et al. Team-based cyber defense analysis. In *Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), 2012 IEEE International Multi-Disciplinary Conference on*, pages 218–221. IEEE, 2012.
- [Cro51] Lee J Cronbach. Coefficient alpha and the internal structure of tests. *psychometrika*, 16(3):297–334, 1951.
- [CS12] Myriam Dunn Cavelty and Manuel Suter. The art of ciip strategy: tacking stock of content and processes. In *Critical Infrastructure Protection*, pages 15–38. Springer, 2012.
- [CSM08] Michael Collins, Dino Schweitzer, and Dan Massey. Canvas: a regional assessment exercise for teaching security concepts. In *Proceedings from the 12th Colloquium for Information Systems Security Education*, 2008.
- [CW06] Art Conklin and Gregory B White. E-government and cyber security: the role of cyber security exercises. In *System Sciences, 2006. HICSS’06. Proceedings of the 39th Annual Hawaii International Conference on*, volume 4, pages 79b–79b. IEEE, 2006.
- [Cyb06] Cyber storm i, exercise report. Technical report, Department of Homeland Security, 2006.
- [cyb11] Government portal brought down, 51 sites attacked, 2011.
- [DEC<sup>+</sup>11] Adam Doupé, Manuel Egele, Benjamin Caillat, Gianluca Stringhini, Gorkem Yakin, Ali Zand, Ludovico Cavedon, and Giovanni Vigna. Hit’em where it hurts: a live security exercise on cyber situational awareness. In *Proceedings of the 27th Annual Computer Security Applications Conference*, pages 51–61. ACM, 2011.
- [DGMM11] Jessica T DeCuir-Gunby, Patricia L Marshall, and Allison W McCulloch. Developing and using a codebook for the analysis of interview data: an example from a professional development research project. *Field Methods*, 23(2):136–155, 2011.
- [DJHN09] Ronald C Dodge Jr, Brian Hay, and Kara Nance. Standards-based cyber exercises. In *Availability, Reliability and Security, 2009. ARES’09. International Conference on*, pages 738–743. IEEE, 2009.
- [DJRR03] Ronald C Dodge Jr, Daniel J Ragsdale, and Charles Reynolds. Organization and training of a cyber security team. In *Systems, Man and Cybernetics, 2003. IEEE International Conference on*, volume 5, pages 4311–4316. IEEE, 2003.

- [DSZ09] Suhazimah Dzazali, Ainin Sulaiman, and Ali Hussein Zolait. Information security landscape and maturity level: Case study of Malaysian public service (mps) organizations. *Government Information Quarterly*, 26(4):584–593, 2009.
- [EO09] Panagiotis Saragiotis Evangelos Ouzounis, Panagiotis Trimintzios. Good practice guide on national exercises, 2009.
- [ETM15] Margus Ernits, Johannes Tammekänd, and Olaf Maennel. i-tee: A fully automated cyber defense competition for students. In *Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication*, pages 113–114. ACM, 2015.
- [FF05] John D Fernandez and Andres E Fernandez. Scada systems: vulnerabilities and remediation. *Journal of Computing Sciences in Colleges*, 20(4):160–168, 2005.
- [Fle81] Joseph L Fleiss. The measurement of interrater agreement. *Statistical methods for rates and proportions*, 2:212–236, 1981.
- [FPB10] Adrian Furtună, Victor-Valeriu Patriciu, and Ion Bica. A structured approach for implementing cyber security exercises. In *Communications (COMM), 2010 8th International Conference on*, pages 415–418. IEEE, 2010.
- [FR11] James P Farwell and Rafal Rohozinski. Stuxnet and the future of cyber war. *Survival*, 53(1):23–40, 2011.
- [GMP11] Harriet Goldman, Rosalie McQuaid, and Jeffrey Picciotto. Cyber resilience for mission assurance. In *Technologies for Homeland Security (HST), 2011 IEEE International Conference on*, pages 236–241. IEEE, 2011.
- [GOS06] Walter M Grayman, Avi Ostfeld, and Elad Salomons. Locating monitors in water distribution systems: Red team–blue team exercise. *Journal of water resources planning and management*, 132(4):300–304, 2006.
- [GR10] A Guerber and D Risk. Methods for enhanced cyber exercises, 2010.
- [Gri04] Michael R Grimaila. A novel scenario-based information security management exercise. In *Proceedings of the 1st annual conference on Information security curriculum development*, pages 66–70. ACM, 2004.
- [GRM03] Ursula Grandcolas, Ruth Rettie, and Kira Marusenko. Web survey bias: sample or mode effect? *Journal of Marketing Management*, 19(5-6):541–561, 2003.
- [Has11] MS Hashim. Malaysias national cyber security policy. 2011.

- [Her11] Stephen Herzog. Revisiting the estonian cyber attacks: Digital threats and multinational responses. *Journal of Strategic Security*, 4(2):4, 2011.
- [HO97] John F Home and John E Orr. Assessing behaviors that create resilient organizations. *Employment Relations Today*, 24(4):29–39, 1997.
- [HRD<sup>+</sup>05] Lance J Hoffman, Tim Rosenberg, Ronald Dodge, et al. Exploring a national cybersecurity exercise for universities. *Security & Privacy, IEEE*, 3(5):27–33, 2005.
- [HS14] Fredrik Hult and Giri Sivanesan. What good cyber resilience looks like. *Journal of business continuity & emergency planning*, 7(2):112–125, 2014.
- [Hys07] Maitland Hyslop. *Critical information infrastructures: Resilience and protection*. Springer Science & Business Media, 2007.
- [ISS14] Suhaila Ismail, Elena Sitnikova, and Jill Slay. Towards developing scada systems security measures for critical infrastructures against cyber-terrorist attacks. In *ICT Systems Security and Privacy Protection*, pages 242–249. Springer, 2014.
- [Jas14] Kick Jason. Cyber exercise playbook. Technical report, The MITRE Corporation, 2014.
- [Joh12] Chris W Johnson. Preparing for cyber-attacks on air traffic management infrastructures: cyber-safety scenario generation. 2012.
- [KB04] John M Kamensky and Thomas J Burlin. *Collaboration: Using networks and partnerships*. Rowman & Littlefield Publishers, 2004.
- [Kir75] Donald L Kirkpatrick. *Evaluating training programs*. Tata McGraw-Hill Education, 1975.
- [Kir09a] Donald L Kirkpatrick. *Implementing the Four Levels: A Practical Guide for Effective Evaluation of Training Programs: Easyread Large Edition*. Read-HowYouWant. com, 2009.
- [Kir09b] J Kirkpatrick. The kirkpatrick model: past, present and future. *Chief Learning Officer*, 8(11):20–55, 2009.
- [LBSDG13] HAM Luijff, Kim Besseling, Maartje Spoelstra, and Patrick De Graaf. Ten national cyber security strategies: A comparison. In *Critical Information Infrastructure Security*, pages 1–17. Springer, 2013.

- [LBW94] K Louise Barriball and Alison While. Collecting data using a semi-structured interview: a discussion paper. *Journal of advanced nursing*, 19(2):328–335, 1994.
- [LC05] Patricia Y Logan and Allen Clarkson. Teaching students to hack: curriculum issues in information security. In *ACM SIGCSE Bulletin*, volume 37, pages 157–161. ACM, 2005.
- [Led92] Linda Costigan Lederman. Debriefing: Toward a systematic assessment of theory and practice. *Simulation & gaming*, 23(2):145–160, 1992.
- [LEP<sup>+</sup>13] Igor Linkov, Daniel A Eisenberg, Kenton Plourde, Thomas P Seager, Julia Allen, and Alex Kott. Resilience metrics for cyber systems. *Environment Systems and Decisions*, 33(4):471–476, 2013.
- [Lew03] James Lewis. Cyber terror: Missing in action. *Knowledge, Technology & Policy*, 16(2):34–41, 2003.
- [Lin03] Russell M Linden. *Working across boundaries: Making collaboration work in government and nonprofit organizations*. John Wiley & Sons, 2003.
- [Lin15] LinkedIn - about us, 2015.
- [Lui12] Eric Luijff. Understanding cyber threats and vulnerabilities. In *Critical Infrastructure Protection*, pages 52–67. Springer, 2012.
- [MA12] Rosmah Mohamed and Arni Ariyani Sarlis Alias. Evaluating the effectiveness of a training program using the four level kirkpatrick model in the banking sector in malaysia. 2012.
- [Mar09] Jim Marshall. The cyber scenario modeling and reporting tool (cybersmart). In *Conference For Homeland Security, 2009. CATCH'09. Cybersecurity Applications & Technology*, pages 305–309. IEEE, 2009.
- [Mat07] Jeffrey A Mattson. Cyber defense exercise: A service provider model. In *Fifth World Conference on Information Security Education*, pages 81–86. Springer, 2007.
- [MCD08] Jason B Moats, Thomas J Chermack, and Larry M Dooley. Using scenarios to develop crisis managers: Applications of scenario planning and scenario-based training. *Advances in Developing Human Resources*, 10(3):397–424, 2008.
- [McM08] Sonia T McManus. *Organisational resilience in new zealand*. PhD thesis, University of Canterbury, 2008.

- [MF06] Martin Mink and Felix C Freiling. Is attack better than defense?: teaching information security the right way. In *Proceedings of the 3rd annual conference on Information security curriculum development*, pages 44–48. ACM, 2006.
- [MFS<sup>+</sup>11] Ashish Malviya, Glenn Fink, Landon Sego, Barbara Endicott-Popovsky, et al. Situational awareness as a measure of performance in cyber security collaborative work. In *Information Technology: New Generations (ITNG), 2011 Eighth International Conference on*, pages 937–942. IEEE, 2011.
- [MHS13] Matthew B Miles, A Michael Huberman, and Johnny Saldaña. *Qualitative data analysis: A methods sourcebook*. SAGE Publications, Incorporated, 2013.
- [ML15] Erik Moore and Dan Likarish. A cyber security multi agency collaboration for rapid response that uses agile methods on an education infrastructure. In *Information Security Education Across the Curriculum*, pages 41–50. Springer, 2015.
- [Mos85] Barbara Mostyn. The content analysis of qualitative research data: A dynamic approach. *The research interview*, pages 115–145, 1985.
- [MR12] Bill Miller and Dale Rowe. A survey scada of and critical infrastructure incidents. In *Proceedings of the 1st Annual conference on Research in information technology*, pages 51–56. ACM, 2012.
- [NF11] Eric C Nicolas F, Liam O M. W32.stuxnet dossier, 2011.
- [Nic06] Eugene Nickolov. Critical information infrastructure protection: analysis, evaluation and expectations. *INFORMATION AND SECURITY*, 17:105, 2006.
- [NWD<sup>+</sup>12] Andrew Nicholson, Stuart Webber, Shaun Dyer, Tanuja Patel, and Helge Janicke. Scada security in the light of cyber-warfare. *Computers & Security*, 31(4):418–436, 2012.
- [Onw12] Cyril Onwubiko. *Situational Awareness in Computer Network Defense: Principles, Methods and Applications: Principles, Methods and Applications*. IGI Global, 2012.
- [O’R07] Thomas D O’Rourke. Critical infrastructure, interdependencies, and resilience. *BRIDGE-WASHINGTON-NATIONAL ACADEMY OF ENGINEERING-*, 37(1):22, 2007.
- [Pal13] Julie Pallant. *SPSS survival manual*. McGraw-Hill Education (UK), 2013.

- [PCC03] Garry D Peterson, Graeme S Cumming, and Stephen R Carpenter. Scenario planning: a tool for conservation in an uncertain world. *Conservation biology*, 17(2):358–366, 2003.
- [PDHP06] Peter Pederson, Danile Dudenhoefter, Steven Hartley, and May Permann. Critical infrastructure interdependency modeling: a survey of us and international research. *Idaho National Laboratory*, 25:27, 2006.
- [PEF<sup>+</sup>12] Frédéric D Petit, Lori K Eaton, Ronald E Fisher, Sean F McAraw, and Michael J Collins III. Developing an index to assess the resilience of critical infrastructure. *International Journal of Risk Assessment and Management*, 16(1-3):28–47, 2012.
- [PF06] Richard Power and Dario Forte. Ten years in the wilderness a retrospective part 2: Cyber security= national security. *Computer Fraud & Security*, 2006(2):16–20, 2006.
- [PF07] James P Peerenboom and Ronald E Fisher. Analyzing cross-sector interdependencies. In *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on*, pages 112–112. IEEE, 2007.
- [PF09] Victor-Valeriu Patriciu and Adrian Constantin Furtuna. Guide for designing cyber security exercises. In *Proceedings of the 8th WSEAS International Conference on E-Activities and information security and privacy*, pages 172–177. World Scientific and Engineering Academy and Society (WSEAS), 2009.
- [PT12] Razvan GAVRILA Panagiotis TRIMINTZIOS. On national and international cyber security exercises-survey, analysis and recommendation, 2012.
- [RB13] Robert Radvanovsky and Jacob Brodsky. *Handbook of SCADA/control systems security*. CRC Press, 2013.
- [Rid11] Gail Ridley. National security as a corporate social responsibility: Critical infrastructure resilience. *Journal of business ethics*, 103(1):111–125, 2011.
- [RMM10] Kenneth Reese, James Marshall, and Dennis McGrath. Cybersmart: Cyber scenario modeling and reporting tool. In *IEEE International Conference on Technologies for Homeland Security*, Waltham, MA, 2010.
- [RNS13] Theodore Reed, Kevin Nauer, and Austin Silva. Instrumenting competition-based exercises to evaluate cyber defender situation awareness. In *Foundations of Augmented Cognition*, pages 80–89. Springer, 2013.

- [SA93] Sandra Shelton and George Alliger. Who's afraid of level 4 evaluation? a practical approach. *Training and Development*, 47(6):43–46, 1993.
- [San99] J Reynaldo A Santos. Cronbachs alpha: A tool for assessing the reliability of scales. *Journal of extension*, 37(2):1–5, 1999.
- [SB09] Stephanie T Solansky and Tammy E Beck. Enhancing community safety and security through understanding interagency collaboration in cyber-terrorism exercises. *Administration & Society*, 40(8):852–875, 2009.
- [SDPS09] Roberto Setola, Stefano De Porcellinis, and Marino Sforna. Critical infrastructure dependency assessment using the input–output inoperability model. *International Journal of Critical Infrastructure Protection*, 2(4):170–178, 2009.
- [SFV13] Elena Sitnikova, Ernest Foo, and Rayford B Vaughn. *The Power of Hands-On Exercises in SCADA Cyber Security Education*. Springer, 2013.
- [SH12] Teodor Sommestad and Jonas Hallberg. Cyber security exercises and competitions as a platform for cyber security experiments. In *Secure IT Systems*, pages 47–60. Springer, 2012.
- [SJ03] Wayne J Schepens and John R James. Architecture of a cyber defense competition. In *Systems, Man and Cybernetics, 2003. IEEE International Conference on*, volume 5, pages 4300–4305. IEEE, 2003.
- [SMR<sup>+</sup>14] Austin Silva, Jonathan McClain, Theodore Reed, Benjamin Anderson, Kevin Nauer, Robert Abbott, and Chris Forsythe. Factors impacting performance in competitive cyber exercises. In *Proceedings of the Interservice/Interagency Training, Simulation and Education Conference, Orlando FL*, 2014.
- [SOC<sup>+</sup>09] Benjamin Sangster, TJ O'Connor, Thomas Cook, Robert Fanelli, Erik Dean, Christopher Morrell, and Gregory J Conti. Toward instrumenting network warfare competitions to generate labeled datasets. In *CSET*, 2009.
- [SPGM11] Christos Siaterlis, Andres Perez-Garcia, and Marcelo Masera. Using an emulation testbed for operational cyber security exercises. In *Critical Infrastructure Protection V*, pages 185–199. Springer, 2011.
- [SRB<sup>+</sup>04] Alan T Sherman, Brian O Roberts, William E Byrd, Matthew R Baker, and John Simmons. Developing and delivering hands-on information assurance exercises: experiences with the cyber defense lab at umbc. In *Information Assurance Workshop, 2004. Proceedings from the Fifth Annual IEEE SMC*, pages 242–249. IEEE, 2004.



- [SRS<sup>+</sup>02] Wayne J Schepens, Daniel J Ragsdale, John R Surdu, Joseph Schafer, and RI New Port. The cyber defense exercise: An evaluation of the effectiveness of information assurance education. *The Journal of Information Security*, 1(2), 2002.
- [Ste10] Amy Victoria Stephenson. Benchmarking the resilience of organisations. 2010.
- [SVS<sup>+</sup>10] Amy Stephenson, John Vargo, Erica Seville, et al. Measuring and comparing organisational resilience in auckland. 2010.
- [sym10] Symantec intelligence quarterly report:october-december,2010, 2010.
- [TGM12] Michael Tyworth, Nicklaus A Giacobe, and Vincent Mancuso. Cyber situation awareness as distributed socio-cognitive work. In *SPIE Defense, Security, and Sensing*, pages 84080F–84080F. International Society for Optics and Photonics, 2012.
- [The13] Paul Theron. *Critical Information Infrastructure Protection and Resilience in the ICT Sector*. IGI Global, 2013.
- [vdM15] Rob van der Meulen. Gartner says 6.4 billion connected "things" will be in use in 2016, up 30 percent from 2015, 2015.
- [WDG04] Gregory B White, Glenn Dietrich, and Tim Gole. Cyber security exercises: testing an organization's ability to prevent, detect, and respond to cyber security events. In *System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on*, pages 10–pp. IEEE, 2004.
- [Wei10] Joseph Weiss. *Protecting industrial control systems from electronic threats*. Momentum Press, 2010.
- [WG04] Gregory White and Tim Gole. The role of exercises in training the nation's cyber first-responders. *AMCIS 2004 Proceedings*, page 560, 2004.
- [Whi10] Exercise white noise post exercise public report. Technical report, Department for Business, Innovation and Skills (BIS ), 2010.
- [Wig14] Ivy Wigmore. Internet of things (iot), 2014.
- [wik16] LinkedIn, <https://en.wikipedia.org/wiki/linkedin>, 2016.
- [Wil03] Clay Wilson. Computer attack and cyberterrorism: Vulnerabilities and policy issues for congress. *Focus on Terrorism*, 9:1–42, 2003.

- [WKR<sup>+</sup>13] Zach R Whitman, Hlekiwe Kachali, Derek Roger, John Vargo, and Erica Seville. Short-form version of the benchmark resilience tool (brt-53). *Measuring Business Excellence*, 17(3):3–14, 2013.
- [WM08] Michael E Whitman and Herbert J Mattord. The southeast collegiate cyber defense competition. In *Proceedings of the 5th annual conference on Information security curriculum development*, pages 1–4. ACM, 2008.
- [WM12] Christian Willems and Christoph Meinel. Online assessment for hands-on cyber security training in a virtual lab. In *Global Engineering Education Conference (EDUCON), 2012 IEEE*, pages 1–10. IEEE, 2012.
- [Wor12a] Partnering for cyber resilience, 2012.
- [Wor12b] The world economic forum - about us, 2012.
- [Wor15] Partnering for cyber resilience, towards the quantification of cyber threats, 2015.
- [Wyb08] Jean-Luc Wybo. The role of simulation exercises in the assessment of robustness and resilience of private or public organizations. In *Resilience of Cities to Terrorist and other Threats*, pages 491–507. Springer, 2008.
- [ZW12] Wanying Zhao and Gannon White. A collaborative information sharing framework for community cyber security. In *Homeland Security (HST), 2012 IEEE Conference on Technologies for*, pages 457–462. IEEE, 2012.