

INFORMATION SECURITY RISK ASSESSMENT
USING SURVIVAL ANALYSIS TECHNIQUE FOR THE
MALAYSIAN PUBLIC SECTOR DATA CENTERS

INTHRANI SHAMMUGAM

UNIVERSITI TEKNOLOGI MALAYSIA

INFORMATION SECURITY RISK ASSESSMENT
USING SURVIVAL ANALYSIS TECHNIQUE FOR THE
MALAYSIAN PUBLIC SECTOR DATA CENTERS

INTHRANI SHAMMUGAM

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Doctor of Philosophy

Razak Faculty of Technology and Informatics
Universiti Teknologi Malaysia

JULY 2021

DEDICATION

I would like to dedicate this thesis to my most beloved father and late mother. My parents, from difficult circumstances and despite the hardships they faced in life, were able to provide me with as much as they could; safe home, an education, plenty of love and encouragement. Back then, me completing my secondary school education and earning a place in university was considered an astounding achievement for someone of my background. Today, to be able to complete a PhD thesis is something far beyond my imagination as a young girl. I am proud to be able to honour my parents for their many sacrifices to allow me to achieve such heights.

ACKNOWLEDGEMENT

This Doctor of Philosophy thesis would be the pinnacle of a lifetime of hard work, learning and persistent effort. As a young girl, I would never have dreamed that one day I would have the opportunity to continuously attain knowledge to this degree and at this age. For this I have to thank the people who have played a great role in helping me realise my dreams.

First and foremost, I would like to thank the Almighty for giving me the determination and strength to complete this thesis. Next, my parents, my father, Mr. Shammugam. N and late mother, Madam Valliamah. M, who tried their utmost to give me the best life possible within their means and without whose blessing this thesis would not have been possible. My father, who is 96 and a lifelong bibliophile, has always been a source of inspiration to me and has never stopped encouraging me to learn and improve since I was young. I will forever be grateful for the opportunities I have been afforded as a result of the path I was able to carve out due to my parents overwhelming confidence and belief in me.

To my supervisors, Dr. Ganthan Narayana Samy and Dr. Pritheega Magalingam, I express my deepest gratitude, for their creative input, infectious enthusiasm, continuous support and encouragement. The guidance and knowledge they imparted were truly crucial to complete my study and produce this manuscript, successfully.

I would like to express my immense gratitude to my husband, Jagathesan. S, who has remained a pillar of strength throughout all my endeavours. This would not have been possible without his sacrifice, encouragement, and never-ending faith in my abilities. To my two wonderful children, Dr. Nhanthinhi Jagathesan and Vigknaraja Jagathesan, who remain my biggest blessings, thank you for supporting me every step of the way. The road to completing my PhD was an arduous one, but the constant support provided by my family and my elder sister, has greatly eased my journey.

Lastly, I would also like to thank my friends and colleagues as I have been fortunate enough to be surrounded by people who have always remained incredibly understanding and helpful, especially Dr. Sri Lakshmi Kanniah. I am humbled by the faith and support extended to me by one and all throughout this challenging, enriching and exploratory journey. I am and always will be grateful.

ABSTRACT

The increase in information security threats and the resulting demand for more robust online services necessitates that the Malaysian Government takes relevant measures to better protect its Critical National Information and Communications Technology Infrastructure (CNII) to ensure business and services continuity. Thus, the Malaysian Public Sector needs to adopt a suitable risk assessment methodology to effectively protect the critical Information and Communication Technology (ICT) assets, primarily housed in data centers. However, selecting a suitable risk assessment methodology out of the plethora currently available is a challenge as the majority only provide very high level guidelines and most use the qualitative approach, which gives inaccurate results, needs repetitive efforts, is tedious, and time consuming. This research aims to develop a comprehensive method, covering all critical ICT assets systematically with standard detailed guidelines of risk assessment approach to identify, analyse as well as evaluate the risks associated with data centers. The proposed risk assessment approach will use the survival analysis technique, which is proven to be a reliable and effective method in predicting potential hazards of covariates accurately, for the subjects under observation and in compliance with the international standards ISO27005: Information Security Risk Management and ISO27001: Information Security Management System Requirements. The study employed the exploratory sequential mixed methods design methodology for the overall data collection, where qualitative and quantitative data were collected in Phase 1 and Phase 2 respectively. In Phase 2, the study took advantage of the medical research design approach and adopted the retrospective cohort study to collect historical data related to data center security incidents over two years, in a selected organization, and applied the survival analysis technique to analyse the collected data using the Cox Proportional Hazard model and the Counting Process layout format as well as the R statistical method, which led to the identification of 20 information security threats. The survival analysis technique was tested for its reliability using data sets of different sizes and was validated as the results had negligible disparity. These results were also consistent with two previous studies in two different environments, a health care system in a traditional environment and a cloud computing environment with a similarity in identifying information security threats of 91% and 69% respectively. The proposed risk assessment approach using the survival analysis technique was applied in a prominent organization and successfully identified the potential threats, their risk levels and significances, which helped them to prioritise the risks as well as focus on the important mitigation plans and optimise the resources. Thus, this study is expected to significantly contribute in identifying and mitigating risks associated with data centers, and safeguarding the government's critical ICT assets effectively. In addition, the study has successfully identified the potential information security threats often encountered by the Malaysian Public Sector data centers. This will help the ICT security officers to implement suitable control measures to prevent any untoward incident or minimise the adverse impact to ensure a safe and secured environment to conduct business and service delivery in their organizations. The study also enhances the risk assessment body of knowledge with a thoroughly researched, developed and tested risk assessment methodology to assess and predict potential information security risks for the data center environment.

ABSTRAK

Peningkatan ancaman keselamatan maklumat dan permintaan perkhidmatan atas talian yang lebih mantap dan menyeluruh telah menyebabkan Kerajaan Malaysia mengambil tindakan pencegahan yang lebih kukuh untuk memastikan keselamatan infrastruktur kritikal Teknologi Maklumat dan Komunikasi (TMK) nasional dan kesinambungan perkhidmatan serta perniagaan. Justeru, Sektor Awam Malaysia perlu mengguna pakai satu metodologi penilaian risiko yang sistematik dan berdaya untuk memastikan keselamatan aset TMK kritikalnya. Walaubagaimanapun, kini organisasi-organisasi sering menghadapi cabaran dalam memilih metodologi penilaian risiko yang sesuai memandangkan terdapat pelbagai jenis metodologi dan kebanyakannya hanya memberi panduan umum dan menggunakan kaedah kualitatif yang kurang tepat serta memerlukan masa dan usaha yang berulang. Kajian ini bertujuan untuk membangunkan satu pendekatan penilaian risiko yang komprehensif dan sistematik, merangkumi semua peralatan kritikal TMK dengan garis panduan terperinci bagi mengenalpasti, menganalisa dan menilai risiko-risiko yang dihadapi oleh pusat-pusat data. Pendekatan penilaian risiko yang dicadangkan akan mengguna pakai kaedah kuantitatif yang terbukti, berdaya dan berkesan dalam meramal dengan tepat risiko kovariate yang berpotensi bagi subjek-subjek di bawah pemerhatian. Selain itu, ia juga menepati piawaian antarabangsa *ISO27005: Information Security Risk Management* dan *ISO27001: Information Security Management System Requirements*. Kajian ini menggunakan *exploratory sequential mixed methods design methodology* bagi tujuan pengumpulan data kualitatif di Fasa 1 dan data kuantitatif Fasa 2. Di Fasa 2, pendekatan *medical research design* dan kaedah *retrospective cohort study* digunakan untuk mengumpul *historical data* berkaitan insiden keselamatan maklumat pusat data di sebuah organisasi kerajaan yang terpilih, bagi tempoh dua tahun. Seterusnya, model *Cox Proportional Hazard* dan *Counting Process layout* format di bawah teknik *Survival Analysis* (SA) telah digunakan untuk menganalisa data kuantitatif dengan *R statistical method*, di mana sebanyak 20 ancaman keselamatan maklumat telah dikenalpasti. Teknik SA ini telah diuji untuk kebolehpercayaannya dengan menggunakan set data yang berlainan saiz dan didapati keputusannya menunjukkan perbezaan yang tipis yang boleh diabaikan. Hasil keputusan juga adalah didapati konsisten dengan dua kajian yang telah dilaksanakan sebelum ini bagi dua jenis persekitaran yang berbeza, iaitu satu bagi sistem kesihatan di persekitaran tradisi dan satu lagi adalah di persekitaran pengkomputeran awan yang menunjukkan persamaan sebanyak 91% dan 69% masing-masing. Kaedah penilaian risiko yang dicadangkan yang telah diguna pakai di organisasi terpilih juga telah berjaya dalam mengenalpasti ancaman-ancaman yang berpotensi, tahap risiko serta signifikannya, lalu, membantu mereka mengoptimalkan sumber sedia ada dan memfokuskan pelan mitigasi berdasarkan keutamaan risiko yang telah dikenalpasti. Adalah diharapkan hasil kajian ini akan menyumbang dengan signifikan dalam pengurusan risiko dan memastikan keselamatan aset TMK kritikal kerajaan secara berkesan dengan merangka tindakan pencegahan yang bersesuaian untuk mengelak atau meminimalkan impak sebarang ancaman bagi memastikan satu persekitaran yang selamat untuk penyampaian perkhidmatan dan urusan perniagaan serta meningkatkan pengetahuan dalam bidang penilaian risiko keselamatan maklumat bagi persekitaran pusat data.

TABLE OF CONTENTS

	TITLE	PAGE
	DECLARATION	iii
	DEDICATION	iv
	ACKNOWLEDGEMENT	v
	ABSTRACT	vi
	ABSTRAK	vii
	TABLE OF CONTENTS	viii
	LIST OF TABLES	xvii
	LIST OF FIGURES	xix
	LIST OF ABBREVIATIONS	xxii
	LIST OF SYMBOLS	xxiv
	LIST OF APPENDICES	xxv
CHAPTER 1	INTRODUCTION	1
1.1	Overview	1
1.2	Background of The Research	6
1.2.1	Data Center	6
1.2.2	Data Center Assets	6
1.2.3	Data Center Services	7
1.2.4	Data Center Information Security Concerns	7
1.2.5	Need for An Effective Risk Assessment Methodology for Data Center	9
1.3	Problem Statement	12
1.4	Research Questions	13
1.5	Research Objectives	14
1.6	Research Scope	14
1.7	Significance of The Study	16
1.7.1	Theoretical Significance	16
1.7.2	Methodological Significance	16

1.7.3	Practical Significance	17
1.8	Organization of Thesis	19
CHAPTER 2	LITERATURE REVIEW	21
2.1	Introduction	21
2.2	Definition of Key Terms and Concepts	21
2.2.1	Definition of Key Terms	22
2.2.2	Risk	23
2.2.3	Critical Assets	25
2.2.4	Risk Management	27
2.2.5	Information Security	28
2.2.6	Information Security Management System	30
2.2.7	Information Security Risk	30
2.3	Information Security Threat	31
2.3.1	Security Threat	31
2.3.2	Classification of Information Security Threats	31
2.3.3	Sources of Threats	39
2.3.4	Threat Assessment Methodology	40
2.3.5	Vulnerability Assessment Methodology	41
2.3.6	Risk Assessment Methodology	41
2.4	Risk Assessment Phase	43
2.4.1	Risk Identification	43
2.4.2	Risk Analysis	44
2.4.3	Risk Evaluation	44
2.5	Risk Treatment Phase	45
2.6	Risk Acceptance Phase	46
2.7	Risk Monitoring & Review Phase	46
2.8	Risk Communication & Consultation Phase	47
2.9	Various Existing Risk Management Methods.	47
2.9.1	Risk Management Methods by International Bodies	48
2.9.1.1	ISO 31000:2018 Risk Management – Principles and Guidelines	48

2.9.1.2	ISO/IEC 27005:2018 – Information Technology-Security Techniques-Information Security Risk Management	49
2.9.1.3	BS ISO/IEC 27002:2013 – Information technology-Security techniques-Code of practice for information security controls	51
2.9.1.4	AS ISO 31000:2018 Risk Management – Principles and Guidelines.	52
2.9.2	Risk Management Methods by Professional Bodies	52
2.9.2.1	COBIT, 2013	52
2.9.2.2	CRAMM, 2001	53
2.9.2.3	CORAS, 2003	53
2.9.2.4	OCTAVE, 2005	54
2.9.2.5	MAGERIT, 2006	54
2.9.2.6	MicroSoft, 2006	56
2.9.2.7	MEHARI, 2007	57
2.9.2.8	NIST800-30, 2016.	58
2.9.3	Risk Management Methods by Malaysian Public Sector	60
2.9.3.1	The Malaysian Public Sector Information Security Risk Assessment Methodology (MyRAM), 2005.	60
2.9.4	Risk Management Methods Intended for Certification Purpose	61
2.9.4.1	ISO/IEC 27001:2013- Information Technology-Security Techniques-Information Security Management Systems (ISMS) - Requirements.	61
2.9.5	Risk Management Methods by Previous Researchers	62
2.9.5.1	Medical Research Design and Method	62

2.9.5.2	A Common Conceptual Framework of Info Structure for Information Security Risk Assessment (ISRA)	63
2.9.5.3	A Comprehensive Framework for Enterprise Information Security Risk Management	65
2.9.5.4	Quantifying Information Security Risk Using Expert Judgment Elicitation	66
2.9.5.5	An Information Systems Security Assessment (ISS) Model Based on The Improved Evidenced Theory	67
2.9.5.6	Event Tree Analysis (ETA) Combined with Fuzzy Decision Theory	67
2.9.5.7	A Formal Model and Risk Assessment Method for Security Critical Real-time Embedded Systems.	68
2.9.5.8	A Multidimensional Approach to Information Security Risk Management Using Failure Mode and Effects Analysis (FMEA) and Fuzzy Theory	68
2.9.5.9	A Functional Quantitative Security Risk Assessment Analysis	70
2.9.5.10	A Formal Methodology for Enterprise Information Security Risk Assessment	71
2.9.5.11	The Framework for Risk Assessment Based on Analysis of Historical Information of Workflow Execution in IT Systems	72
2.9.5.12	A Multidimensional Failure Cost Model.	73
2.9.5.13	A System Dynamic Model	73
2.10	Comparisons of Existing Risk Assessment Methodologies	75
2.10.1	Critical Analysis and Comparisons of Existing Risk Assessment Methodologies	81
2.11	Data Center Security Threats	82

2.12	Medical Research Design and Method	85
2.12.1	Basic Research	86
2.12.2	Clinical Research	86
2.12.3	Epidemiological Research	86
2.12.3.1	Cohort Study	87
2.12.4	Survival Analysis	88
2.12.4.1	Censored Data (Incomplete Data)	89
2.12.4.2	Recurrent Events	90
2.12.4.3	Counting Process Approach	90
2.12.4.4	Cox Proportional Hazard Model (Cox PH Model)	93
2.12.5	The Application of Survival Analysis in Risk Assessment	95
2.13	Research Gaps	98
2.13.1	Issues Highlighted by Past Researchers On Proposed Research Area and Current Risk Assessment Practices.	98
2.13.2	Identified Gaps in the Research Area.	103
2.13.2.1	Lack of Studies On Data Center Security.	104
2.13.2.2	No Data Center Specific Risk Assessment Method for Is Available	105
2.13.2.3	Available Methods Do Not Detail the Specific Steps of the Risk Assessment Processes.	105
2.14	Chapter Summary	106
CHAPTER 3 RESEARCH METHODOLOGY		107
3.1	Introduction	107
3.2	Research Design	107
3.2.1	Research Philosophy	108
3.2.2	Research Design Method	108
3.2.2.1	Qualitative Method	109
3.2.2.2	Quantitative Method	109

3.2.2.3	Mixed Method Research Design and Types.	110
3.2.2.4	Rationales for Mixed Methods Design	112
3.3	Research Procedures	113
3.4	Operational Framework of the Proposed Study	115
3.5	Population	117
3.5.1	Selected Organization's Profile: Ministry-A	118
3.6	The Chosen Mixed Methods Design: Exploratory Sequential Mixed Methods Design	119
3.6.1	Justification for Exploratory Sequential Mixed Methods Design	120
3.7	Data Collection and Analysis	121
3.7.1	Literature Review and Preliminary Data Collection	122
3.7.2	Field Setting	123
3.7.1.1	Stage 1 of Phase 1	125
3.7.1.2	Stage 2 of Phase 1	125
3.7.1.3	Phase 2	129
3.7.3	Qualitative Data Collection (Phase1): Semi Structured Interview	129
3.7.4	Quantitative Data Collection (Phase2): Retrospective Cohort Study	132
3.7.4.1	Medical Research Design and Method that Adopted for This Study	134
3.7.4.2	Justification of Adapting Medical Research Design, Survival Analysis Method, Cox PH Model and Retrospective Cohort Study.	135
3.8	Data Analysis	138
3.9	Assumptions	139
3.10	Chapter Summary	140
CHAPTER 4 A RISK ASSESSMENT APPROACH FOR MALAYSIAN PUBLIC SECTOR DATA CENTER		141
4.1	Introduction	141

4.2	Importance of an Effective Risk Assessment Approach	141
4.3	Proposed Risk Assessment Approach for The Malaysian Public Sector Data Centers	143
4.3.1	Establish Context	145
4.3.2	Risk Identification	147
4.3.3	Risk Analysis	148
4.3.4	Risk Evaluation	150
4.3.5	Risk Treatment	152
4.3.6	Risk Monitoring and Review	153
4.3.7	Risk Communication and Consultation	153
4.4	The Overall Differences Between the Traditional Risk Management Processes and Risk Management Processes Adopting Medical Research Design Approach	154
4.5	The Advantages and Characteristics of the Proposed Information Security Risk Assessment Using Survival Analysis Technique	156
4.6	Justification of Proposed Risk Assessment Approach Using the Survival Analysis Technique	156
4.7	The Recommended Relevant Guidelines for the Proposed Risk Assessment Using Survival Analysis Technique for Data Center in The Malaysia Public Sector	160
4.8	Chapter Summary	162
CHAPTER 5 RESULTS AND DISCUSSIONS		163
5.1	Introductions	163
5.2	Context Establishment Phase	163
5.2.1	Clients Distributions of Ministry-A	164
5.2.2	The Services Hosted at Ministry-A's Data Centers	164
5.2.3	The Critical ICT Assets in Ministry-A's Data Center	165
5.2.4	Defining Risk Criteria	166
5.3	Risk Identification Phase	169
5.3.1	The list of Information Security Threats Identified for this Study.	169

5.4	Risk Analysis Phase	174
5.4.1	Model Adopted: The Survival Analysis Method and Cox PH Model	175
5.4.2	Method Adopted: Efron Likelihood Estimation Method	175
5.4.3	Quantitative Analysis and Results	175
5.4.4	Data Summary	177
5.4.5	Results Analysis	178
5.4.5.1	Positive Regression Coefficient Values and High Level of Hazard	181
5.4.5.2	Negative Regression Coefficient Values and Low Level of Hazard	182
5.4.5.3	Zero Regression Coefficient Values and Zero Level of Hazard	183
5.4.5.4	Proportional Hazard Ratio	183
5.4.5.5	P-Value and Significance	186
5.5	Risk Evaluation and Discussion	188
5.5.1	Threat with High Risk Level and Significant	188
5.5.2	Threats with Low Level Risk and Significant	191
5.6	Risk Treatment	193
5.6.1	Proposed Guidelines and Purposes	193
5.7	Risk Monitoring and Review	195
5.8	Risk Communication and Consultation	195
5.9	Model Validation	195
5.9.1	Validation of Method Using Different Sizes of Data Set	196
5.9.2	Validation of Adopted Method by Comparing Different Environment	203
5.10	Chapter Summary	209
CHAPTER 6 CONCLUSION		211
6.1	Introduction	211
6.2	Achievement of Research Objectives	211

6.2.1	RO1: To Identify the Information Security Threats Faced by Data Centers in the Malaysian Public Sector Organizations	212
6.2.2	RO2: To propose, apply, and validate a risk assessment method adopting medical research design approach and survival analysis technique to effectively identify the potential information security threats and analyze the associated risks in the Malaysian Public Sector data center environment	213
6.2.3	RO3: To propose relevant guidelines for information security practitioners, risk analysts and those who are involved in managing data center security based on the proposed information security risk assessment method.	216
6.3	Research Contributions	217
6.3.1	Theoretical Contributions	217
6.3.2	Methodological Contributions	218
6.3.3	Practical Contributions	221
6.4	Limitations of the Research	222
6.5	Future Research	225
6.6	Concluding Remarks	226
	REFERENCES	227
	LIST OF PUBLICATIONS	307

LIST OF TABLES

TABLE NO.	TITLE	PAGE
Table 2.1	Definitions of Key Terms (ISO, 2014; 2018a)	22
Table 2.2	Example of Qualitative and Semi-Quantitative Scale (Snedaker et al, 2013; Zuheros et al, 2018).	40
Table 2.3	Differences Between Quantitative and Qualitative Methodologies (Goh, 2008; Shameli-Sendi et al, 2016)	42
Table 2.4	Comparison Among Several Types of Preferred Information Security Risk Assessment Methods	75
Table 2.5	Issues Highlighted by Past Researchers on Proposed Research Area and Current Risk Assessment Practices.	98
Table 3.1	Operational Framework	115
Table 3.2	Data Collection Methods Applied in This Study	121
Table 3.3	Information of Respondents and their Experiences in Handling Data Center in Ministry-A	126
Table 3.4	Experts Background	131
Table 5.1	Users or Clients Distribution of Ministry-A	164
Table 5.2	Services Hosted at Data Centers	165
Table 5.3	Critical ICT Assets at Data Centers	166
Table 5.4	Risk Criteria Measure Cox (1972)	168
Table 5.5	Information Security Threats	170
Table 5.6	The List of Threats Recorded During Over 731 Days for Ministry-A	176
Table 5.7	Data Summary	177
Table 5.8	The Results Obtained for the Entire Data Collected	178
Table 5.9	Security Threats with Positive Regression Coefficient Values	181
Table 5.10	Security Threats with Negative Regression Coefficient Values	182
Table 5.11	Security Threats with Hazard Ratio Value Greater Than One	184

Table 5.12	Security Threats with Hazard Ratio Values Less Than One	185
Table 5.13	Security Threats and Significant Values	186
Table 5.14	The Security Threats with High Risk Level and Significant	189
Table 5.15	The Security Threats with Low Risk Level and Significant	192
Table 5.16	Proposed Guidelines and Purposes	193
Table 5.17	The Results Obtained of Statistical Analysis for All Data Set, Data Collected in 2016 and their Comparisons.	197
Table 5.18	The Results Obtained of Statistical Analysis for All Data Set, Data Collected in 2017 and their Comparisons.	200
Table 5.19	Comparison of The Results Using Survival Analysis Method in HIS and DC Environments.	204
Table 5.20	Comparison of The Results Using Survival Analysis Method in Cloud Computing and Data Center Environments.	207

LIST OF FIGURES

FIGURE NO.	TITLE	PAGE
Figure 1.1	Data Center Services (Gusmão et al, 2016)	7
Figure 2.1	Risk and Other Security Elements Relationships Model (ISO, 2004).	24
Figure 2.2	Risk Management Process (ISO, 2018a)	28
Figure 2.3	A Multi-dimensions Threats Classification Model (Jouini et al, 2014)	33
Figure 2.4	Insider Activities and The Consequences (Sarkar, 2010)	34
Figure 2.5	Zero-Day Vulnerabilities, Annual Total (Symantec Corporation, 2016)	37
Figure 2.6	Security Incidents Statistic of Malaysia Based on General Classification for 2016 (Cybersecurity, 2016)	38
Figure 2.7	Security Incidents Statistic of Malaysia Based on General Classification for 2017 (Cybersecurity, 2017)	38
Figure 2.8	Information Security Risk Management Process ISO (2018b)	50
Figure 2.9	Conceptual Framework of Info-structure (Shamala et al, 2013)	64
Figure 2.10	The Enterprise Information Security Risk Management Framework (Saleh et al, 2011)	66
Figure 2.11	Failure Modes Associated with Each Dimension of an Information Security (Silva et al, 2014)	69
Figure 2.12	A Quantitative Risk Assessment Model for Critical Assets (Staalduinen et al, 2017)	71
Figure 2.13	Audit Findings in Percentages Classified by Category (Knapp et al, 2011).	83
Figure 2.14	Event Tree Analysis for Data Center Invasion (Gusmão et al, (2016)	84
Figure 2.15	Divisions and Various Types of Medical Study (Röhrig et al, 2009)	85
Figure 2.16(a)	General Layout (Kleinbaum et al, 2012)	91
Figure 2.16(b)	Counting Process Layout Format (Kleinbaum et al, 2012)	91

Figure 2.17	Differences in Forming the Likelihood Function for Cox PH Model (Kleinbaum et al, 2012).	92
Figure 2.18	Gaps Found in The Research Area.	104
Figure 3.1	Research Procedures of the Proposed Study.	114
Figure 3.2	Overview of The Research Design and Method	119
Figure 3.3	Application of Exploratory Sequential Mixed Methods Design for Data Collection in Phase 1 and Phase 2 and Risk Assessment.	124
Figure 3.4	Types of Observation: (a) Type I, (b) Type II, and (c) Type III (Sameer, 2016)	133
Figure 3.5	The Selected Medical Approach for This Study (Kartsonaki, 2016)	134
Figure 4.1	Proposed Risk Assessment Adopting Medical Research Design Approach and Survival Analysis Technique integrated in the Risk Management Framework of ISO27005	144
Figure 4.2	Activities in Establish Context Phase	145
Figure 4.3	Differences between the traditional and Medical Research Design and Approach in Context Establishment Phase	146
Figure 4.4	Detailed Activities in Risk Identification Phase	147
Figure 4.5	Differences between the traditional and Medical Research Design approaches in Risk Identification Phase	148
Figure 4.6	Activities in Risk Analysis Phase	149
Figure 4.7	Differences Between the Traditional and Medical Research Design and Approaches in Risk Analysis Phase	149
Figure 4.8	Activities in Risk Evaluation Phase	151
Figure 4.9	Differences between the traditional and Medical Research Design and Approaches in Risk Evaluation Phase	151
Figure 4.10	Detailed Activities in Risk Treatment Phase	152
Figure 4.11	Risk Monitoring and Review Activities	153
Figure 4.12	Risk Communication and Consultation Activities	154
Figure 4.13	Differences Between the Traditional Risk Management Processes and Risk Management Processes Adopting the Medical Research Design Approach.	155
Figure 4.14	The Recommended Guidelines for the Proposed Risk Assessment Approach for Data Centers.	161

Figure 5.1	The Results Obtained for the Entire Data Collected	180
Figure 5.2	Analysis Comparison of Regression Coefficient Values of All Data Set against Data Set for 2016.	199
Figure 5.3	Analysis Comparison of Regression Coefficient Values of All Data Set against Data Set for 2017.	202

LIST OF ABBREVIATIONS

AD	-	Active Directory
CBK	-	Common Body of Knowledge
CCTA	-	Central Communication and Telecommunication Agency
CCTV	-	Closed Circuit Television
CISO	-	Chief ICT Security Officers
CNII	-	Critical National Information Infrastructure
COBIT	-	Control Objectives for Information and Related Technologies
COX PH	-	Cox Proportional Hazards
CP	-	Counting Process
CRAMM	-	CCTA Risk Analysis and Management Method
CSM	-	Cyber Security Malaysia
DC	-	Data Center
DMAIC	-	Define, Measure, Analyze, Improve and Control
ETA	-	Event Tree Analysis
FMEA	-	Failure Mode and Effects Analysis
HA	-	High Availability
HR	-	Hazard Ratio
ICT	-	Information and Communication Technology
IPS	-	Intrusion Protection System
IS	-	Information Security
ISACA	-	Information Systems Audit and Control Association
ISMS	-	Information Security Management Systems
ISO	-	International Organization for Standardization
ISS	-	Information Systems Security
LAN	-	Local Area Network
MAMPU	-	Malaysian Administrative Modernisation and Management Planning Unit
MEHARI	-	MEthod for Harmonized Analysis of RIsk
MMFC	-	Multidimensional Failure Cost
MyCERT	-	Malaysian Computer Emergency Response Team

MyRAM	-	Malaysia Public Sector Information Security Risk Assessment Methodology
NA	-	Not Available
NCCCC	-	National Cyber Coordination and Command Center
NIST	-	National Institute of Standard and Technology
OCTAVE	-	Operationally Critical Threat, Asset and Vulnerability
OGC	-	Office of Government Commerce
OS	-	Operating System
PDSA	-	Pusat Data Sektor Awam
PMBOK	-	Project Management Body of Knowledge
PRINCE2	-	Project in Controlled Environment
RA	-	Risk Assessment
RC	-	Regression Coefficient
RM	-	Risk Management
RTP	-	Risk Treatment Plan
SA	-	Survival Analysis
SaaS	-	Software as a Service
SOP	-	Standard Operating Procedure
SPSS	-	Statistical Package Social Science
SQL	-	Structured Query language
STOPE	-	Strategy, Technology, Organization, People and Environment
SWOT	-	Strengths, Weaknesses, Opportunities and Threats
UPS	-	Uninterrupted Power Supply
WAF	-	Web Application Firewall
WAN	-	Wide Area Network
WAP	-	Wireless Access Points

LIST OF SYMBOLS

b_i	-	Regression Coefficient
$\exp(b_i)$	-	Hazard Ratio
=	-	Equal
>	-	More than
<	-	Less than
+ve	-	Positive
-ve	-	Negative

LIST OF APPENDICES

APPENDIX	TITLE	PAGE
Appendix A	Data Collected During Preliminary Study	239
Appendix B	Initial List of Threats Compiled Based On Literature Review and Preliminary Data Collection	244
Appendix C	List of Interview Participants for Phase 1	250
Appendix D	Questionnaire for Semi Structured Interview	265
Appendix E	Sample Interview Script	269
Appendix F	Analysis of Data Collected in Phase-1 on Threats That Encountered by Data Centers in 34 Agencies in The Malaysian Public Sector	277
Appendix G	List of Final Threats	282
Appendix H	Approval Letter for Data Collection	288
Appendix I	Sample Data Collection	289
Appendix J	Letter of Verification on Application of the Proposed Risk Assessment Using Survival Analysis Technique	293
Appendix K	Sample Data Counting Process Layout Format	296
Appendix L	Analysis of recorded events using counting processing format	302

CHAPTER 1

INTRODUCTION

1.1 Overview

Throughout the world, the Information and Communication Technology (ICT) revolution has tremendously changed the way businesses and governments operate as well as the life style of the people. The technological advancement has broken the barriers between countries and allows people to interact and share information instantly across the globe. The significance of time and place in communications has completely transformed. The global cyber world connects people, businesses, states, countries and continents in an entirely new manner (Lehto, 2016).

While the citizens, business communities, public sector, and the economy benefit greatly from globally networked services, the digital world contains numerous inherent vulnerabilities which pose threats and generate security risks for everyone involved. The attackers too have become more sophisticated in evading the perimeter defenses and their capabilities are growing exponentially. As mentioned by Jouini and Rabai (2016), in current digital world, information systems are common place and targets for information security attacks. This has led to more focus on the security concerns regarding the development and exploitation of information systems as the security threats are ever changing rapidly and vary over time.

The alarming increase in premeditated attacks to independent network and information systems across the globe with potential catastrophic damages has necessitated a greater need for critical information infrastructure protection initiatives (Cybersecurity Malaysia, 2016). In the recent report for 2019, Symantec Corporation, a software company which monitors internet threats worldwide stated that attacks such as website compromise, enterprise ransomware, malicious emails, supply chain attacks, destructive malware targeting organizations as well as email SPAM on

businesses and government organizations were on the rise in 2018 as compared to 2017 (Symantec Corporation, 2019). This shows that cybercrime has gradually become a part of our daily lives as the real and virtual become indistinguishable from each other. Attacks against nations and businesses constantly hit the headlines and the public have become numb to the sheer volume and rapidity of cyber threats.

Feng and Li (2011) cited that organizations are becoming increasingly dependence on the information systems and this has resulted in increased abuses in the information systems security. This phenomenon has attracted much attention from both information security researchers and practitioners as the information systems security has become one of the critical factors in current digital world. Jouini et al (2016) agreed that factors such as use of new technology, pressure for innovation, and pressure to cut cost demand security risk assessments to be addressed in a new perspective, especially the management of information security risk. Neglecting or discarding any of these factors can affect an organization's reputation and customer confidence tremendously. The authors also stressed that information security management can be costly if it is not done in a proactive and systematic manner.

In 2017, the world faced a major global cyber-attack by WannaCry ransomware. Security software maker Kaspersky Lab reported that more than 150 countries were affected across the world including countries like Malaysia, Russia, Ukraine, Britain, France, Germany, Italy, Poland, and United States with nearly 200,000 cases reported but the actual total number of attacks remains unknown (Reuters, 2017).

In Malaysia, information security incidents and threats started to attract public attention from 2002 when hackers defaced the websites of prominent government institutions and public universities such as the Malaysian Parliament and University Technology MARA (UiTM), which was considered very dangerous and damaging to the image of the country (Mohamed, 2013). The author also stated that cybercrimes and information security threats have become one of the modern problems, which will continue to increase and threaten the public security and economy. It is also a big

challenge in this country, as Malaysia lacks the essential skills, tools and technologies (Mohamed, 2013).

According to the Malaysian Computer Emergency Response Team (MyCERT), a department under Cyber Security Malaysia (CSM), the year 2019 saw the highest number of cyber-crimes with over 400 defacement incidents by end of August 2019 and this number did not include the unreported cases (Tariq, 2019). The National Cyber Coordination and Command Center (NCCCC) revealed that an increased amount of attacks on Malaysian organizations involving distributed denial of service, malware, and web defacement were detected in the month of August 2019 (Law, 2019).

The alarming spike in cyber threats and incidents in recent years is a cause of concern and worrying. CSM also stated that the 2020 saw a spike in the cyber threats in Malaysia with a total of 7,765 incidents reported in the first eight months of 2020, and based on the trend the number is expected to surpass 2019's record of 10,772 by end of 2020 (Bernama, 2020). In addition, CSM also mentioned that exposure to cyber threats is a problem that we have to deal with as we embrace the new norm of lifestyle in this Covid-19 era (Bernama, 2020).

A study by Szczepaniuk, E. K., Szczepaniuk, H., Rokicki, T., and Klepacki, B. (2020) revealed that information security management in public administration affects the reliability, efficiency and quality of their services and countries where public administration adopted and operate on new technologies have become more sensitive to disruption in their delivery system. The authors have emphasized that preventing the potential threats and providing information security involves a significant challenge, both for specific countries and international communities. E. Szczepaniuk et al (2020) have also highlighted that many countries and organizations acknowledge the need to develop efficient solutions that would increase the level of information security. The authors concluded that the information security in public administration requires a systematic approach.

In a recent cyber threat incident, a hacker group has threatened to bring down many government websites. The hackers have successfully hacked systems belonging to the Sabah and Johor State Governments as well as the Ministry of International Trade and Industry, a prominent federal ministry, (Free Malaysia Today, 2021). This clearly indicates that cyber threats will be a continuous challenge for Malaysian Public Sector. This, warrants the public sector organizations to strengthen their information security strategies and preventive actions as well as to be vigilant all the times.

Following the trends and development in cyber threats, for the Malaysian Public Sector, the information security issue is of paramount importance as the expectations of the citizens for the availability of reliable on-line services and confidential data, regardless of the geographical position, continues to increase. These expectations require the public sector organizations in Malaysia to be innovative and creative in taking advantage of the advancement of information technology to provide services that fulfil the citizens' needs.

In light of that, the Malaysian Public Sector is implementing many citizen-centric services through end-to-end ICT applications in order to increase its service efficiency, ease of doing business and global competitiveness. The public sector organizations are striving to further enhance and increase the online services to provide quality and effective services that meets the citizens' expectations in a timely manner, regardless of the time and place. According to *Laporan Perkhidmatan Dalam Talian Sektor Awam* (2016), released by Malaysian Administrative and Modernization Planning Unit (MAMPU), as of August 2016, 87.50% (or 11,261 of 12,869) of Government services were available online, although the initial target was 90% by end of 2016 (MAMPU, 2016). The *Pelan Pendigitalan Penyampaian Perkhidmatan Awam* (2017), has stated that the target for the Government to achieve online services is 90% by end of 2020 (MAMPU, 2017). Besides that, the Government also aims to achieve 40% end-to-end online services and 60% Government e-Payment services by end of 2020. A recent study on information security threats encountered by data centers in the Malaysian Public Sector by Shammugam, I., Narayana Samy, G., Magalingam, P., Maarop, N., Perumal, S., & Shanmugam, B. (2021) found that 94% of the respondents stated the Malaysian Public Sector need a suitable risk assessment methodology to

effectively manage the risks and other security related challenges in their organizations.

Thus, it is imperative to have a comprehensive and systematic risk assessment approach for data centers in the Malaysian Public Sector that covers all critical ICT assets, including threats from the people, process and technology aspects with standard detailed guidelines, which can predict the potential information security threats in advance and enable to be prepared to provide a suitable response promptly, to any information security incident in order to ensure the critical ICT assets are well protected. This will establish a safe and secure ICT environment for business operations as well as ensure business and service continuity. In addition, this will also enable the organizations to ensure permanent improvement in the delivery system.

Moreover, with the advent of IoTs, e-Commerce and Big Data Analytics initiatives in Malaysia, the future business landscape will be driven by more agile and adaptable technological changes. Henceforth, the dependency on ICT and information systems will see an upward trend, making these services and systems indispensable. The dependency of ICT has become even more prevailing with the recent Covid -19 pandemic, which has forced people to stay at home and created new working norms. There is a sudden surge in the usage of ICT leading to an exponential increase in the dependency on ICT. Malaysian leaders are demanding for more government services to go online to facilitate all the necessary services and businesses transactions, setting a new target for online services at 95% or even 100% (Khoo, 2020). The Prime Minister of Malaysia expects the digitalization of government services to be more comprehensive to facilitate people to adopt the new normal work and life style (Mahalingam, 2020).

1.2 Background of The Research

This session discusses on the proposed research domain, which is the data center, the services hosted in data centers and the information security threats often faced by data centers as well as the need to for an effective risk assessment approach, which can accurately predict the potential information security faced by data centers.

1.2.1 Data Center

A data center is a facility, which acts as a central repository for all the critical ICT assets such as information, data, servers, main network equipment, application systems as well as the people and processes involved directly in an organization. The size of the data center generally depends on the size of the organization. A data center is sometimes referred as a server room, server farm, computer room, network operations center, storage area by organizations, depending on the size. A data center will typically support one or more organizations and an organization can have more than one data center. In current business environment, it is common to find some large organizations having multiple data centers at different locations and even across multiple countries and continents to help mitigate risks in the event of a disaster at any single location to ensure their business continuity. Whether an organization uses its own data center or subscribes to a cloud computing service, ultimately the ICT critical assets such as information, data, critical hardware, critical applications and other software are stored in physical data center (Jouini et al, 2015).

1.2.2 Data Center Assets

In organizations, data centers house all the critical ICT assets and operate all the IT-centric services regardless of whether the data center services are operated in-house or outsourced. The Basics of Information Security (2014) cited that in the current connected computing environment, logical assets such as information, data and systems are equally as valuable as any other physical assets such as hardware and network equipment in the data center facility. In addition, the people who are involved in the operations are also considered valuable asset as organizations cannot conduct

any business without them. Organizations can duplicate their physical and logical assets and keep backup copies of them at alternative sites in order to protect them from any form of undesirable security incident or catastrophe. However, the organizations cannot operate and maintain their heavily information technology dependent business operations without the skilled personal.

1.2.3 Data Center Services

Data centers are considered the heart of all IT-centric services. Failure or disruption of any critical assets in data center will affect the running of an organization’s business. In worst case scenario it can result in a complete halt of the services provided by an organization which can be disastrous and affect the business continuity causing monetary losses and damage to its reputation. Some of the main services provided by data centers, stated by Gusmão et al (2016) in their study are shown as in Figure 1.1.

Data center services.	
Services	Description
Website	A hosting service that allows people or companies to store their information, pictures, videos or any other content on online systems accessible via the web.
E-commerce	A service providing a technical platform with secure payment methods, purchasing and large database backend, supporting the sale of products and services through the Internet.
Database-as-a-service	A service that hosts databases in the cloud, and a viable option for businesses developing bespoke web based applications.

Figure 1.1 Data Center Services (Gusmão et al, 2016)

1.2.4 Data Center Information Security Concerns

As the ICT revolution and advancement have changed the business world, work and lifestyle tremendously, undeniably, every sector in a country is heavily

dependent on ICT. As a result, businesses and organizations across the world leverage data center infrastructure facilities like never before as the data centers serve as repositories for data storage with a variety of critical ICT assets (Munodawafa and Awad, 2018). The authors also emphasized that in recent years many organizations opted for cloud computing and although the cloud computing offers business model that encompasses many concepts, it still operates on data centers as the underlying layer. As such, the data centers in particular have become the main target of cybercrimes as all the critical ICT services such as applications, databases, websites, backups, disaster recovery services as well as all critical ICT software, hardware and invaluable information assets are hosted at data centers (Jouini, M., Rabai, L. B., and Khedri, R., 2015). Therefore, it is imperative to safeguard the data centers in order to stay relevant while ensuring business and service continuity.

Young (2016) stated that data centers have become the focus of attention and an increasing concentration of information security risks, which are driven by the popularity of virtualization and the general trend in cloud computing. Knapp, K. J., Denney, G. D., and Barner, M. E. (2011); Snedaker and Rima (2013); Gusmão, A. P., Silva, L. C., Silva, M. M., Poletto, T., and Costa, A. P. (2016); Munodawafa et al (2018) too mentioned that all disastrous information security incidents, which caused major damage and business disruptions to organizations were targeted at data centers. Among the common hazardous internal and external threats are denial of services, defacement of websites, malware attacks, critical information thefts, intrusions, unauthorised access to servers, unauthorised access to critical systems, sabotages, fires, flood and power failures (Knapp et al, 2011; Snedaker et al, 2013; Gusmão et al, 2016). These threats are generally caused by insiders, outsiders and other sources like natural disasters. As a result, managing the risks associated with data centers has obviously become a major challenge in the current cyber world. Therefore, data centers require high level security strategies covering areas such as physical, virtualization vulnerabilities and environmental exposure.

Knapp et al (2011) highlighted that factors like the growth in internet-based cloud computing and the rising volume of electronic data as well as the need for secure and affordable big-scale data storage contributed to the increasing reliance on data

centers in business society. The authors also emphasized that proper data center security is essential in order to protect data centers from both internal and external threats such as malicious human threats, human mistakes and natural disasters, especially to process and securely store huge volumes of sensitive, critical and valuable information as well as critical ICT assets. Even though the cyber security is getting more attention and priority, the security breaches and threats seem to be unavoidable and continue to be a huge challenge. As a result, the security of data centers has become an utmost concern for both the government and the ICT industry. The authors too highlighted that a data center audit report involving four prominent government organizations in US, showed that ultimately, all findings were related to risk management and failure to conduct comprehensive risk assessments. Their findings also suggested that risk assessments were not implemented effectively in data centers, even in developed and advanced countries like the US (Knapp et al, 2011). As such, it is imperative for organizations to take the necessary steps to ensure their data centers are secure and reliable.

1.2.5 Need for An Effective Risk Assessment Methodology for Data Center

In view of the recurring and increasing ICT security threats involving data centers in various forms and from various unknown sources, it is crucial for organizations to identify the potential threats comprehensively in a systematic manner. This is to implement the necessary preventive measures to safeguard all the critical ICT assets from any disastrous damage such as the loss of sensitive and critical information, unavailability of critical systems and information, damage to hardware and software, and most importantly the loss of the client confidence and reputation of the organizations.

Nazareth and Choi (2015) stressed that securing ICT assets is of critical importance for organizations, hence, organizations need to invest adequately in ICT security efforts and initiatives such as attack prevention, vulnerability reduction, and threat deterrence to ensure effective information security management. Srinivas, Das, and Kumar (2019) too emphasized that it is crucial to protect various essential services and infrastructure such as critical national infrastructure, systems and data to overcome

the growing cyber security threats which can have adverse implications on consumer confidence, public protection as well as economic growth.

Jouini et al (2015) stated that information security is the most challenging aspect of information processing. Business organizations, governments, and individuals face many information security risks, which can cause serious damage that might lead to significant financial losses, breach of the confidentiality of sensitive information, loss of integrity and lack of availability of sensitive data. Thus, better identification, understanding, and assessment of security threats and their characteristics is crucial to facilitate the effective protection of information (Jouini et al, 2015). Shamala, P., Ahmad, R., and Yusoff, M. (2013) mentioned that information security risk assessments enable the government and private organizations to identify their security risks as well as provide a measured and analysed security profile of critical information assets in order to develop effective and economically viable strategies to keep the risks under control.

Currently, although there are numerous risk assessment methods available, selecting a suitable method that would best fit an organization has become a challenge to many organizations of different sizes (Saleh and Alfantookh, 2011; Shamala et al, 2013; Sokratis, 2013; Shameli-Sendi, A., Aghababaei-Barzegar, R., and Cheriet, M., 2016; Shamala, Ahmad, Zolait, and Sedek, 2017).

Most of the methodologies use the qualitative or hybrid approaches, which have many weaknesses such as inaccuracies in analysis and evaluation values, non-automated or repeatable processes. This is also due to the disadvantages and challenges posed by the quantitative assessment methods, such as involving considerable initial information gathering activities, difficulty in obtaining the required data, requiring tedious and repetitive effort if done manually without automated tools, involving complex calculations, as well as insufficient scientifically collected and analysed data (Goh, 2008; Ryan, J. J., Mazzuchi, T. A., Ryan, D. J., Cruz, J. L., and Cooke, R., 2012; Gusmão et al, 2016; Shameli-Sendi et al, 2016). The current standards such as ISO31000:2018-Risk Management Principles and Guidelines and ISO27002:2013-Information Technology Security Techniques Code of practice for information

security controls Requirements by International Organization for Standardization (ISO) too hardly consider quantitative methods (Ni, S., Zhuang, Y., Gu, J., and Huo, Y., 2016) due to the challenges post by quantitative analysis. Thus, this study proposes risk assessment approach using a quantitative technique to overcome the major concerns of the past researchers, citing that most of the current methodologies only apply qualitative or hybrid approaches and also to address the challenges in applying the quantitative analysis.

Olechowski, A., Oehmen, J., Seering, W., and Ben-Daya, M. (2016) cited that previous studies tend to cover different methods and sets of tools, but lack standardization as well as collection of best practices from the available methods. Thus, a systematic method with standard guidelines is needed to identify, assess, control and monitor all potential threats and associated risks effectively. This will also enable enterprises to implement risk management proactively without much hassle in order to protect their critical ICT assets.

Zeng and Koutny (2019) stated that traditionally, information security research has been focused solely on the products and technology such as the architecture of the system, access controls policies and the functionality of the products. The authors have emphasized that the human aspect which has been identified as one of the critical factors must be taken into account in ensuring the effectiveness of security measures. Thus, it is important to implement a comprehensive risk assessment approach that covers all aspects, including the people, process and technology in order to create an effective information security system in an organization.

As a result of growing security threats targeting data centers and demands for reliable online services, it is imperative for organizations to stay ahead of threats to ensure business and service continuity as well as stay relevant in the competitive business environment. Hence, it is time to rethink security strategies and establish strong information security risk management through a comprehensive and systematic risk assessment approach, as the risk assessment phase is the heart of risk management.

This study adopted the medical research design and survival analysis technique taking into consideration the many advantages of the medical research design as mentioned in Section 3.7.4.2 of Chapter 3, to overcome the shortcomings and weaknesses in the traditional risk assessment methods in the computing environments. Medical science is one of the oldest fields in the world and it has its own approach and method to conduct researches and data analysis. The survival analysis technique, which often applied in medical research design is proven to be very effective for prognostic purposes. Survival analysis is considered as the most efficient method in predicting expected hazards based on the available historical data and provides precise results compared to other methods. Currently, the survival analysis technique is not only applied in the medical field but also in many other fields such as engineering, oil and gas, social sciences and information security to assess certain events of interest and their trends (Ma and Krings, 2008; Samy, 2011; Kleinbaum et al, 2012; Sameer, 2016; Kong Fah Tee, Konstantinos Pesinis, and Tahani Coolen-Maturi, 2019). Therefore, it is time this proven and most efficient technique is applied in the Malaysian Public Sector data center environments, to effectively thwart the increasing information security threats and challenges that they encounter daily.

1.3 Problem Statement

A comprehensive and systematic risk assessment approach is crucial for organizations in this cyber era as information security threats are ubiquitous and can come from anywhere, at any time and in any form. Securing the critical ICT assets and ensuring information security has become a major challenge and critical importance for organizations as they are increasingly becoming dependent on ICT. In view of the increasing cyber threats, the Malaysian Public Sector must protect the critical ICT assets, primarily hosted in data centers as well as the people and processes involved directly. As data centers, which host all the critical ICT assets becoming the main target of cybercrimes, it is crucial for organizations to identify the potential information security threats and related risks comprehensively and systematically, covering all the technology, people and process aspects. Therefore, the organizations need a risk assessment approach that can identify or predict the threats effectively and

analyse the associated risks accurately. However, selecting a suitable risk assessment approach out of the numerous currently available methodologies is a challenge as the majority only provide very high level guidelines and most do not use the quantitative analysis approach, which can assess the risks more precisely. The qualitative or hybrid analysis risk assessment methods are mostly done based on interviews and brainstorming activities with stakeholders in ad-hoc manners. In these methods, the security risk levels are evaluated based on the experts' experience, opinions, awareness of the company staff as well as environment and estimation of the security risk impact and probability, as such, these factors may influence and affect the accuracy of the expert evaluations and do not give accurate results. Besides that, these qualitative or hybrid approaches are tedious, need more resources and time consuming. Thus, this research aims to develop a comprehensive and systematic risk assessment method, covering all critical ICT assets with standardised detailed guidelines, using a quantitative risk analysis technique to effectively identify, analyse and evaluate the potential risks faced by organizations in the Malaysian Public Sector. For this purpose, the study will employ the medical research design approach and Cox Proportional Hazard (PH) model using the Counting Process (CP) layout format under the survival analysis quantitative technique to effectively identify or predict the potential information security threats, analyse and evaluate the related risks accurately in the Malaysian Public Sector data centers environment. The required historical data was collected through observation using retrospective cohort study and the risk analysis was automated using software solution.

1.4 Research Questions

This study was guided by the following research questions:

- (a) What are the information security threats encountered by the data center environments in the Malaysian Public Sector?
- (b) How to adopt a risk assessment method using quantitative technique to effectively identify potential information security threats, analyse and evaluate

the associated risks in the Malaysian Public Sector data center environment and validate the proposed risk assessment method?

- (c) What are the relevant guidelines for the proposed risk assessment method using the quantitative technique?

1.5 Research Objectives

Based on the research questions, the objectives of this research are as follows:

- (a) To identify the information security threats faced by data centers in the Malaysian Public Sector organizations.
- (b) To propose, apply, and validate a risk assessment method adopting medical research design approach and survival analysis technique to effectively identify the potential information security threats and analyse the associated risks in the Malaysian Public Sector data center environment.
- (c) To propose relevant guidelines for information security practitioners, risk analysts and those who are involved in managing data center security based on the proposed information security risk assessment method.

1.6 Research Scope

The research scope covers the following areas:

- (a) The research focused on various existing risk assessment methodologies by professional bodies, international best practices for risk management, methods by previous researchers as well as the medical research design, which is relevant to the study.

- (b) For the medical research design approach, the research focused by adopting retrospective cohort study to identify the threats that normally occur in data center environments. For risk assessment and to predict potential information security threats in future, the Cox PH model under the survival analysis method was adopted. The research applied the Counting Process layout format under Cox PH model, which allows multiple data lines as the data collected showed recurrent events for the same subjects or entity observed.
- (c) The research also focused on two international standards related to information security, which are relevant to this study. The proposed information risk assessment complies with information security risk management framework stated in the ISO27005:2018-Information Security Risk Management international standard, which supports the general concepts specified on information security management and the ISO27001:2013-Information Security Management System (ISMS), which is the only international standard intended for information security certification purpose (ISO, 2013a; 2018b). This is to enable the Public Sector Organizations to certify their data centers to the requirement of ISMS standard as per the Malaysian Government's directive, particularly meeting the requirement of the risk assessment and overall risk management.
- (d) For qualitative data collection, the research focused on the information security threats that currently occur in Malaysia and worldwide.
- (e) For quantitative data collection and to apply and validate the viability and effectiveness of the proposed risk assessment method using quantitative technique, the research was conducted at a data center in one of the prominent organizations in the Malaysian Public Sector. The approach covered detailed processes in assessing risks, the various elements and attributes involved in the risk assessment process and risk management related to data centers in the Malaysian Public Sector.

1.7 Significance of The Study

The following section discusses the significance and contributions of the research.

1.7.1 Theoretical Significance

This study will significantly contribute to increasing the knowledge in the area of risk management principles and guidelines, especially in risk assessment of information security. The thesis deliberates various aspects of information security and risk assessment. Besides that, many theories and concepts involving risk assessment, in particular, and risk management, in general, too are discussed in detail. In addition, the study has identified, scrutinized and deliberated many existing risk assessment methodologies and best practices relevant to information security risk assessment in the course of this research. This provides detailed insights into available risk assessment practices and enhances the knowledge of those who wish to select and implement a suitable risk assessment approach for their organizations. The strengths and weaknesses of both the quantitative and qualitative risk analysis approaches explored in this thesis will be invaluable to risk practitioners and those who are involved in information security risk assessment and risk management. The detailed risk assessment guidelines given will enhance the knowledge of data center managers in assessing and managing information security risks effectively in order to reduce the potential damage and loss. Thus, theoretically, this research will contribute to the body of knowledge in the risk assessment field.

1.7.2 Methodological Significance

- i) The study will significantly contribute in identifying and predicting the potential threat effectively by adopting the medical research design approach and survival analysis technique. The Cox PH model using the CP layout format under survival analysis, which was applied in this

study, used in more complicated situations and able to analyse data on recurrent events by allowing multiple lines of data for the same subject or entity observed. Thus, the CP layout format will predict the potential threats more accurately as compared to the General layout format, which only allows one line of data for each subject observed and is only used for simple and straight forward situations. According to Cox (1972); Samy (2011); Sameer (2016), the CP method is more dynamic and accurate in predicting the information security threats. Therefore, it is a suitable method as recurrent events for the same subjects are common phenomena in the data center environment in the Malaysian Public Sector.

- ii) Another significant contribution of this research is the proposed standard detailed guidelines to carry out the risk assessment approach systematically. The standard detailed risk assessment guidelines proposed will assist in identifying the potential risks systematically in a proactive manner without much hassle, thus, enabling the assessment of the risks, severity of the adverse impacts as well as planning and implementation of the required mitigation or preventative controls. This proposed risk assessment approach will allow the Public Sector organizations to keep the identified risks under control and minimize the adverse impacts to ensure their ICT assets are well protected and secured at all times. This will also ensure that all business and service delivery can be conducted safely in a secured environment, hence, increase the clients' and investors' confidence, and gives a good return for the investment made by the Malaysian Government.

1.7.3 Practical Significance

- i) The study will effectively identify the various types of threats that are commonly encountered by the data centers in the Malaysian Public Sector. This will give a greater degree of awareness and understanding of the threats to the ICT security officers, who are entrusted with data

center security. The public sector organizations will be able to implement the necessary controls to better prevent any information security threats and disruptions to services delivered through ICT. This is very crucial, especially now when the demand for secure and timely services necessitates the Public Sector organizations in Malaysia be innovative and creative in providing services regardless of the geographical position.

- ii) Aligned with the Malaysian Government's aim to safeguard Critical National Information Infrastructure (CNII) and to improve service delivery to the public, the Public Sector will also be able to optimize the services rendered through ICT. Thus, the Malaysian Public Sector organizations will be able to meet the ever increasing demand for effective and efficient services. This will also improve customer confidence and safeguard the image and reputation of the Malaysian Public Sector.
- iii) Risk Assessment is one of the seven major processes involved in business continuity and disaster recovery planning. Therefore, the establishment of a risk assessment using the quantity approach will help in the effective implementation of business continuity and disaster recovery plans in the Malaysian Public Sector organizations.
- iv) Besides that, it will also contribute in enhancing the existing Malaysia Public Sector Information Security Risk Assessment Methodology (MyRAM) currently used by the Malaysian Public Sector organizations by providing an alternative approach using a quantitative risk analysis method.

1.8 Organization of Thesis

This thesis comprises of the following six chapters.

Chapter 1 gives the overview and purpose of the proposed study. It briefly discusses the background of the problem, which explains the need for a comprehensive and systematic risk assessment with detailed guidelines, covering all critical assets hosted in data centers in the Malaysian Public Sector organisations. The chapter also briefly covers the domain of the study, which is the data center with an emphasis on the critical assets and services hosted in data centers as well as the security threats related to data centers. It also describes the problem statement explaining the need for this study. Besides that, it illustrates the research questions, objectives and scope with the expected outcome and output as well as the significant contributions of the research. Finally, this chapter outlines the organization of this thesis.

Chapter 2 explains the important terms, theories, and concepts in risk management as defined by various schools of thought and risk management professionals and justifies the purpose of the proposed study. It also analyses and compares the various available risk management methodologies and risk assessment approaches as well as deliberates on the existing published research in this field, highlighting the issues raised by previous researchers related to risk assessment. The chapter also discusses the research design and method selected for the study as well as the justifications and applications of the chosen approach by previous researchers. Finally, it highlights the issues in the suggested research area and explains the gaps found in it.

Chapter 3 describes the methodologies to achieve the objectives of the study. The selected methodology and most suitable research strategy identified for this study are described and the research design is presented to explain how the proposed risk assessment adopting the medical research design approach using the survival analysis technique will be developed. The chapter also discusses the research procedure, phases, activities involved in each phase and outputs through an operational framework. The research method adopted and the relevant justifications, as well as the

instruments used, data collection and analysis procedure, sampling type and target population, were also elaborated. Finally, it explains the assumptions of the methodology.

Chapter 4 presents in detail the proposed risk assessment adopting the medical research design approach using the survival analysis technique for data centers in the Malaysian Public Sector. It discusses how the proposed risk assessment approach in this study is incorporated into the information security risk management framework as in the ISO27005. It also describes the characteristics of the proposed risk assessment and deliberates on the justifications. The chapter illustrates the differences in risk assessment processes between the traditional approach and the proposed approach using the medical research design and survival analysis technique. Finally, the chapter explains the proposed standard detailed activities as guidelines in each phase of risk management, namely the Establish Context, Risk Identification, Risk Analysis, Risk Evaluation, Risk Treatment, Risk Monitoring and Review and Risk Communication and Consultation to facilitate effective implementation of risk assessment in particular and overall risk management.

Chapter 5 discusses in detail the analysis results of this study. It discusses the findings of both qualitative and quantitative data collected and analysed in the preliminary data collection, context establishment and risk identification phases. The chapter also deliberates the results of the risk evaluation phase based on the results obtained from the previous analysis phase. The chapter also briefly reflects the risk treatment, risk monitoring and review, and risk communication and consultation phases. Finally, it explains the methods applied to validate the survival analysis quantitative technique and reports the outcomes.

Chapter 6 provides the conclusion of this research work. It summarizes the research findings and reflects how the research objectives were achieved based on the research questions formulated. It also highlights the contributions of this research. The chapter also discusses the limitations of this research and proposes future work. Finally, it summarizes the chapter.

REFERENCES

- Almut Dutz., & Steffen Lock. (2019). Radiotherapy and Oncology. *ScienceDirect*, 130, 185-189.
- Andrade, R. O., & Yoo, S. G. (2019). Cognitive security: A comprehensive study of cognitive science in cybersecurity. *Journal of Information Security and Applications*, 48, 102352.
- Antoniadis, A., & Grégoire, G. (1993). Nonparametric estimation in change point hazard rate models for censored data: A counting process approach. *Journal of Nonparametric Statistics*, 3(2), 135-154.
- AS/NZS International Organization for Standard (2009). Risk Management-Principles and Guidelines (AS/NZS 31000:2009).
- AS International Organization for Standard (2018). Risk Management-Principles and Guidelines (AS ISO 31000:2009).
- Aven, T. (2012). The risk concept—historical and recent development trends. *Reliability Engineering & System Safety*, 99, 33-44.
- Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research*, 253(1), 1-13.
- Baiardi, F., Corò, F., Tonelli, F., & Sgandurra, D. (2014). Automating the assessment of ICT risk. *Journal of Information Security and Applications*, 19(3), 182-193.
- Bernama. (2020, September 8). Spike in cyber threats; fraud tops list. *New Straits Times*. Retrieved February 1, 2021, from <https://www.nst.com.my/news/nation/2020/09/622861/spike-cyber-threats-fraud-tops-list>.
- Bhattacharjee, J., Sengupta, A., & Mazumdar, C. (2013). A formal methodology for Enterprise Information Security risk assessment. *2013 International Conference on Risks and Security of Internet and Systems (CRiSIS)*.
- Boehm BW. Software Risk Management: Principles and Practices, IEEE Software, 1991.
- Bryman, A. (2012) *Social research methods*. Oxford university press.

- Burdon, M., & Coles-Kemp, L. (2019). The significance of securing as a critical component of information security: An Australian narrative. *Computers & Security*, 87, 101601.
- Chapman C, Ward S. (1997) Project Risk Management: Processes, Techniques and Insights. John Wiley.
- Chapter1, What is Information Security? (2014). In *The Basics of Information Security* (pp. 1-22). Elsevier.
- Cyber Security Malaysia (2016). Available:
<http://cnii.cybersecurity.my/main/about.html>
- COBIT 5 ISACA's new framework for IT Governance, Risk, Security and Auditing (Publication). (2013). Retrieved September 20, 2016.
- Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches*. Thousand Oaks: Sage.
- Creswell, J. W., & L., P. Clark. (2011). *Designing and conducting mixed methods research* (2nd ed.). Los Angeles: SAGE.
- David G. Kleinbaum Mitchel Klein. (2012). *Survival Analysis, A Self-Learning Text* (3rd ed.). New York: Springer)
- Dorofee, A. J. (1996). *Continuous risk management guidebook*. Pittsburgh, PA: Carnegie Mellon University.
- Dudovskiy, J. (2016). *The Ultimate Guide to Writing a Dissertation in Business Studies: A Step-by-Step Assistance* [E-book]. Available at: <http://research-methodology.net/about-us/ebook/> (Accessed: 31 December 2019).
- Economic Planning Unit, Prime Minister Department, Malaysia (2016). Rancangan Malaysia Ke-11. Available: <http://rmk11.epu.gov.my/index.php>.
- EY's Global Information Security (2013). Insights on governance, risk and compliance. Retrieved September 25, 2016, from <http://www.ey.com/GL/en/Services/Advisory/IT/IT-risk-library-page>.
- Fazlida, M., & Said, J. (2015). Information Security: Risk, Governance and Implementation Setback. *Procedia Economics and Finance*, 28, 243-248.
- Feng, N., & Li, M. (2011). An information systems security risk assessment model under uncertain environment. *Applied Soft Computing*, 11(7), 4332-4340.
- Firoozjaei, M. D., Jeong, J., Ko, H., & Kim, H. (2016). Security challenges with network functions virtualization. *Future Generation Computer Systems*.

- Flowerday, S. V., & Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who. *Computers & Security*, *61*, 169-183.
- FMT Reporters. (2021, February 18) Anonymous 11 are found out by the cops. *Free Malaysia Today*. Retrieved February 18, 2021, from <https://www.freemalaysiatoday.com/category/nation/2021/02/18/anonymous-11-are-found-out-by-the-cops>.
- Gantz, S. D. (2014). *The basics of IT audit: Purposes, processes, and practical information*. Elsevier. (Chapter7 – IT Audit Drivers)
- Goh, M. H. (2008). *Analyzing & reviewing the risks for business continuity planning*. Singapore: GMH Pte.
- Goh, M. H. (2013). *BCMpedia: Dictionary of business continuity and disaster recovery*.
- Government of United Kingdom (2016). National Security Strategy and Strategic Defence and Security Review 2015. Available: <https://www.gov.uk/government/publications/national-security-strategy-and-strategic-defence-and-security-review-2015>.
- Gunasekaran, A., Irani, Z., Choy, K., Filippi, L., & Papadopoulos, T. (2015). Performance measures and metrics in outsourcing decisions: A review for research and applications. *International Journal of Production Economics*, *161*, 153-166.
- Gusmão, A. P., Silva, L. C., Silva, M. M., Poletto, T., & Costa, A. P. (2016). Information security risk analysis model using fuzzy decision theory. *International Journal of Information Management*, *36*(1), 25-34.
- Hammersley, M. (2013) *What is Qualitative Research? (The “What is?” Research Methods Series)* (1st edn.). Bloomsbury Academic.
- Huai, J. (2012). Apply TQM to E-Government Outsourcing Management. *Physics Procedia*, *24*, 1159-1165.
- International Organization for Standardization (2004). Information Technology – Security techniques – Management of Information and Communications Technology Security (ISO/IEC 13335-1:2004).
- International Organization for Standardization (2009). Risk Management-Vocabulary (ISO Guide 73:2009).

- International Organization for Standardization (2011). Information technology- Security Techniques-Information security risk management (ISO/IEC 27005:2011).
- International Organization for Standardization (2013a). Information Technology – Security Techniques – Information Management Systems – Requirements (ISO/IEC 27001:2013).
- International Organization for Standardization (2013b) Information Technology – Security Techniques – Code of practice for information security controls – Requirements (ISO/IEC 27002:2013).
- International Organization for Standardization (2014). Information technology – Security techniques – Information security management systems (ISO/IEC 27000:2014).
- International Organization for Standardization (2018a). Risk Management-Principles and Guidelines (ISO/IEC 31000:2018)
- International Organization for Standardization (2018b). Information technology- Security Techniques-Information security risk management (ISO/IEC 27005:2018).
- International Organization for Standardization (2019). Medical devices – Application of risk management to medical devices (ISO 14971:2019).
- Islam, S., Mouratidis, H., & Weippl, E. R. (2014). An empirical study on the implementation and evaluation of a goal-driven software development risk management model. *Information and Software Technology*, 56(2), 117-133.
- IT Outsourcing (2014). [online]: The reasons, Risks, Rewards. Available: <http://www.corpcomputersevice.com/articles/outsourcing-reason>.
- Jørgensen, M. (2014). Failure factors of small software projects at a global outsourcing marketplace. *Journal of Systems and Software*, 92, 157-169.
- Jouini, M., Rabai, L. B., & Aissa, A. B. (2014). Classification of Security Threats in Information Systems. *Procedia Computer Science*, 32, 489-496.
- Jouini, M., Rabai, L. B., & Khedri, R. (2015). A Multidimensional Approach towards a Quantitative Assessment of Security Threats. *Procedia Computer Science*, 52, 507-514.
- Jouini, M., & Rabai, L. B. (2016). Comparative Study of Information Security Risk Assessment Models for Cloud Computing systems. *Procedia Computer Science*, 83, 1084-1089.

- Kartsonaki, C. (2016). Survival analysis. *Diagnostic Histopathology*, 22(7), 263-270.
- Kearney, W., & Kruger, H. (2016). Can perceptual differences account for enigmatic information security behaviour in an organisation? *Computers & Security*, 61, 46-58.
- Kendrick, T. (n.d.). *Identifying and managing project risk: Essential tools for failure proofing your project*. New York : AMACOM, 2015. (third edition)
- Khidzir, N. Z., Mohamed, A., & Arshad, N. H. (2013). ICT Outsourcing Information Security Risk Factors: An Exploratory Analysis of Threat Risks Factor for Critical Project Characteristics. *Journal of Industrial and Intelligent Information JIII*, 1(4), 218-222.
- Khoo, D. (2020, May 21). All public services to go online. Retrieved from <https://www.thestar.com.my/business/business-news/2020/05/21/all-public-services-to-go-online>.
- Kliem, R. L., & Ludin, I. S. (1997). *Reducing project risk*. Aldershot, England: Gower.
- Knapp, K. J., Denney, G. D., & Barner, M. E. (2011). Key issues in data center security: An investigation of government audit reports. *Government Information Quarterly*, 28(4), 533-541.
- Komljenovic, D., Gaha, M., Abdul-Nour, G., Langheit, C., & Bourgeois, M. (2016). Risks of extreme and rare events in Asset Management. *Safety Science*, 88, 129-145.
- Kong Fah Tee, Konstantinos Pesinis, Tahani Coolen-Maturi. (2019). Competing risks survival analysis of ruptured gas pipelines: A nonparametric predictive approach. *International Journal of Pressure Vessels and Piping*, 175, 103919.
- Kumar, R. (2019) *Research Methodology: A Step-by-Step Guide for Beginners*. (5th edn.). SAGE Publications Ltd.
- Larionovs, A., Teilans, A., & Grabusts, P. (2015). CORAS for Threat and Risk Modeling in Social Networks. *Procedia Computer Science*, 43, 26-32.
- Law, J. (2019, August 30). Malaysian Websites Experience Increased Amount of Cyber Attacks Leading To Merdeka Day. Retrieved September 1, 2019, from <https://www.lowyat.net/2019/192983/malaysian-website-cyber-attack-merdeka-day>.
- Lee, E. T. and Wang, J. (2003). *Statistical Methods for Survival Data Analysis*. (3rd ed.). Wiley & Sons, Inc, Canada.

- Lehto, M. (2016). Cyber Security Education and Research in the Finland's Universities and Universities of Applied Sciences. *International Journal of Cyber Warfare and Terrorism*, 6(2), 15-31.
- Li-yong Zheng, Yun-tao Chang. Risk assessment model of bottlenecks for urban expressways using survival analysis approach. World Conference on Transport Research – WCTR 2016 Shanghai. 10-15 July 2016. ScienceDirect, Procedia
- Li, Z., Yang, S., & Li, Z. (2016). Overview of Risk Management System of Commercial Bank Data Center. *IJSIA International Journal of Security and Its Applications*, 10(3), 245-258.
- Liu, S., & Wang, L. (2014). Understanding the impact of risks on performance in internal and outsourced information technology projects: The role of strategic importance. *International Journal of Project Management*, 32(8), 1494-1510.
- Mahalingam, S. a/l. (2020, April 25). New normal needs a more comprehensive digitalisation system, says PM. Retrieved from <https://www.thestar.com.my/news/nation/2020/04/25/new-normal-needs-a-more-comprehensive-digitalisation-system-says-pm>.
- Malaysian Administrative Modernization and Planning Unit, (2016). *Laporan Perkhidmatan Dalam Talian Sektor Awam* (2016).
- Malaysian Administrative Modernization and Planning Unit (2017). *The Pelan Pendigitalan Penyampaian Perkhidmatan Awam* (2017).
- Malaysian Administrative Modernization and Planning Unit (2005). *The Malaysia Public Sector Information Security Risk Assessment Methodology* (2005)
- Managing successful projects with PRINCE2*. (2009). London: TSO.
- Miles, M. B., Huberman, A. M., & Saldaña, J. (2018). *Qualitative data analysis: A methods sourcebook*. Sage publications.
- Mohamed, D. B. (2013). Combating the threats of cybercrimes in Malaysia: The efforts, the cyberlaws and the traditional laws. *Computer Law & Security Review*, 29(1), 66-76.
- Moon, J., Lee, C., Park, S., Kim, Y., & Chang, H. (2016). Mathematical model-based security management framework for future ICT outsourcing project. *Discrete Applied Mathematics*.
- Munodawafa, F., & Awad, A. I. (2018). Security risk assessment within hybrid data centers: A case study of delay sensitive applications. *Journal of Information Security and Applications*, 43, 61–72.

- Ministry of Communication and Multimedia Malaysia (2016). National Cyber-Security Policy (NCSP). Available: <http://nitc.kkmm.gov.my/index.php/national-ict-policies/national-cyber-security-policy-ncsp>.
- Nazareth, D. L., & Choi, J. (2015). A system dynamics model for information security management. *Information & Management*, 52(1), 123-134.
- Ni, S., Zhuang, Y., Gu, J., & Huo, Y. (2016). A formal model and risk assessment method for security-critical real-time embedded systems. *Computers & Security*, 58, 199-215.
- National Institute of Standards and Technology (2016). NIST Special Publication 800-53. Retrieved October 02, 2016, from https://en.wikipedia.org/wiki/NIST_Special_Publication_800-53
- Noordzij, M., Leffondre, K., Stralen, K. J. V., Zoccali, C., Dekker, F. W., & Jager, K. J. (2013). When do we need competing risks methods for survival analysis in nephrology? *Nephrology Dialysis Transplantation*, 28(11), 2670–2677.
- Olavsrud, T. (2016, September 22). How to protect your mission-critical information. [online]. Available at: <http://www.cio.com/article/3122834/security/how-to-protect-your-mission-critical-information.html>. (Access: 25 September 2016).
- Olechowski, A., Oehmen, J., Seering, W., & Ben-Daya, M. (2016). The professionalization of risk management: What role can the ISO 31000 risk management principles play? *International Journal of Project Management*,
- Patanakul, P., Kwak, Y. H., Zwikael, O., & Liu, M. (2016). What impacts the performance of large-scale government projects? *International Journal of Project Management*, 34(3), 452-466.
- Prasetyo, S., & Sucahyo, Y. G. (2014). Information security risk management planning: A case study at application module of state asset directorate general of state asset ministry of finance. *2014 International Conference on Advanced Computer Science and Information System*.
- Prentice, R. L., Williams, B. J., & Peterson, A. V. (1981). On the regression analysis of multivariate failure time data. *Biometrika*, 68(2), 373-379.
- Rahimian, F., Bajaj, A., & Bradley, W. (2016). Estimation of deficiency risk and prioritization of information security controls: A data-centric approach. *International Journal of Accounting Information Systems*, 20, 38-64.

- Reuters. (2017, June 27). Cyber attack sweeps globe, researchers see WannaCry link: *New Straits Times*. Retrieved July 1, 2017, from <https://www.nst.com.my/world/2017/06/252553/cyber-attack-sweeps-globe-researchers-see-wannacry-link>.
- Röhrig, B., du Prel, J. B., Wachtlin, D. and Blettner, M. (2009). Types of Study in Medical Research- Part 3 of a Series on Evaluation of Scientific Publications. *Deutsches Arzteblatt International*. 106(15), 262-268.
- Runeson, P., & Höst, M. (2009). Guidelines for conducting and reporting case study research in software engineering. *Empirical software engineering*, 14(2), 131-164.
- Ryan, J. J., Mazzuchi, T. A., Ryan, D. J., Cruz, J. L., & Cooke, R. (2012). Quantifying information security risks using expert judgment elicitation. *Computers & Operations Research*, 39(4), 774-784.
- Saleh, M. S., & Alfantookh, A. (2011). A new comprehensive framework for enterprise information security risk management. *Applied Computing and Informatics*, 9(2), 107-118.
- Sameer Hasan Saif Qaid. (2016) *Security Risk Assessment Framework for Cloud Computing Environment Using Survival Analysis Method*. PhD Thesis. Universiti Teknologi Malaysia.
- Samy, G. N., Ahmad, R. and Ismail, Z. (2010). A Framework for Integrated Risk Management Process using Survival Analysis Approach in Information Security. *2010 Sixth International Conference on Information Assurance and Security*. Atlanta, GA: IEEE, 185-190.
- Samy, G. N., Ahmad, R. and Ismail, Z. (2012). *Adopting and Adapting Medical Approach in Risk Management Process for Analysing Information Security Risk*. in Emblemsvåg, J. *Risk Management for the Future Theory and Cases*. INTECH Open Access Publisher; 368-388.
- Samy, G. N. (2012) *Analysing Information Security Threats in Healthcare Information Systems Using Survival Analysis Method*. PhD Thesis. Universiti Teknologi Malaysia.
- Sarkar, K. R. (2010). Assessing insider threats to information security using technical, behavioural and organisational measures. *Information Security Technical Report*, 15(3), 112-133.

- Saunders, M. N., Saunders, M., Lewis, P., & Thornhill, A. (2011) *Research methods for business students*. 5th edn. Pearson Education India.
- Schilling, A., & Werners, B. (2016). Optimal selection of IT security safeguards from an existing knowledge base. *European Journal of Operational Research*, 248(1), 318-327.
- Shamala, P., Ahmad, R., & Yusoff, M. (2013). A conceptual framework of info structure for information security risk assessment (ISRA). *Journal of Information Security and Applications*, 18(1), 45-52.
- Shamala, P., Ahmad, R., Zolait, A., & Sedek, M. (2017). Integrating information quality dimensions into information security risk management (ISRM). *Journal of Information Security and Applications*, 36, 1–10.
- Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). *Computers & Security*, 57, 14-30.
- Shammugam, I., Narayana Samy, G., Magalingam, P., Maarop, N., Perumal, S., & Shanmugam, B. (2021). Information security threats encountered by Malaysian public sector data centers. *Indonesian Journal of Electrical Engineering and Computer Science*, 21(3), 1820-1829. doi:<https://doi.org/10.11591/ijeecs.v21.i3>
- Silva, M. M., Gusmão, A. P., Poletto, T., Silva, L. C., & Costa, A. P. (2014). A multidimensional approach to information security risk management using FMEA and fuzzy theory. *International Journal of Information Management*, 34(6), 733-740.
- Sipayung, J. J., & Sembiring, J. (2015). Risk assessment model of application development using Bayesian Network and Boehm's Software Risk Principles. *2015 International Conference on Information Technology Systems and Innovation (ICITSI)*.
- Snedaker, S., & Rima, C. (2013). *Business continuity and disaster recovery planning for IT professionals*.
- Sokratis K. Katsikas (2013). Chapter 53, Risk Management. In *Computer and Information Security Handbook* (pp. 905-927). Elsevier.
- Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems*, 92, 178–188.

- S. Sreejesh and Sanjay Mohapatra (2013) *Mixed Method Research Design: An Application in Consumer-Brand Relationships (CBR)*. 1st edn. Springer International Publishing.
- Staalduinen, M. A., Khan, F., Gadag, V., & Reniers, G. (2017). Functional quantitative security risk analysis (QSRA) to assist in protecting critical process infrastructure. *Reliability Engineering & System Safety*, 157, 23-34.
- Standards Australia (2009). Risk Management – Principles and Guidelines (AS/NZS ISO 31000:2009). Homebush, NSW: Standards Australia.
- Stephanie, M. (2011, September 9). *How To Mitigate Risk in an Overheated Outsourcing Market*. [Www.Cio.Com](http://www.cio.com) [online]. Available: <https://www.cio.com/article/2404617/how-to-mitigate-risk-in-an-overheated-outsourcing-market.html> (Accessed: 10 October 2017).
- Surat Ketua Pengarah MAMPU, MAMPU.BPICT.700-4/3/5 Jld. 2(6), Panduan Keperluan Dan Persediaan Pelaksanaan Pensijilan MS ISO/IEC 27001:2007 Dalam Sektor Awam, Jabatan Perdana Menteri, 24 November 2010.
- Syalim, A., Hori, Y., & Sakurai, K. (2009). Comparison of Risk Analysis Methods: Mehari, Magerit, NIST800-30 and Microsoft's Security Management Guide. *2009 International Conference on Availability, Reliability and Security*, 726-731.
- Symantec (2016). Internet Security Threat Report [online]. Available: <https://www.symantec.com/security-center/threat-report>.
- Szczepaniuk, E. K., Szczepaniuk, H., Rokicki, T., & Klepacki, B. (2020). Information security assessment in public administration. *Computers & Security*, 90, 101709.
- Tariq, Q. (2019, September 13). CyberSecurity Malaysia: Watch out for cyberattacks ahead of Malaysia Day. *The Star*. Retrieved September 13, 2019, from <https://www.thestar.com.my/tech/tech-news/2019/09/13/cybersecurity-malaysia-watch-out-for-cyberattacks-ahead-of-malaysia-day>.
- Tashakkori, A., & Teddlie, C. (2010) *Sage handbook of mixed methods in social & behavioral research*. Sage.
- Thekdi, S., & Aven, T. (2016). An enhanced data-analytic framework for integrating risk management and performance management. *Reliability Engineering & System Safety*, 156, 277-287.

- Torabi, S. A., Giahi, R., & Sahebjamnia, N. (2016). An enhanced risk assessment framework for business continuity management systems. *Safety Science*, 89, 201-218.
- Vernon Gayle and Paul Lambert (2018) *The “What is?” Research Methods Series*. 1st edn. Bloomsbury Academic.
- Vicente, E., Mateos, A., & Jiménez-Martín, A. (2014). Risk analysis in information systems: A fuzzification of the MAGERIT methodology. *Knowledge-Based Systems*, 66, 1-12.
- Vrhovec, S. L., Hovelja, T., Vavpotič, D., & Krisper, M. (2015). Diagnosing organizational risks in software projects: Stakeholder resistance. *International Journal of Project Management*, 33(6), 1262-1273.
- Webb, J., Ahmad, A., Maynard, S. B., & Shanks, G. (2014). A situation awareness model for information security risk management. *Computers & Security*, 44, 1-15.
- Wickboldt, J. A., Bianchin, L. A., Lunardi, R. C., Granville, L. Z., Gasparly, L. P., & Bartolini, C. (2011). A framework for risk assessment based on analysis of historical information of workflow execution in IT systems. *Computer Networks*, 55(13), 2954-2975.
- Young, C. S. (2016). Data Centers: A Concentration of Information Security Risk. *Information Security Science*, 339–357.
- Zhang, L., Wang, Q., & Tian, B. (2013). Security threats and measures for the cyber-physical systems. *The Journal of China Universities of Posts and Telecommunications*, 20, 25-29.
- Zeng, W., & Koutny, M. (2019). Modelling and analysis of corporate efficiency and productivity loss associated with enterprise information security technologies. *Journal of Information Security and Applications*, 49, 102385.
- Zhiwei, Y., & Zhongyuan, J. (2012). A Survey on the Evolution of Risk Evaluation for Information Systems Security. *Energy Procedia*, 17, 1288-1294.
- Zuheros, C., Li, C. C., Cabrerizo, F. J., Dong, Y., Herrera-Viedma, E., & Herrera, F. (2018). Computing with words: Revisiting the qualitative scale. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 26(Suppl. 2), 127-143.

Appendix A Data Collected During Preliminary Study

I) Types of Security Incidents at PDSA Compiled by MAMPU for Year 2016 & 2017

Num.	Types of Security Incidents
2016	
1.	Website Defacement / Compromised
2.	Agencies' Server unable to communicate to PDSA's gateway
3.	An agency's Single Sign On application cannot be accessed at PDSA
4.	Agency's Load Balance (LB) down due to some maintenance work done on the previous day as the IP connection to LB failed
5.	Portal / Service disruption/ unavailability
6.	All Virtual Machine in new Cluster down at PDSA
7.	Very High Network Congestion due to broadcast storm
8.	SPAM emails
9.	Failure to follow SOP. Cabling work done by an agency without PDSA's permission and the switch was not properly configured and connected to PDSA's switch
10.	Network (LAN/ WAN/ WiFi) service failure/ unavailability
11.	Very high volume packet transaction at MOA Server using Public IP
12.	Network congestion
13.	Eavesdropping (network function virtualization)
14.	Traffic sniffing
15.	IPS disruption / intermittent
16.	Firewall Services disruption / intermittent /unstable
17.	Data Center (DC) Switches disruption / intermittent
18.	Some equipment at the back of N5K (DC Switches) failed to reach the respective gateways
19.	Black hole / Packet drop attacks
20.	Direction of misleading attacks
21.	Network System at PDSA disrupted / intermittent
22.	Vulnerable code of System / Unpatched software
23.	Earthquakes/ Tremor

Num.	Types of Security Incidents
24.	Chiller System down – Heat exchange burst / high pressure gas / bearing pump broke / high water pressure
25.	Power failure at DC Control Room
26.	Network room switch accidentally disconnected
27.	Very high temperature at DC (27.8C)
28.	Power supply/failure to few racks disconnected
29.	Power trip at Miniature Circuit Breaker (MCB)
30.	Short Circuit at Circuit Breaker Power Distribution Units
31.	UPS Battery faulty / UPS down
32.	IP Server down
33.	Malware attacks
34.	Six nodes of network management system down
36.	Information Leakage
37.	Cross-site Scripting
38.	Java code injection
39.	Incoming power failure supplied by PDU
40.	Data Storage V3700 down
41.	SQL Injection attacks
42.	Incoming power supply disconnected
43.	Service unavailability/disruption as all systems were down
44.	UPS failure or related hardware faulty (battery & other parts)
45.	Continuous attempt to hack Agency's IP
46.	Faulty switches
47.	Phishing emails
2017	
1.	Website Defacement / Compromised
2.	Malware attacks
3.	Data / Information breach
4.	User Datagram Protocol (UDP) flood attack
6.	Vulnerable Own Cloud / Next Cloud
7.	Failure of internal network connection to command and control server

Num.	Types of Security Incidents
8.	Intermittent network service / failure
10.	High intermittent network service / disruption
11.	Very high traffic flood detected / network congestion
12.	Network Switches malfunction
13.	Unavailability of Wi-Fi connection
14.	IP address issue at Dynamic Host Configuration Protocol
16.	Internal Connection to Host Categorized as Malware
17.	One of the agency's Portal was compromised
18.	Potential Credential Leakage
19.	SQL injection
20.	BotNet attacks
21.	Controller V-center accidentally switched off
22.	Portal / Systems unavailability / unable to access
23.	Online services disruption / unavailability
24.	Storage Controller IBM V3700 down
25.	Internal power failure /disruption
26.	Failure / disruption in external power supply
27.	Fire suppression discharge in transformer room
28.	Access to malicious site
29.	Vulnerability in Portal / Web site detected
30.	Compromised user account
31.	Software failure due to expired license
32.	Backup failure
33.	Driver Host Bus Adaptor (HBA) faulty
34.	Chiller malfunction due to high pressure of gas, broken heat exchanger & bearing pump
35.	SPAM emails
36.	Phishing emails

II) Security Incidents Encountered by 2 Government Agencies 2016

Internal Threats	
1.	Lack of ICT security awareness, access to vulnerable web sites, downloading of illegal software, information leakage misuse/loss, mishandling of critical ICT assets, etc
2.	Incompetency of IT personnel that causes information loss/misuse, accidental database deletion, weakness in configuring and handling ICT Assets, damage to data integrity/confidentiality/availability and other critical assets
3.	Temporary Staff causing leaking of information, misuse or theft of ICT assets
4.	Information theft, misuse, loss causing damage to image and reputation of organization. Loss of client's confidence
5.	Sabotage by internal users causing deliberate database corruption, service disruption and unavailability
6.	Misleading SOP dan Procedure causing mishandling/damage to ICT assets, service disruption and unavailability
7.	Breach of security and Unauthorised access to information and systems
8.	Fire
9.	Power outage/surge
10.	Hardware failure
11.	Application Systems or software failure
12.	Database failure
13.	Back-up failure
14.	Lack of integrity or incompetency of Vendors those who carry out maintenance work.
15.	Outdated and obsolete technology
16.	Theft (notebook)
17.	Internal power outage/ failure / disruption
18.	Network unavailability / disruption
19.	Accidental deletion of customer data
20.	Password sharing among users and unauthorised access to systems
External Threats	
21.	Cross site scripting,
22.	SQL Injection

23.	Malware / Virus attacks
24.	Hackers intrusion
25.	Sabotage by external users
26.	Sabotage by vendors
27.	Natural disaster like earthquake , tremor
28.	Information theft, misuse, loss
29.	Portal / Website defacement or compromise
30.	External power failure / supply disruption
31.	Hacker's intrusion /Unauthorized access to systems or information.
32.	Network services shutdown by MAMPU/GITN if the trend shows serious attempts to hacking.
33.	Lack of incompetency of Vendors those who carry out maintenance work.
34.	Physical access to datacenter facility by many others as the PDSA is shared by other agencies too.

Appendix B Initial List of Threats Compiled Based On Literature Review and Preliminary Data Collection

Num.	Threat ID	Threat Category & Title	Source	Agents
			LR: Literature Review WR: Written Interview (Initial data gathering)	H: Human E: Environmental T: Technological
	A	Category: Virus, Trojan, Malware, Ransomware, Viral Websites Threats Description: A program or malicious codes designed to alter the way a computer operates, without the permission or knowledge of the user. A virus replicates and executes itself, usually doing damage to the data stored and computers in the process.		
1.	T01	Introduction of virus, Trojan through unlicensed software / attempts	LR & WI	H
2.	T02	Malicious codes or Malware attacks / attempts	LR & WI	H
3.	T03	Viral Websites -Introduction of virus, Trojan and malware through illegal websites	LR	H
	B	Category: Spyware, Phishing, SPAM, Bluesnarfing Threats Description: Spyware is any program that monitors online activities or installs programs without the owner's consent for profit or to capture personal information. Phishers masquerade as a trustworthy person or business and attempt to steal sensitive financial or personal information through fraudulent email or instant messages.		
4.	T04	Theft and Illegal usage/ misuse of personal information captured through Spyware.	LR & WI	H
5.	T05	Phishing:- Theft, disclosure and illegal use of sensitive financial or personal information through fraudulent email or instant messages.	LR & WI	H
6.	T06	Bluesnarfing:- Theft, disclosure of personal information through Bluetooth.	LR	H
7.	T07	Changing passwords/ accounts of administrator/ user accounts by masquerading	LR	H

Num.	Threat ID	Threat Category & Title	Source	Agents
8.	T08	SPAM email	LR & WI	H
9.	T09	Form-jacking (use of malicious code to steal credit card / other payment details)	LR	H
	C	<p>Category: Social Engineering</p> <p>Description: Exploiting the natural tendency of a person to trust and/or exploiting a person's emotional response to obtain computer security and personal information.</p>		
10.	T10	Attempts / Tricking computer users into revealing computer security or private information such as passwords, email addresses, etc.	LR & WI	H
	D	<p>Category: Unsecured Wireless Access Points (WAP) / Network Service</p> <p>Description: If WAP, Routers n other network related equipment are not secured, anyone with mobile or other devices will be able to get access to the network and disrupt the network services. Internet based attacks while your computer is connected to the Internet can be subjected to attack through the network communications.</p>		
11.	T11	Network (LAN/ WAN/ WiFi) service failure/ unavailability	LR & WI	H/T/E
12.	T12	Network congestion	LR & WI	H/T
13.	T13	Eavesdropping (network function virtualization)	LR	H/T
14.	T14	Traffic sniffing	LR	H/T
15.	T15	Confidentiality compromise (network function virtualization)	LR	H/T
16.	T16	High volume of packet transmission or flooding attacks	LR & WI	H/T
17.	T17	Control network denial of service attacks	LR	H/T
18.	T18	Aggregation node or nodes attacks	LR	H/T
19.	T19	Black hole / Packet drop attacks	LR	H/T
20.	T20	Direction of misleading attacks	LR	H/T
21.	T21	Wormhole attacks	LR	H/T
22.	T22	Trap doors Sybil attacks	LR	H/T

Num.	Threat ID	Threat Category & Title	Source	Agents
	E	Category: Natural Disaster / Environmental Description: Natural disasters are extreme, sudden events caused by environmental factors that injure people and damage property as well as ICT assets.		
23.	T23	Earthquakes/ Tremor	LR & WI	E
24.	T24	Flash Flood	LR & WI	E
25.	T25	Fire	LR & WI	H/T/E
26.	T26	Tsunami	LR	E
27.	T27	Haze drought	LR & WI	E
	F	Category: Technical Threats Description: Technical threats are threats that caused by hardware and software failures.		
28.	T28	Portal / Service disruption/ unavailability	LR & WI	H/T/E
29.	T29	Application Systems failure/ Cannot be accessed	LR & WI	H/T/E
30.	T30	Hardware malfunction (Server, Load balancer, Storage, Printer, etc.)	LR & WI	H/T/E
31.	T31	Software malfunction (OS, web service, etc.)	LR & WI	H/T/E
32.	T32	Failure/ faulty of network equipment (switches, routers, Netapp controller, etc)	LR & WI	H/T/E
33.	T33	Failure/ faulty of security hardware & software (IPS, Firewall, Antivirus, etc)	LR & WI	H/T/E
34.	T34	Faulty communication lines	LR & WI	H/T/E
35.	T35	Electromagnetic leakages/ interferences	LR	H/T/E
36.	T36	Power surge/ trip/ failure	LR & WI	H/T
37.	T37	Unpatched vulnerabilities of software (not known to the users until something occurs)	LR & WI	H/T

Num.	Threat ID	Threat Category & Title	Source	Agents
38.	T38	Backup failure, Faulty/ defective storage media (tapes, hard disk, cartridges)	LR	T
39.	T39	Failure of database caused by technical faulty in hardware/ software error.	LR	T
40.	T40	External power supply failures	LR & WI	H/T
41.	T41	Internal power supply disruption/ failure (rack / fuse, etc.)	LR & WI	H/T
42.	T42	Air conditioning / Ventilation disruption / High temperature	LR & WI	T
43.	T43	Chiller system down/ faulty	LR & WI	T
44.	T44	UPS failure or related hardware faulty (battery & other parts)	LR & WI	T
	G	<p>Category: Human Error (Accidental)</p> <p>Description: Threats caused by human can be categorized in to two types, deliberate and accidental. The accidental acts are caused by human error without any malicious intent to harm an organization's assets and reputation.</p>		
45.	T45	Accidental destruction / corruption of part of or whole database	LR & WI	H
46.	T46	Accidental Deletion of customer data	LR & WI	H
47.	T47	Accidentally Deleting proprietary software	LR & WI	H
48.	T48	Accidentally Deleting backups	LR & WI	H
49.	T49	Accidentally Deleting proprietary designs	LR & WI	H
50.	T50	Incompetency of internal staff	LR & WI	H
51.	T51	Incompetency of External Vendors in outsourced project (misconfiguration of hardware or software)	WI	H
52.	T52	Incompetency of Temporary / Contract staff	WI	H
53.	T53	Hazards posed by janitors or cleaners (vacuum, sweep, wipe, empty thrash)	LR	H

Num.	Threat ID	Threat Category & Title	Source	Agents
54.	T54	Mishandling of critical ICT assets and other equipment	WI	H
55.	T55	Misleading SOP and Procedures	WI	H
56.	T56	Accidentally Shutting down of hardware (servers, console, etc.)	LR & WI	H/T/E
57.	T57	Accidentally Shutting down software (application, software, database, etc.)	LR & WI	H/T/E
	H	<p>Category: Deliberate Human Threats</p> <p>Description: Threats caused by human can be categorized in to two types, deliberate and accidental. The deliberate acts are done with the malicious intent to cause damages to the assets and reputation of an organization.</p>		
58.	T58	Deliberate destruction / corruption of part of or whole database	LR & WI	H
59.	T59	Elevation of privilege	LR	H
60.	T60	Unauthorized modification or deletion of customer data	LR & WI	H
61.	T61	Planting logic bombs in application systems	LR	H
62.	T62	Deleting proprietary software or designs	LR	H
63.	T63	Deleting backups	LR	H
64.	T64	Denial of services / legitimate access	LR	H/T/E
65.	T65	Denial of information usage / unavailability of data	LR & WI	H/T/E
66.	T66	Service violation attacks	LR	H
67.	T67	Distributed denial of service attack	LR & WI	H
68.	T68	Physical attacks	LR	H
69.	T69	Supply chain attack (exploit third party services / software to compromise a final target)	LR	H
70.	T70	Crypto jacking (secretly run coin miners on victim's device without their knowledge and use their CPU power to mine cryptocurrencies)	LR	H

Num.	Threat ID	Threat Category & Title	Source	Agents
71.	T71	Cloud services attack (targeted attack on cloud services instances)	LR	H
72.	T72	Pandemics	LR	H/E
73.	T73	Riots	LR	H
74.	T74	Wars	LR	H
75.	T75	Terrorist attacks	LR & WI	H
76.	T76	Unauthorized Access to data center facility/ restricted area (illegal entry)	LR & WI	H
77.	T77	Vandalism /theft / loss of hardware/ software	LR & WI	H
78.	T78	Website Defacement / Compromised	LR & WI	H
79.	T79	Unauthorized access to servers / critical systems	LR & WI	H
80.	T80	Sabotage by Internal staff (integrity)	LR & WI	H
81.	T81	Sabotage by External Vendors in outsourced project (integrity)	WI	H
82.	T82	Sabotage by Temporary / Contract staff (integrity)	WI	H
83.	T83	Attempts to hack IP/ intrusion/ invasion of network threats	LR & WI	H
84.	T84	SQL injection	LR & WI	H
85.	T85	Cross site scripting	LR & WI	H
86.	T86	Data breach / information Leakage	LR	H/T
87.	T87	Privacy in data mining	LR	H
88.	T88	Control command forged attacks	LR	H
89.	T89	Shutting down of hardware (servers, console, etc.)	LR & WI	H
90.	T90	Shutting down software (application, software, database, etc.)	LR & WI	H

Appendix C List of Interview Participants for Phase 1

Respondent Reference	Agency Reference	Gender (M-Male/ F-Female)	Designation / Unit	Experience in IT Security / Data Center (Years)	Experience in Government organization (Years)	Are you the Information Security Officer (ICTSO) of the Organization?	Key Roles in Information Security (IS)
R1	A1	F	Senior Principal Secretary / Operation / Security	5-10 years	15 years	No	<ul style="list-style-type: none"> - Assist in managing organization's ICT Infrastructure, Network equipment and security. - Assist in day to day operations of data center. - Assist in handling IS related issues.
R2	A2	M	IT Manager	>15 years	27 years	Yes	<ul style="list-style-type: none"> - Chief ICT Security Officer - Overall responsible for the organization's IS. - Overall in charge for Managing IS of organization's ICT security policy; assets including hardware, software and Network Infrastructure 24 x 7.
R3	A3	M	Senior Principal Secretary / Operation / Security	5-10 years	17 years	No	<ul style="list-style-type: none"> - Assist in managing organization's ICT Infrastructure, Network equipment and security. - Assist in day to day operations of data center. - Assist in handling IS related issues.

Respondent Reference	Agency Reference	Gender (M-Male/ F-Female)	Designation / Unit	Experience in IT Security / Data Center (Years)	Experience in Government organization (Years)	Are you the Information Security Officer (ICTSO) of the Organization?	Key Roles in Information Security (IS)
R4	A4	M	Senior Principal Secretary / Operation / Security	>15 years	16 years	No	<ul style="list-style-type: none"> - Assist in managing organization's ICT Infrastructure, Network equipment and security. - Assist in day to day operations of data center. - Assist in handling IS related issues.
R5	A5	M	Head of Data Center / Operation	>15 years	25 years	Yes	<ul style="list-style-type: none"> - Chief ICT Security Officer - Overall responsible for the organization's IS. - Overall in-charge of Data Center operations including database, servers, VM and equipment, ensuring service continuity and IS.
R6	A6	F	Head of Data Center/Network Operation	5-10 years	23 years	Yes	<ul style="list-style-type: none"> - Chief ICT Security Officer - Overall responsible for the organization's IS. - Overall in-charge of Data Center operations including database, servers, VM and equipment, ensuring service continuity and IS.

Respondent Reference	Agency Reference	Gender (M-Male/ F-Female)	Designation / Unit	Experience in IT Security / Data Center (Years)	Experience in Government organization (Years)	Are you the Information Security Officer (ICTSO) of the Organization?	Key Roles in Information Security (IS)
R7	A7	M	Deputy IT Director/ Head of Operation	5-10 years	24 years	Yes	<ul style="list-style-type: none"> - Chief ICT Security Officer - Overall responsible for the organization's IS. -Overall in-charge of Data Center operations including database, servers, VM and equipment, ensuring service continuity and IS.
R8	A8	M	Deputy IT Manager/ Head of Operation	>15 years	25 years	Yes	<ul style="list-style-type: none"> - Chief ICT Security Officer - Overall responsible for the organization's IS. -Overall in-charge of Data Center operations including database, servers, VM and equipment, ensuring service continuity and IS.
R9	A9	F	Head of Data Center / Operation	>15 years	20 years	Yes	<ul style="list-style-type: none"> - Chief ICT Security Officer - Overall responsible for the organization's IS. - Overall in-charge of Data Center operations including database, servers, VM and equipment, ensuring service continuity and IS.

Respondent Reference	Agency Reference	Gender (M-Male/ F-Female)	Designation / Unit	Experience in IT Security / Data Center (Years)	Experience in Government organization (Years)	Are you the Information Security Officer (ICTSO) of the Organization?	Key Roles in Information Security (IS)
R10	A10	M	Senior Principal Secretary / Operation / Security	5-10 years	15 years	No	<ul style="list-style-type: none"> - Assist in managing organization's ICT Infrastructure, Network equipment and security. - Assist in day to day operations of data center. - Assist in handling IS related issues.
R11	A11	F	IT Director	>15 years	28 years	Yes	<ul style="list-style-type: none"> - Chief ICT Security Officer - Overall responsible for the organization's IS. - Overall in charge for Managing ICT Security of organization's ICT security policy; assets including hardware, software and Network Infrastructure 24 x 7.
R12	A12	F	Senior Principal Secretary / Operation / Security	5-10 years	18 years	No	<ul style="list-style-type: none"> - Assist in managing organization's ICT Infrastructure, Network equipment and security. - Assist in day to day operations of data center. - Assist in handling IS related issues.

Respondent Reference	Agency Reference	Gender (M-Male/ F-Female)	Designation / Unit	Experience in IT Security / Data Center (Years)	Experience in Government organization (Years)	Are you the Information Security Officer (ICTSO) of the Organization?	Key Roles in Information Security (IS)
R13	A13	F	IT Manager	>15 years	30 years	No	-Overall responsible for the Ministry's IS. -In charge of the Ministry's ICT Security Policy.
R14	A14	M	Senior Principal Director / Operation	>15 years	20 years	No	- Assist in managing organization's ICT Infrastructure, Network equipment and security. -Assist in day to day operations of data center. - Assist in handling IS related issues.
R15	A15	M	Deputy IT Manager/ Operation Head	11-15 years	23 years	Yes	- Chief ICT Security Officer - Overall responsible for the organization's IS. - Overall in-charge of Data Center operations including database, servers, VM and equipment, ensuring service continuity and IS.
R16	A16	M	Senior Principal Secretary / Operation / Security	5-10 years	20 years	No	- Assist in managing organization's ICT Infrastructure, Network equipment and security. -Assist in day to day operations of data center. - Assist in handling IS related issues.

Respondent Reference	Agency Reference	Gender (M-Male/ F-Female)	Designation / Unit	Experience in IT Security / Data Center (Years)	Experience in Government organization (Years)	Are you the Information Security Officer (ICTSO) of the Organization?	Key Roles in Information Security (IS)
R17	A17	M	Head of Data Center / Security	5-10 years	15 years	Yes	<ul style="list-style-type: none"> - Chief ICT Security Officer - Overall responsible for the organization's IS. - Overall in-charge of Data Center operations including database, servers, VM and equipment, ensuring service continuity and IS.
R18	A18	M	IT Manager	11-15 years	30 years	Yes	<ul style="list-style-type: none"> - Chief ICT Security Officer - Overall responsible for the organization's IS. - Overall in charge for Managing ICT Security of organization's ICT security policy; assets including hardware, software and Network Infrastructure 24 x 7.
R19	A19	F	Head of Data Center / Operation / Security	11-15 years	25 years	Yes	<ul style="list-style-type: none"> - Chief ICT Security Officer - Overall responsible for the organization's IS. -Overall in-charge of Data Center operations including database, servers, VM and equipment, ensuring service continuity and IS.

Respondent Reference	Agency Reference	Gender (M-Male/ F-Female)	Designation / Unit	Experience in IT Security / Data Center (Years)	Experience in Government organization (Years)	Are you the Information Security Officer (ICTSO) of the Organization?	Key Roles in Information Security (IS)
R20	A20	F	Head of Data Center / Operation	>15 years	22 years	Yes	<ul style="list-style-type: none"> - Chief ICT Security Officer - Overall responsible for the organization's IS. -Overall in-charge of Data Center operations including database, servers, VM and equipment, ensuring service continuity and IS.
R21	A21	M	Senior Principal Secretary / Operation /Security	5-10 years	15 years	No	<ul style="list-style-type: none"> - Assist in managing organization's ICT Infrastructure, Network equipment and security. -Assist in day to day operations of data center. - Assist in handling IS related issues.
R22	A22	M	Senior Principal Secretary / Operation / Security	5-10 years	17 years	No	<ul style="list-style-type: none"> - Assist in managing organization's ICT Infrastructure, Network equipment and security. -Assist in day to day operations of data center. - Assist in handling IS related issues.

Respondent Reference	Agency Reference	Gender (M-Male/ F-Female)	Designation / Unit	Experience in IT Security / Data Center (Years)	Experience in Government organization (Years)	Are you the Information Security Officer (ICTSO) of the Organization?	Key Roles in Information Security (IS)
R23	A23	F	IT Manager	>15 years	29 years	No	-Overall responsible for the Ministry's Information Security. -In charge of the Ministry's ICT Security Policy.
R24	A24	F	IT Director	>15 years	30 years	Yes	- Chief ICT Security Officer - Overall responsible for the organization's IS. - Overall in charge for Managing ICT Security of organization's ICT security policy; assets including hardware, software and Network Infrastructure 24 x 7.
R25	A25	M	IT Director	>15 years	28 years	Yes	- Chief ICT Security Officer - Overall responsible for the organization's IS. - Overall in charge for Managing ICT Security of organization's ICT security policy; assets including hardware, software and Network Infrastructure 24 x 7.

Respondent Reference	Agency Reference	Gender (M-Male/ F-Female)	Designation / Unit	Experience in IT Security / Data Center (Years)	Experience in Government organization (Years)	Are you the Information Security Officer (ICTSO) of the Organization?	Key Roles in Information Security (IS)
R26	A26	F	Senior Principal Director /Operation	11-15 years	18 years	No	<ul style="list-style-type: none"> - Assist in managing organization's ICT Infrastructure, Network equipment and security. -Assist in day to day operations of data center. - Assist in handling IS related issues.
R27	A27	F	Senior IT Operation Manager	>15 years	23 years	Yes	<ul style="list-style-type: none"> - Chief ICT Security Officer - Overall responsible for the organization's IS. <p>Overall in-charge of Data Center operations including database, servers, VM and equipment, ensuring service continuity and IS.</p>
R28	A28	M	Operation Head	5-12 years	22 years	No	-Overall in-charge of Data Center operations including database, servers, VM and equipment, ensuring service continuity and IS.
R29	A29	M	Head of Data Center / Operation	>15 years	20 years	Yes	<ul style="list-style-type: none"> - Chief ICT Security Officer - Overall responsible for the organization's IS. <p>Overall in-charge of Data Center operations including database, servers, VM and equipment, ensuring service continuity and IS.</p>

Respondent Reference	Agency Reference	Gender (M-Male/ F-Female)	Designation / Unit	Experience in IT Security / Data Center (Years)	Experience in Government organization (Years)	Are you the Information Security Officer (ICTSO) of the Organization?	Key Roles in Information Security (IS)
R30	A30	F	Head of Data Center / Operation	>15 years	25 years	Yes	<ul style="list-style-type: none"> - Chief ICT Security Officer - Overall responsible for the organization's IS. - Overall in-charge of Data Center operations including database, servers, VM and equipment, ensuring service continuity and IS.
R31	A31	M	Head of Data Center/ Operation	11-15 years	26 years	Yes	<ul style="list-style-type: none"> - Chief ICT Security Officer - Overall responsible for the organization's IS. - Overall in-charge of Data Center operations including database, servers, VM and equipment, ensuring service continuity and IS.
R32	A32	F	Deputy IT Manager/ Operation Head	11-15 years	28 years	Yes	<ul style="list-style-type: none"> - Chief ICT Security Officer - Overall responsible for the organization's IS. - Overall in-charge of Data Center operations including database, servers, VM and equipment, ensuring service continuity and IS.

Respondent Reference	Agency Reference	Gender (M-Male/ F-Female)	Designation / Unit	Experience in IT Security / Data Center (Years)	Experience in Government organization (Years)	Are you the Information Security Officer (ICTSO) of the Organization?	Key Roles in Information Security (IS)
R33	A33	F	IT Manager	5-10 years	30	Yes	<ul style="list-style-type: none"> - Chief ICT Security Officer - Overall responsible for the organization's IS. - Overall in charge for Managing ICT Security of organization's ICT security policy; assets including hardware, software and Network Infrastructure 24 x 7.
Ministry-A							
R34	A34	F	IT Director	11-15 years	28	No	<ul style="list-style-type: none"> -Overall responsible for the Ministry's Information Security. -In charge of the Ministry's ICT Security Policy.

Respondent Reference	Agency Reference	Gender (M-Male/ F-Female)	Designation / Unit	Experience in IT Security / Data Center (Years)	Experience in Government organization (Years)	Are you the Information Security Officer (ICTSO) of the Organization?	Key Roles in Information Security (IS)
R35	A34	M	Manager/ Network & Security Unit	>15 years	25	Yes	<ul style="list-style-type: none"> -Chief ICT Security Officer -Overall in charge for Managing ICT Security of organization's ICT assets including hardware, software and Network Infrastructure. Monitor ICT security 24 x 7. -Managing and reviewing documentation of ICT security policies, emergency measures policies, procedures, and testing. -Identifying relevant IT security training and organizing as well as promoting. -Conduct ICT security awareness through awareness programs. -Conducting Security Posture Assessment and other relevant activity.
R36	A34	F	Senior Manager/ Operations Unit	11-15 years	27	No	<ul style="list-style-type: none"> -Overall in-charge of Data Center operations including database, servers, VM and equipment, ensuring service continuity and security.

Respondent Reference	Agency Reference	Gender (M-Male/ F-Female)	Designation / Unit	Experience in IT Security / Data Center (Years)	Experience in Government organization (Years)	Are you the Information Security Officer (ICTSO) of the Organization?	Key Roles in Information Security (IS)
R37	A34	M	Senior IT Officer/ Network & Security Unit	11-15 years	13	No	-Assist in managing Ministry's ICT Infrastructure, Network equipment and security. -Assist in documenting and reviewing ICT Security Policies, ICT security emergency response, monitoring ICT security safeguards in place and conduct ICT security awareness programs.
R38	A34	M	Senior IT Officer / Operations Unit	5-10 years	10	No	-In charge of database administration, storage and backups and its security at data center at Ministry's HQ. -In charge of VM and servers its security policies.
R39	A34	M	Senior IT Officer / Operations Unit	5-10 years	10	No	-In Charge of Data Center Security, Servers Security, Security Policies of ISMS, DRC.
R40	A34	F	IT Officer / Network & Security Unit	5-10 years	10	No	-In charge of ministry's email, network & ICT security, ISMS Documentations, security audit
R41	A34	M	IT Officer / Operations Unit	5-10 years	7	No	-Assist in backups, managing servers, database, managing DRC,

Respondent Reference	Agency Reference	Gender (M-Male/ F-Female)	Designation / Unit	Experience in IT Security / Data Center (Years)	Experience in Government organization (Years)	Are you the Information Security Officer (ICTSO) of the Organization?	Key Roles in Information Security (IS)
							managing Data Center Critical & Supporting Equipment, ISMS Documentations.
R42	A34	M	Senior Programmer / Network & Security Unit	>15 years	20	No	-Assist officers in managing Ministry's ICT Infrastructure, Network equipment and security. -Assist in documenting and reviewing ICT Security Policies, ICT security emergency response, monitoring ICT security safeguards in place.
R43	A34	F	Senior Programmer / Operations Unit	11-15 years	15	No	-Assist officers in backup, managing servers, managing database, managing DRC, managing Data Center Critical & Supporting Equipment.
R44	A34	M	Programmer / Network & Security Unit	5-10 years	8	No	-Assist officers in managing Ministry's ICT Infrastructure, Network equipment and security. -Assist in ICT security emergency response, monitoring ICT security safeguards in place.
R45	A34	F	Programmer / Operations Unit	5-10 years	5	No	-Assist officers in backup, managing servers, managing DRC,

Respondent Reference	Agency Reference	Gender (M-Male/ F-Female)	Designation / Unit	Experience in IT Security / Data Center (Years)	Experience in Government organization (Years)	Are you the Information Security Officer (ICTSO) of the Organization?	Key Roles in Information Security (IS)
							managing Data Center Critical & Supporting Equipment.
R46	A34	M	Technician / Network & Security Unit	5-10 years	8	No	-Provide technical support for email and other security related software to users.
R47	A34	M	Technician / Network & Security Unit	5-10 years	7	No	-Provide technical support for email and other security related software for users.
R48	A34	M	Technician / Operations Unit	5-10 years	10	No	-Provide technical support for data center equipment and other related software to users.

Appendix D Questionnaire for Semi Structured Interview

Section A: Demographic		
<p>Instruction: Please answer all questions. Fill in the information required or mark 'X' where appropriate. (Can be in English or Bahasa Malaysia)</p>		
1.	Name	:
2.	Gender	: Male <input type="checkbox"/> Female <input type="checkbox"/>
3.	Experience in government agency	: Years:
4.	Highest Academic Qualification	: PhD <input type="checkbox"/> Masters <input type="checkbox"/> Bachelor <input type="checkbox"/> Diploma <input type="checkbox"/>
5.	ICTSO	: Yes <input type="checkbox"/> No <input type="checkbox"/>
6.	Unit/Division/Organisation	:
7.	Years of experience in IT Security / Data Center	:
8.	Designation and Information Security key role	:

Section B: Organization Information Security Requirements

Instruction:

**Please answer all questions. Fill in the information required by writing or typing
(Can be in English or Bahasa Malaysia)**

1.	What are Security Requirements of the Management in your Organization?									
2.	What are your Organization's Security Objectives? List down Please.									
i) ii)										
3.	What are your Organization's Internal and External Context?									
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; text-align: center;"><u>Internal</u></td> <td style="width: 50%; text-align: center;"><u>External</u></td> </tr> <tr> <td>i)</td> <td>i)</td> </tr> <tr> <td>ii)</td> <td>ii)</td> </tr> <tr> <td>iii)</td> <td>iii)</td> </tr> </table>			<u>Internal</u>	<u>External</u>	i)	i)	ii)	ii)	iii)	iii)
<u>Internal</u>	<u>External</u>									
i)	i)									
ii)	ii)									
iii)	iii)									
4.	What are the Strengths and Weaknesses? List down Please.									
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; text-align: center;"><u>Strengths</u></td> <td style="width: 50%; text-align: center;"><u>Weaknesses</u></td> </tr> <tr> <td>i)</td> <td>i)</td> </tr> <tr> <td>ii)</td> <td>ii)</td> </tr> <tr> <td>iii)</td> <td>iii)</td> </tr> </table>			<u>Strengths</u>	<u>Weaknesses</u>	i)	i)	ii)	ii)	iii)	iii)
<u>Strengths</u>	<u>Weaknesses</u>									
i)	i)									
ii)	ii)									
iii)	iii)									
5.	What are the Opportunities and Threats? List down Please.									
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; text-align: center;"><u>Opportunities</u></td> <td style="width: 50%; text-align: center;"><u>Threats</u></td> </tr> <tr> <td>i)</td> <td>i)</td> </tr> <tr> <td>ii)</td> <td>ii)</td> </tr> <tr> <td>iii)</td> <td>iii)</td> </tr> </table>			<u>Opportunities</u>	<u>Threats</u>	i)	i)	ii)	ii)	iii)	iii)
<u>Opportunities</u>	<u>Threats</u>									
i)	i)									
ii)	ii)									
iii)	iii)									

Section C: Data Center Information Security

Instruction:

Please answer all questions. Fill in the information required by writing or typing
(Can be in English or Bahasa Malaysia)

Note: If your Organization has more than 1 Data Center, Please repeat this Section C accordingly.

I) Data Center in	
1.	What are the services hosted in your data center?
i) ii) iii)	
2.	What are the types of ICT assets in the data center? <i>(e.g. data, hardware, software, etc)</i> and the possible Vulnerabilities?
Assets	
Vulnerabilities	
x)	
xi)	
xii)	
3.	What are the potential Internal ICT threats faced by your organization? and their impact?
Internal Threats	
Impact	
i)	
ii)	
iii)	
4.	What are the potential External ICT threats faced by your organization? and their impact?
External Threats	
Impact	
i)	
ii)	
iii)	
5.	What are the potential risks faced by the Data Center in your Organization?
i)	
ii)	
iii)	
6.	What are the existing safeguards or controls currently in place?
Safeguards	
Purpose	
i)	
ii)	

iii)		
7.	What are the critical success factors in ensuring information security of critical ICT assets in the data center in your organization?	
i) ii) iii) iv)		
8.	Does your organization adopt any standard or any other best practices for information security for this data center? <i>(If Yes, Please specify)</i>	
9.	Does the standard give detailed guidelines for information security risk assessment process? <i>(Please mark 'X')</i>	
	Yes <input type="checkbox"/> No <input type="checkbox"/>	
10.	Do you use any specific methodology or tool to assess information security risks for this data center? <i>(If Yes, Please specify)</i>	
	Yes <input type="checkbox"/> No <input type="checkbox"/>	

Appendix E Sample Interview Script

Below is an example of the script of the semi structured interview conducted. The interview questions refer to identify various types of information security threats encountered in the Data Center environment.

Interviewer	:	Ms. Inthrani Shammugam
Respondent	:	Mr. A
Respondent Designation	:	Head of Network & Security Unit. Information and Communication Technology (ICT) Security Officer.
Date	:	2 February June 2018 (Time: 10-11am)
Place	:	Information Technology (IT) Division, Ministry-A.

INTERVIEW SCRIPT:

Interviewer: Good Morning Mr. A.

Respondent: Good morning.

Interviewer: First of all, thank you very much for agreeing to this interview and allocating your time despite your busy schedule. I am very grateful for that. Please allow me introduce myself before we begin the interview. I am Inthrani Shammugam, currently pursuing my PhD in Computer Science at Universiti Teknologi Malaysia (UTM). The main aim of my PhD thesis is to apply a quantity analysis method to analyse information security risks in a data center environment. One of the research objectives of my thesis is to identify the threats that are often encountered by the data centers in our Malaysian Public Sector organizations. Therefore, the purpose of this interview is to identify the different types of information security threats that usually occur in data center environments. I have prepared a list of questions as a guide to conduct this interview. You can have a look at the questions. However, the questions will not be limited to the list and there may be some additional questions. Please feel free to clarify should you have any question. I will be typing out your answers as we go along. You can check your responses at the end of this session.

Respondent: Sure, no problem. Please proceed with your questions. I will fill up my personal information later.

Interviewer: How long you have been in the government service?

Respondent: Oh, this is my 26th year in public service.

Interviewer: I am sure you have had vast experience working in many organizations. Could you share some of your experience, particularly in handling data center and security?

Respondent: This is my 3rd organization, in fact this is my second time working here. Currently, I am the head of Network and Security Unit. Previously, I was mainly handling technical support and also security here. I was involved in system application for a short period at my other place, but my interest has been always in security.

Interviewer: Sir, I understand you are the ICT Security Officer (ICTSO) of this organization. How many years you have been the ICTSO? Could you elaborate on your responsibilities and job scope as an ICTSO please?

Respondent: You are right. I have been the ICT Security Officer for this organization for the past 5 years. I am also the Head of the Security and Network Unit. So, you can imagine my responsibilities. It is a huge task, to be in charge of the ICT security of an organization like this, especially nowadays. We don't even know when security incidents will take place or where the threats will come from, Hahaha! My job scope and responsibilities include being in charge of managing the ICT Security of the organization's ICT assets including the hardware, software and Network Infrastructure; monitoring ICT security 24 x 7; managing and reviewing documentation of ICT security policies, emergency measures policies, procedures, and testing; identifying relevant IT security training and organizing as well as promoting; conducting ICT security awareness through awareness programs; and conducting Security Posture Assessment and other relevant activity. I am also the management representative in the Information Security Management System Committee. You know the ISO/IEC 27001? For your information, our data center has been certified for the past 6 years. So, I also need to report to and advice my head of department and top management about any issues and updates related to information security.

Interviewer: That's really a tall order Sir. Could you please share with me the security requirement of the management? I mean their expectation. Also, your organization's security objectives.

Respondent: The management expect us to ensure all ICT assets and services are secured to give confidentiality, availability and integrity of the information. Our organization's security objectives are very specific. We have 6 objectives like:

- i) Ensure business continuity and service availability,
- ii) Prevent and minimize security incident,
- iii) Ensure security, confidentiality and integrity of digital information and documents,
- iv) Ensure information and documents are from reliable and legal sources,
- v) Ensure only authorized users are given access to information, and

- vi) Ensure security, reliability, integrity, availability and confidentiality of ICT assets.

Interviewer: Thank you Sir, for the detailed answer. Next, could you answer some questions on your organization's internal and external context, please?

Respondent: Sure. Our internal contexts are the organization's culture, values, principles, policies, and capabilities of our people and systems. Our external contexts are like external clients' needs, other government agencies' needs, political climate, and technological advancement. These are some of our internal and external context factors.

Interviewer: I would also like to know about some of your organization's strengths, weaknesses, opportunities and threats. Since, you have mentioned that your organization is ISMS certified. Would you mind sharing it?

Respondent: I can't give all the information but I can share some in general. Our strengths are like the strong management support and commitment, strong security policies and controls in place as well as capable and competent staff. Our opportunities are like exploring new technologies, and further strengthening our security systems and controls in place. Our threats are of course the alarming increase in the security threats from outsiders like continuous attempts to hack our network and systems. Every now and then we hear news about the hackers outside there trying very hard to deface some of our government websites.

Interviewer: Thank you, Sir. How about the questions under Section C of the questionnaire, related to the data center? The services hosted; types of assets and their vulnerabilities; potential threats and their impacts; the existing safe guards or control measures and their purposes? And the critical success factors in ensuring information security? Could you provide some information on these topics?

Respondent: Well, I am sorry. I cannot answer all the questions as some of the information is confidential, especially the safeguards that we have implemented. But I can share information on the threats encountered, services hosted and assets in general terms.

Interviewer: Thank you very much, Sir, for your kind consideration.

Respondent: We have 2 data centers, the main one is located here in HQ and the secondary data center is located at *Pusat Data Sektor Awam*, in Putrajaya. (other answers are listed in the attached questionnaire).

Based on my experience in managing information security, some of the main threats here are the continuous attempts by hackers to penetrate our network, SPAM emails, phishing to get important information, software malfunction, application system failures and hardware failures. I don't

have the details right now but we can refer to our security incident records later.

Interviewer: In your experience, which is the threats occurs the most?

Respondent: Oh, the most frequent one is the threat related to one of our core systems. It is a legacy system running on an old operating system. The frequent failure of the system is the biggest threat now as this system provides online services to our main clients. Currently another agency is already developing a comprehensive system, which also includes the functions of this system. Hopefully, the system will be ready in 2 years-time, until then we have deal with this threat. I think that this is followed by continuous attempt by hackers and SPAM emails. I need to check the records to be sure. We continuously monitor the hackers' attempts as we have tools and strong control measures and systems in place to monitor that. However, the SPAM emails seem to be a continuous problem. You see the senders are very clever and every time when we block the email source, they will come up with a new email.

Interviewer: You mentioned earlier that the hackers are trying very hard to hack the government websites. So far has anyone managed to hack your network and system? Any serious SPAM email incidents?

Respondent: Thank God, fortunately no. So far there have been no such major incidents. We managed to prevent them successfully. As I said, we have a strong system in place for 24x7 monitoring. Besides that, we regularly blast emails and pamphlets on SPAM, phishing emails and information security to our users. So, our users are quite aware on that. But the system failure is our major concern, we just have to take swift action and rectify the problems immediately.

Interviewer: What are the other threats faced by your data center?

Respondent: Some of the other threats that we often face are virus and malware attacks and a couple of incidents related to power failure, which caused some servers to go down. I remember there was a major power failure incident which affected the whole data center and our management was very upset, but we managed to restore everything within 2 hours with the help of generators.

Interviewer: Any idea what was the reason?

Respondent: According to the Tenaga Nasional, it was due to some major power disruption issue at the construction site behind our building.

Interviewer: Have there been any threats related to network infrastructure failures or errors such as connection failure, using unsecured wireless network, network software failure and network congestion?

Respondent: Oh yes! There were a few incidents caused by network infrastructure related threats such as network congestion, breakdown of switches and software failures. Network congestion occurs when there are heavy and continuous attempt by hackers. Sometimes it happens just before long holiday breaks when our clients rush to submit their online applications for their permits.

Interviewer: Have you experienced any kind of human threats?

Respondent: You mean purposely causing damages like sabotage?

Interviewer: Actually there are two categories of human threats. One is doing things with the intention of causing damage, known as a deliberate human threat. The other is known as accidental human threats, which is actually done accidentally without any malicious intention.

Respondent: Yes of course, the deliberate one is the attempt by hackers to penetrate our network and systems, which happens from time to time. But the accidental one is very rare. If I am not mistaken there was one incident some time ago, where our junior officer accidentally switched off the wrong server.

Interviewer: Did you identify the cause? What did you do prevent such accidental human error?

Respondent: Well, we realised it was due to lack of documentation and SOPs, I mean standard operating procedure. So, we immediately came up with proper documentation and SOPs to ensure that equipment is properly labelled and everyone must strictly follow the SOPs when handling critical equipment. Since then, there have been no such incidents.

Interviewer: Besides that, have you encountered any theft issues?

Respondent: You mean equipment or information?

Interviewer: Both Sir, and also password theft.

Respondent: No. As far as I know, there have been no such cases so far.

Interviewer: Very well. Do you encounter any other threats related to obsolete or outdated hardware and software?

Respondent: As I mentioned earlier, we have only one legacy system, which is running on an old operating system. Other than that, we don't face such threats as we just replaced most of our equipment 2 years ago when we shifted to the new building.

Interviewer: Has there been any incident of unauthorised personal entering the data center? How do you manage this kind of threats?

Respondent: Good question. Actually, we have put in a strict control measure for this. No outsiders are allowed to be on the level where our data center is located. Even the maintenance contractors and cleaners must be accompanied and supervised by our staff in charge at all times until they have completed their work and leave the floor. We have to use access cards to enter the data center and only the relevant officers are given access. For your information, even our IT manager does not have permission to enter our data center as she is not involved in handling any of the equipment. We accompany her whenever she does the site visits.

Interviewer: Wow! Your SOPs are very strict Sir.

Respondent: Yes, because we are ISMS certified and the system report can show the entry details such as who and when. We also maintain manual records to cross check the entries. These are only some of the controls and I can't disclose all the rest of them.

Interviewer: No problem, Sir. Have any threats related to insufficient storage space and back up occurred so far?

Respondent: We used to have those threats, but we no longer do as we have replaced the old hardware and procured additional storage and new back-up systems when we moved to the new building here.

Interviewer: Going back to the human related threats. How do you educate the staff in your organization on how to prevent security threats and create awareness on information security?

Respondent: I must say that it is a big challenge and we faced some major issues in the past. However, after a series of technology update sessions; continuous awareness programs and briefings on ICT security; and engagement with stakeholders, things have improved tremendously. The ISMS certification was an eye opener for stakeholders. In addition, the stakeholders are also very worried as many government agencies' were affected by the recent website defacement incidents. So, we are given budget allocations to conduct education and awareness programs as required by the ISMS, which is actually giving good results.

Interviewer: Good to hear that you have your management's commitment and support on this.

Interviewer: How about the staff involved in operational work? I mean those who are involved in data center and security related work? Are they well trained to handle all their operational work? Do you have any problems such as incompetence or lack of training for staff to manage the data center and security related work?

Respondent: Yes, we do face this kind of problems whenever staff transfers take place. Sometimes we have staff moving in and out due to promotions and other reasons. When new staff come in, we have to train them for at least 6 months and must always make sure they are competent before we allow

them to handle any critical equipment or issues. For the existing staff, I personally make sure they attend at least one technical course every year, preferably a data center and security related certification course. This is basically to enhance their knowledge and skill as well as to overcome the staff shortage issue.

Interviewer: Have there ever been any threats from contractors? Incidents of existing contractors trying to gain unauthorised access to confidential information and systems in your data center?

Respondent: So far no. As I mentioned earlier, the contractors must be accompanied by our staff all the times and often senior staff are the ones who will supervise the contractors.

Interviewer: Were there any incidents where the staff misuse the information system resources and facilities given? Such as accessing to unauthorised websites and installing or downloading unwanted software or content?

Respondent: We used to have this threat a few years back. We don't face these threats any longer, as we have installed the relevant tools in our servers to detect and prevent such activities. In addition, I must say that the information security education and awareness programs have been very effective so far.

Interviewer: Were there are any threats related to natural disasters such as fires at the server side, floods, lightning strikes or earthquake incidents?

Respondent: So far such incidents have not occurred in the data center or in our IT department in this new building. However, once there was an incident of a lightning strike after a heavy downpour, which caused the whole data center to go down for a day, a few years back in the old building. Other than that we have never experienced any other natural disaster such as floods and earthquake.

Interviewer: Are there any threats which related to terrorism?

Respondent: No, we have never experienced such threats.

Interviewer: How do you maintain the records on information security incidents?

Respondent: We maintain very detailed records as it is one of the requirements for our ISMS certification. Besides that, it is also an instruction from our IT Director. She will monitor every month. I have to submit a monthly report on this.

Interviewer: Does this ISMS standard give clear detailed guidelines on how to carry out risk assessment?

Respondent: No. It just state that we have to risk identification and assessment, but no detailed guidelines are stated.

Interviewer: How did you carry out the risk identification and assessment processes then? in order to set the priority to mitigate them.

Respondent: We identified the risk and assessed them based on expert opinion of experts. We had a workshop for this activities with our main users and stakeholders. We identified based on the input given by them. The assessment too was done based on their input like the frequency and the estimated damage or impact. Then, we set the priority accordingly.

Interviewer: Sir, in your opinion, how effectively is the risk assessment process being carried out currently? Can you explain a bit on that?

Respondent: Currently, we are doing on our own for overall risk assessment. For the hardware we refer to MyRAM. But not on a regular basis. We do that whenever required by MAMPU. Sometimes, we also find it difficult as MyRAM only covers the hardware and not all the other ICT assets as defined and required by ISMS and we don't have the guidance or guidelines to conduct a comprehensive risk assessment that covers all the ICT assets. It will be great if your study can consider this, hahaha.

Interviewer: Hahaha, sure Sir. One last question, please? I have prepared a list of threats based on my research and interview with other organization. Could you help me just tick the threats that encountered by your data centers?

Respondent: No problem. My officer will do that based on our incident records.

Interviewer: Thank you Sir, for your time and willingness to share the information required for my study, especially on the potential threats encountered by your data center.

Respondent: You are welcome and you can always contact me should you need clarification or further information related to this. All the best for your study.

Interviewer: Thank you Sir. Greatly appreciate that.

Appendix F Analysis of Data Collected in Phase-1 on Threats That Encountered by Data Centers in 34 Agencies in The Malaysian Public Sector

Num.	Threat ID	Types of Threats	Threats Occurred	AGENCIES																																		
				A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16	A17	A18	A19	A20	A21	A22	A23	A24	A25	A26	A27	A28	A29	A30	A31	A32	A33	A34	
1	T1	Introduction of virus, trojan, through unlicensed software/attempts	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2	T2	Malicious codes or Malware attacks /attempts	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
3	T3	Viral Websites - Introduction of virus, trojan and malware through	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
4	T4	Theft and illegal usage/ misuse of personal information captured through Spware.	✓		✓																						✓	✓						✓				
5	T5	Phishing- Theft, disclosure and illegal use of sensitive financial or personal information through fraudulent email or instant messages	✓	✓																																✓	✓	
6	T6	Bluesnarfing- Theft, disclosure of personal information through	✓										✓																							✓		
7	T7	Changing passwords/ accounts of administrator/ user accounts by	✓			✓																														✓	✓	
8	T8	SPAM email	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
9	T9	Formjacking (use of malicious code to steal credit card / other payment																																				
10	T10	Attempts / Tricking computer users into revealing computer security or private information such as	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
11	T11	Network (LAN/ WANI/ WiFi) service failure/	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
12	T12	Network congestion	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
13	T13	Eavesdropping (network function virtualization)	✓			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
14	T14	Traffic sniffing	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
15	T15	Confidentiality compromisation (network	✓	✓		✓	✓	✓																			✓	✓								✓		
16	T16	High volume of packet transmission or flooding	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
17	T17	Control network denial of service attacks	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

18	T18	Aggregation node or nodes attacks	✓		√																																			√																
19	T19	Black hole / Packet drop attacks	✓																																												√	√								
20	T20	Direction of misleading attacks	✓	√		√																																											√							
21	T21	Wormhole attacks	✓									√																																√												
22	T22	Trap doors Sybil attacks	✓		√												√																																							
23	T23	Earthquakes/Tremor	✓		√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√							
24	T24	Flash Flood	✓		√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√							
25	T25	Fire	✓		√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√						
26	T26	Tsunami	✓																																																		√			
27	T27	Haze drought	✓		√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√				
28	T28	Portal / Service disruption/ unavailability	✓	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√				
29	T29	Application Systems failure/ Can not be	✓	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√				
30	T30	Hardware malfunction (Server, Loadbalancer, Storage, Printer, etc)	✓	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√				
31	T31	Software malfunction (OS, webservice, etc)	✓	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√			
32	T32	Failure/ faulty of network equipment (switches, routers, Netapp controller,	✓	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√			
33	T33	Failure/ faulty of security hardware & software (IPS, Firewall, Antivirus, etc)	✓	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√			
34	T34	Faulty communication lines	✓	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√		
35	T35	Electromagnetic leakages/interferences	✓	√		√	√																																																	
36	T36	Power surgetrip/failure	✓										√	√																																										
37	T37	Unpatched vulnerabilities of software	✓	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√		
38	T38	Backup failure, Faulty/ defective storage media (tapes, hard disk	✓	√		√	√	√	√	√	√																																													
39	T39	Failure of database caused by technical faulty hardware/software error.	✓																																																					
40	T40	External power supply failures	✓	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√		
41	T41	Internal power supply disruption/ failure (rack / fuse, etc)	✓	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	

61	T61	Planting logic bombs in application systems	✓																							√	√						√	√																										
62	T62	Deleting proprietary software or designs	✓											√														√	√							√	√																							
63	T63	Deleting backups	✓										√																															√																
64	T64	Denial of services / legitimate access	✓		√								√	√															√	√												√	√																	
65	T65	Denial of information usage / unavailability of data	✓																√										√	√													√																	
66	T66	Service violation attacks	✓		√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√														
67	T67	Distributed denial of service attack	✓	√		√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√												
68	T68	Physical attacks	✓																																														√											
69	T69	Supply chain attack (exploit third party services / software to compromise a final target)																																																										
70	T70	Crypto jacking (secretly run coinminers on victim's device without their knowledge and use their CPU power to mine)																																																										
71	T71	Cloud services attack (targeted attack on cloud services instances)																																																										
72	T72	Pandemics	✓		√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√										
73	T73	Riots	✓		√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√								
74	T74	Wars	✓																																																			√						
75	T75	Terrorist attacks	✓																																																					√				
76	T76	Unauthorised Access to data center facility/ restricted area (illegal entry)	✓		√								√	√																	√	√													√	√	√													
77	T77	Vandalism /theft/loss of hardware/software	✓								√	√																		√	√	√								√	√	√			√	√	√													
78	T78	Website Defacement / Compromised	✓																		√																																		√					
79	T79	Unauthorised access to servers / critical systems	✓																																																				√					
80	T80	Sabotage by Internal staff (integrity)	✓															√																																					√			√		

Appendix G List of Final Threats

No	Threat ID	Threat Title
Category A : Virus, Trojan, Malware, Ransomware, Viral (A program or malicious codes designed to alter the way a computer operates, without the permission or knowledge of the user. A virus replicates and executes itself, usually doing damage to the data stored and computers in the process)		
1	T01	Introduction of virus, Trojan through unlicensed software / attempts.
2	T02	Malicious codes or Malware attacks / attempts.
3	T03	Viral Websites -Introduction of virus, Trojan and malware through illegal websites
Category B : Spyware, Phishing, Bluesnarfing Threats (Spyware is any program that monitors online activities or installs programs without the owner's consent for profit or to capture personal information. Phishers masquerade as a trustworthy person or business and attempt to steal sensitive financial or personal information through fraudulent email or instant messages)		
4	T04	Theft and Illegal usage/ misuse of personal information captured through Spyware.
5	T05	Phishing:- Theft, disclosure and illegal use of sensitive financial or personal information through fraudulent email or instant messages.
6	T06	Bluesnarfing:- Theft, disclosure of personal information through Bluetooth.
7	T07	Changing passwords/ accounts of administrator/ user accounts by masquerading
8	T08	SPAM email.
Category C : Social Engineering (Exploiting the natural tendency of a person to trust and/or exploiting a person's emotional response to obtain computer security and personal information)		
9	T09	Attempts / Tricking computer users into revealing computer security or private information such as passwords, email addresses, etc.

No	Threat ID	Threat Title
Category D : Unsecured Wireless Access Points (WAP) / Network (If WAP, Routers n other network related equipment are not secured, anyone with mobile or other devices will be able to get access to the network and disrupt the network services. Internet based attacks while your computer is connected to the Internet can be subjected to attack through the network communications)		
10	T10	Network (LAN/ WAN/ WiFi) service failure/ unavailability
11	T11	Network congestion.
12	T12	Eavesdropping (network function virtualization).
13	T13	Traffic sniffing.
14	T14	Confidentiality compromisation (network function virtualization).
15	T15	High volume of packet transmission or flooding attacks.
16	T16	Control network denial of service attacks
17	T17	Aggregation node or nodes attacks
18	T18	Black hole / Packet drop attacks
19	T19	Direction of misleading attacks.
20	T20	Wormhole attacks
21	T21	Trap doors Sybil attacks
Category E : Natural Disaster / Environmental (Natural disasters are extreme, sudden events caused by environmental factors that injure people and damage property as well as ICT assets)		
22	T22	Earthquakes/ Tremor
23	T23	Flash Flood
24	T24	Fire
25	T25	Tsunami
26	T26	Haze drought

No	Threat ID	Threat Title
Category F : Technical Threats (Technical threats are threats that caused by hardware and software failures)		
27	T27	Portal / Service disruption/ unavailability
28	T28	Application Systems failure/ Cannot be accessed
29	T29	Hardware malfunction (Server, Load Balancer, Storage, Printer, etc.)
30	T30	Software malfunction (OS, web service, etc.)
31	T31	Failure/ faulty of network equipment (switches, routers, Netapp controller, etc.)
32	T32	Failure/ faulty of security hardware & software (IPS, Firewall, Antivirus, etc.)
33	T33	Faulty communication lines
34	T34	Electromagnetic leakages/ interferences
35	T35	Power surge/ trip/ failure
36	T36	Unpatched vulnerabilities of software (not known to the users until something occurs)
37	T37	Backup failure, Faulty/ defective storage media (tapes, hard disk, cartridges)
38	T38	Failure of database caused by technical faulty hardware/ software error
39	T39	External power supply failures
40	T40	Internal power supply disruption/ failure (rack / fuse, etc)
41	T41	Air conditioning / Ventilation disruption / High temperature
42	T42	Chiller system down/ faulty
43	T43	UPS failure or related hardware faulty (battery & other parts)

No	Threat ID	Threat Title
Category G : Accidental Human Error (The accidental acts are caused by human error without any malicious intent to harm an organization's assets and reputation)		
44	T44	Accidental destruction / corruption of part of or whole database
45	T45	Accidental Deletion of customer data
46	T46	Accidentally Deleting proprietary software
47	T47	Accidentally Deleting backups
48	T48	Accidentally Deleting proprietary designs
49	T49	Incompetency of internal staff
50	T50	Incompetency of External Vendors in outsourced project (misconfiguration of hardware or software)
51	T51	Incompetency of Temporary / Contract staff
52	T52	Hazards posed by janitors or cleaners (vacuum, sweep, wipe, empty thrash)
53	T53	Mishandling of critical ICT assets and other equipment
54	T54	Misleading SOP and Procedures
55	T55	Accidentally Shutting down of hardware (servers, console, etc.)
56	T56	Accidentally Shutting down software (application, software, database, etc.)
Category H : Deliberate Human Threats (The deliberate acts are done with the malicious intent to cause damages to the assets and reputation of an organization)		
57	T57	Deliberate destruction / corruption of part of or whole database
58	T58	Elevation of privilege

No	Threat ID	Threat Title
59	T59	Unauthorised modification or deletion of customer data
60	T60	Planting logic bombs in application systems
61	T61	Deleting proprietary software or designs
62	T62	Deleting backups
63	T63	Denial of services / legitimate access
64	T64	Denial of information usage / unavailability of data
65	T65	Service violation attacks
66	T66	Distributed denial of service attack
67	T67	Physical attacks
68	T68	Pandemics
69	T69	Riots
70	T70	Wars
71	T71	Terrorist attacks
72	T72	Unauthorised Access to data center facility/ restricted area (illegal entry)
73	T73	Vandalism /theft / loss of hardware/ software
74	T74	Website Defacement / Compromised
75	T75	Unauthorised access to servers / critical systems
76	T76	Sabotage by Internal staff (integrity)
77	T77	Sabotage by External Vendors in outsourced project (integrity)
78	T78	Sabotage by Temporary / Contract staff (integrity)
79	T79	Attempts to hack IP/ intrusion/ invasion of network threats
80	T80	SQL injection

No	Threat ID	Threat Title
81	T81	Cross site scripting
82	T82	Data breach / information Leakage
83	T83	Privacy in data mining
84	T84	Control command forged attacks
85	T85	Shutting down of hardware (servers, console, etc)
86	T86	Shutting down software (application, software, database, etc)

Appendix H Approval Letter for Data Collection

PUAN INTHRANI SHAMMUGAM
STUDENT
ADVANCED INFORMATICS SCHOOL (UTM AIS)
UNIVERSITY TECHNOLOGY MALAYSIA,
JALAN SULTAN YAHYA PETRA,
54100, KUALA LUMPUR

Date: 25 June 2018

Dear Madam,

**RE: DATA COLLECTION FOR RESEARCH ON 'INFORMATION SECURITY RISK ASSESSMENT
FRAMEWORK FOR DATA CENTERS IN MALAYSIAN PUBLIC SECTOR'**

Please to inform that the Information Management Division, Ministry of International Trade and Industry has no objection for your request to collect data for your research on Information Security Risk Assessment Framework for Data Centers in The Malaysian Public Sector. However, you are required to adhere to the following conditions.

- i) The data collected must be strictly used for the intended purpose only;
 - ii) You have to work with our staff during the data collection phase; and
 - iii) You are required to get a written approval should you need to share the data with others.
- 2) Your cooperation is highly appreciated.

Yours faithfully,



(HAJI MOHD NADZRI YUSOF)
Chief ICT Security Officer
Information Management Division
Ministry of International Trade and Industry Malaysia

Appendix I Sample Data Collection

RECORDS OF SECURITY INCIDENTS, MINISTRY A (JANUARY 2016 -- DECEMBER 2017)

Num.	Date	Time	Types of Threats	Location	Category (A, B, C, D, E, F, G, H)	Threat ID	No of Entities/Subjects Affected By The Incident						
							Hardware	Network Devices	Applications	Internal Users (Staff)	External Users (Clients)	External Offices/Agencies Under	TOTAL
1	5-Jan-16	9.00am	Network rack failure due to power surge		F	T35	10	20	38	1000	5000	28	6096
2	7-Jan-16	7.30am	internet down		D	T10	10	5	38	1000	5000	28	6081
3	7-Jan-16	2.00pm	Rack Power outage / incoming power failure		F	T35	50	20	38	1000	5000	28	6136
4	12-Jan-16	8.00am	Attempt to hack IP MITI		H	T79	10	10	0	0	0	0	20
5	12-Jan-16	8.10am	Attempt to hack IP MITI		H	T79	10	10	0	0	0	0	20
6	12-Jan-16	8.20am	Attempt to hack IP MITI		H	T79	10	10	0	0	0	0	20
7	12-Jan-16	8.40am	Attempt to hack IP MITI		H	T79	10	10	0	0	0	0	20
8	12-Jan-16	1.40pm	Attempt to hack IP MITI		H	T79	10	10	0	0	0	0	20
9	12-Jan-16	2.00pm	Attempt to hack IP MITI		H	T79	10	10	0	0	0	0	20
10	12-Jan-16	2.20pm	Attempt to hack IP MITI		H	T79	10	10	0	0	0	0	20
11	12-Jan-16	8.20am	SPAM email		B	T8	0	0	1	1000	0	0	1001
12	12-Jan-16	10.20am	SPAM email		B	T8	0	0	1	1000	0	0	1001
13	12-Jan-16	4.20pm	SPAM email		B	T8	0	0	1	1000	0	0	1001
14	13-Jan-16	8.00am	Attempt to hack IP MITI		H	T79	10	10	0	0	0	0	20
15	14-Jan-16	4.15pm	Switch faulty		F	T31	0	1	38	1000	0	0	1039
16	14-Jan-16	4.15pm	internet down		D	T10	10	10	38	1000	5000	28	6086
17	14-Jan-16	11.40am	service unavailable		F	T28	2	0	1	3	500	0	506
18	18-Jan-16	4.00pm	SPAM email		B	T8	0	0	1	1000	0	0	1001
19	27-Jan-16	9.30am	SPAM email		B	T8	0	0	1	1000	0	0	1001
20	5-Feb-16	8.03pm	SPAM email		B	T8	0	0	1	1000	0	0	1001
21	5-Feb-16	4.40pm	SPAM email		B	T8	0	0	1	1000	0	0	1001
22	6-Feb-16	10.51pm	SPAM email		B	T8	0	0	1	1000	0	0	1001
23	15-Feb-16	2.00pm	SPAM email		B	T8	0	0	1	1000	0	0	1001
24	16-Feb-16	9.00am	Network down		D	T10	30	10	38	1000	5000	28	6106
25	16-Feb-16	8.40am	Application system intermittent/ down		F	T28	20	10	38	1000	5000	28	6096
26	16-Feb-16	9.00am	Email down		F	T28	0	0	1	1000	0	0	1001
27	23-Feb-16	8.30am	Power failure		F	T35	30	15	38	1000	5000	28	6111
28	23-Feb-16	8.30am	Telephone (VOIP) down		F	T33	900	30	1	1000	500	28	2459
29	23-Feb-16	8.30am	Internet down		F	T10	10	5	38	1000	5000	28	6081

30	26-Feb-16	7.14pm	SPAM email		B	T8	0	0	1	1000	0	0	1001
31	27-Feb-16		SPAM email		B	T8	0	0	1	1000	0	0	1001
32	2-Mar-16	8.03pm	SPAM email		B	T8	0	0	1	1000	0	0	1001
33	3-Mar-16		VC System down		F	T28	20	5	1	100	0	17	143
34	4-Mar-16		VC System down		F	T28	20	5	1	100	0	17	143
35	5-Mar-16		VC System down		F	T28	20	5	1	100	0	17	143
36	6-Mar-16		VC System down		F	T28	20	5	1	100	0	17	143
37	7-Mar-16		VC System down		F	T28	20	5	1	100	0	17	143
38	25-Mar-16	4.40pm	SPAM email		B	T8	0	0	1	1000	0	0	1001
39	26-Mar-16	7.14pm	SPAM email		B	T8	0	0	1	1000	0	0	1001
40	16-Apr-16	10.51pm	SPAM email		B	T8	0	0	1	1000	0	0	1001
41	21-Apr-16	2.30pm	Internet down		D	T10	10	10	38	1000	5000	28	6086
42	21-Apr-16	2.30pm	System email down		F	T28	0	0	1	1000	0	0	1001
43	5-May-16	10.00am	lose of official email		F	T28	0	0	1	100	0	0	101
44	12-May-16	11.30am	TFIS system can't be accessed - service unavailable		F	T28	0	0	1	35	500	0	536
45	1-Jul-16	9.00am	All virtual machines / server down		F	T29	70	0	20	1000	500	28	1618
46	1-Jul-16	9.00am	Software / Application Failure		F	T28	70	0	38	1000	5000	0	6108
47	16-Jul-16	10.51pm	SPAM email		B	T8	0	0	1	1000	0	0	1001
48	16-Jul-16	4.00pm	Unable to login Sistem Single		F	T28	2	20	1	1000	5000	28	6051
49	1-Aug-16	9.51am	Application system down	TFIS Server	F	T28	0	0	1	35	500	0	536
50	1-Aug-16	9.51am	Application system down	Crystal Report	F	T28	0	0	1	10	0	0	11
51	2-Aug-16	8.03pm	SPAM email		B	T8	0	0	1	1000	0	0	1001
52	9-Aug-16	10.00am	Battery failure	CSPS EMC Storage	F	T43	1	0	0	0	0	0	1
53	9-Aug-16	10.00am	Hardware malfunction	Harddisk EMC Storage	F	T29	1	0	0	0	0	0	1
54	9-Aug-16	11.07am	Application system down	TFIS Server	F	T28	0	0	1	35	500	0	536
55	16-Aug-16	3.23pm	Application system down	TFIS Server	F	T28	0	0	1	35	500	0	536
56	19-Aug-16	5.03pm	Application system down	TFIS Server	F	T28	0	0	1	35	500	0	536
57	22-Aug-16	10.21am	Application system down	TFIS Server	F	T28	0	0	1	35	500	0	536
58	22-Aug-16	12.20pm	Application system down	TFIS Server	F	T28	0	0	1	35	500	0	536
59	22-Aug-16	3.05pm	Application system down	TFIS Server	F	T28	0	0	1	35	500	0	536
60	26-Aug-16	7.14pm	SPAM email		B	T8	0	0	1	1000	0	0	1001
61	26-Aug-16	9.36am	Application system down	Linkup MITI-JPI	D	T10	0	0	1	3	500	0	504
62	6-Sep-16	10.45am	Server malfunction	MYGSOC Server	F	T29	1	0	1	3	0	0	5
63	8-Sep-16	10.16am	Application system down	Consol SANCR	F	T29	0	0	1	35	500	0	536
64	8-Sep-16	10.46am	Application system down	TFIS Server	F	T28	0	0	1	35	500	0	536
65	8-Sep-16	12.21pm	Application system down	TFIS Server	F	T28	0	0	1	35	500	0	536
66	9-Sep-16	2.05pm	Application system down	TFIS Server	F	T28	0	0	1	35	500	0	536
67	9-Sep-16	10.26am	Application system down	Consol SANCR	F	T29	0	0	1	35	500	0	536

68	11-Sep-16		Aircond Failure		F	T41	3	0	0	0	0	0	3
69	15-Sep-16	11.48am	Application system down	TFIS Server	F	T28	0	0	1	35	500	0	536
70	25-Sep-16	4.40pm	SPAM email		B	T8	0	0	1	1000	0	1001	
71	2-Oct-16	9.15am	Deletion of customer data by vendor (accidental)	TFIS Data Folder	G	T45	0	0	1	35	10000	0	10036
72	4-Oct-16	2.01pm	Email from unknown source tried tricking user to reveal personal information (Bill for Parcel)	Email	C	T9	0	0	1	20	0	0	21
73	5-Oct-16	8.03pm	SPAM email		B	T8	0	0	1	1000	0	0	1001
74	5-Oct-16	4.40pm	SPAM email		B	T8	0	0	1	1000	0	0	1001
75	5-Oct-16	10.51pm	SPAM email		B	T8	0	0	1	1000	0	0	1001
76	6-Oct-16	7.14pm	SPAM email		B	T8	0	0	1	1000	0	0	1001
77	6-Oct-16	8.23pm	Email from unknown source tried tricking user to reveal personal information (sending receipt)	Email	C	T9	0	0	1	20	0	0	21
78	6-Oct-16	8.01pm	SPAM email		B	T8	0	0	1	1000	0	0	1001
79	6-Oct-16	9.01pm	SPAM email (Malware Alert)		B	T8	0	0	1	1000	0	0	1001
80	12-Oct-16	9.35am	Application system down	JBoss	F	T28	0	0	1	35	500	0	536
81	21-Oct-16	10.51pm	SPAM email		B	T8	0	0	1	1000	0	0	1001
82	26-Oct-16	9.59am	Application system down	AP Payment	F	T28	0	0	1	35	500	0	536
83	26-Oct-16	10.54am	Application system down	AP Payment	F	T28	0	0	1	35	500	0	536
84	26-Oct-16	4.39pm	Application system down	Linkup MITI-JPJ	D	T10	0	0	1	3	500	0	504
85	26-Oct-16	5.10pm	Application system down	TFIS Server	F	T28	0	0	1	35	500	0	536
86	18-Nov-16	8.01am	Application system down	TFIS Server	F	T28	0	0	1	35	500	0	536
87	21-Nov-16	8.01am	Hardware malfunction	UPS	F	T43	2	0	0	0	0	0	2
88	22-Nov-16	2.30pm	Application system down	EIS	F	T28	0	0	1	58	0	28	87
89	23-Nov-16	4.02pm	Application system down	Linkup MITI-JPJ	D	T10	0	0	1	3	500	0	504
90	23-Nov-16	4.40pm	Hardware malfunction	Firewall	F	T32	1	1	0	0	0	17	19
91	30-Nov-16	10.00am	NetBackup BBU failure	NetBackup Appliance	F	T37	1	0	1	0	0	0	2
92	7-Dec-16	9.45am	Dis-5 error / disk failure	NetBackup Appliance	F	T37	1	0	1	0	0	0	2
93	8-Dec-16	2.04pm	Application system down	TFIS Server	F	T28	0	0	1	35	500	0	536
94	12-Dec-16	8.01am	Line faults	MyMesyuarat	D	T10	0	0	1	80	0	0	81
95	16-Dec-16	12.24pm	Application system down	TFIS Server	F	T28	0	0	1	35	500	0	536
96	21-Dec-16	11.16am	Application system down	TFIS Server	F	T28	0	0	1	35	500	0	536
97	22-Dec-16	4.01pm	SPAM email		B	T8	0	0	1	1000	0	0	1001
98	22-Dec-16	4.01pm	SPAM email		B	T8	0	0	1	1000	0	0	1001
99	22-Dec-16		Deletion of customer data by staff (accidental)	Research Information System Data Folder	G	T45	0	0	1	1000	0	0	1001
100	22-Dec-16		Deletion of customer data by staff (accidental)	My Training System Data Folder	G	T45	0	0	1	1000	0	0	1001

101	4-Jan-17	10.39am	Application system down	TFIS Server	F	T28	0	0	1	35	500	0	536
102	5-Jan-17	12.53pm	Application system down	TFIS Server	F	T28	0	0	1	35	500	0	536
103	8-Jan-17	3.00pm	Hard disk failure	3PAR (Enterprise Storage)	F	T37	1	0	0	0	0	0	1
104	11-Jan-17		SPAM email		B	T8	0	0	1	1000	0	0	1001
105	12-Jan-17	1.00pm	DAC cable malfunction	HP Blade System	F	T31	21	0	0	0	0	0	21
106	13-Jan-17		SPAM email		B	T8	0	0	1	1000	0	0	1001
107	16-Jan-17	10.00am	Hardware malfunction	Netbackup	F	T29	1	0	38	0	0	0	39
108	22-Jan-17	3.00pm	Server SUN Oracle cannot be accessed	Server SUN	F	T29	1	0	3	35	500	0	539
109	24-Jan-17	12.12pm	Application system down	TFIS Server	F	T28	0	0	1	35	500	0	536
110	25-Jan-17	9.00am	SPAM email		B	T8	0	0	1	1000	0	0	1001
111	26-Jan-17	11.21am	Application system down	TFIS Server	F	T28	0	0	1	35	500	0	536
112	27-Jan-17	3.30pm	Application system down	EIS	F	T28	0	0	1	58	0	0	59
113	27-Jan-17	3.39pm	EIS server down - license failed		F	T30	0	0	1	58	0	0	59
114	29-Jan-17	8.00am	SPAM email		B	T8	0	0	1	1000	0	0	1001
115	30-Jan-17	8.00am	SPAM email		B	T8	0	0	1	1000	0	0	1001
116	2-Feb-17	2.02pm	Backup replication failed to functioning		F	T37	1	0	38	0	0	0	39
117	6-Feb-17	11.19am	Backup replication failed to functioning		F	T37	1	0	38	0	0	0	39
118	6-Feb-17	4.00pm	Wifi can not be accessed	VLAN Guest	D	T10	1	10	0	800	0	0	811
119	8-Feb-17	3.04pm	Application system down	TFIS Server	F	T28	0	0	1	35	500	0	536
120	9-Feb-17	9.57am	Application system down	TFIS Server	F	T28	0	0	1	35	500	0	536
121	10-Feb-17	8.07am	Application system down	TFIS Server	F	T28	0	0	1	35	500	0	536
122	10-Feb-17	11.20pm	No power supply	ORACLE SPARC MODE01	F	T40	1	0	1	35	500	0	537
123	11-Feb-17	2.40pm	Hardware malfunction	EMC Storage	F	T29	1	0	0	0	0	0	1
124	14-Feb-17	5.00pm	Backup replication failed to functioning		F	T37	1	0	38	0	0	0	39
125	15-Feb-17		SPAM email		B	T8	0	0	1	1000	0	0	1001
126	15-Feb-17	2.33pm	Hardware malfunction	SPARC T3	F	T29	1	0	1	35	500	0	537
127	22-Feb-17		SPAM email		B	T8	0	0	1	1000	0	0	1001
128	28-Feb-17	12.12pm	Application system down	TFIS Server	F	T28	0	0	1	35	500	0	536
129	1-Mar-17	9.26am	Application system down	TFIS Server	F	T28	0	0	1	35	500	0	536
130	1-Mar-17	10.50am	Application system down	TFIS Server	F	T28	0	0	1	35	500	0	536
131	2-Mar-17	10.44am	Backup replication failed to functioning		F	T37	1	0	38	0	0	0	39
132	3-Mar-17	10.38am	Wifi can not be accessed	Wireless/Wifi Controller	D	T10	1	10	0	800	0	0	811
133	9-Mar-17	11.00am	Access card reader malfunction	Card reader	F	T29	1	0	0	800	0	0	801
134	9-Mar-17	10.14am	Application system down	TFIS Server	F	T28	0	0	1	35	500	0	536
135	10-Mar-17	11.00am	SPAM email		B	T8	0	0	1	1000	0	0	1001

136	15-Mar-17	3.00pm	SPAM email		B	T8	0	0	1	1000	0	0	1001
137	16-Mar-17	3.45pm	Misconfiguration of Firewall HW	Firewall	G	T50	1	1	0	0	0	17	19
138	20-Mar-17	2.00pm	SPAM email		B	T8	0	0	1	1000	0	0	1001
139	20-Mar-17	4.00pm	SPAM email		B	T8	0	0	1	1000	0	0	1001
140	21-Mar-17	2.04pm	Network cable faulty	Informix & Netbackup Server	F	T31	2	0	5	35	500	0	542
141	22-Mar-17	3.35pm	Air Conditionner Light failure	PAC Alarm (Light)	F	T41	1	0	0	0	0	0	1
142	30-Mar-17	9.24am	Application system down	Linkup MITI-JPJ	D	T10	0	0	1	3	500	0	504
143	30-Mar-17	3.39pm	Application system down	Linkup MITI-JPJ	D	T10	0	0	1	3	500	0	504
144	4-Apr-17	5.39pm	Application system down	TFIS Server	F	T28	0	0	1	35	500	0	536
145	4-Apr-17	5.39pm	Application system down	TFIS Server	F	T28	0	0	1	35	500	0	536
146	5-Apr-17	10.13am	Continuous attempts of intrusion by hackers	SSO Server VPN & Load Balancer	H	T79	2	20	38	1000	5000	28	6088
147	5-Apr-17	1.30pm	Continuous attempts of intrusion by hackers	SSO Server VPN & Load Balancer	H	T79	2	20	38	1000	5000	28	6088
148	6-Apr-17	12.07pm	Continuous attempts of intrusion by hackers	Digital Library	H	T79	0	0	1	1000	0	0	1001
149	11-Apr-17	12.00n	Tape media faulty for Netbackup		F	T37	1	0	1	0	0		2
150	13-Apr-17	10.11am	Application system down	AP Payment	F	T28	0	0	1	35	500	0	536
151	17-Apr-17		SPAM email		B	T8	0	0	1	1000	0	0	1001
152	21-Apr-17	4.36pm	Application system down	TFIS Server	F	T28	0	0	1	35	500	0	536
153	25-Apr-17	7.20am	Application system down	TFIS Server	F	T28	0	0	1	35	500	0	536
154	4-May-17	9.05am	Application system down	TFIS Server	F	T28	0	0	1	35	500	0	536
155	9-May-17	10.20am	Hardware malfunction	TFIS Server	F	T29	1	0	1	35	500	0	537
156	11-May-17	10.07am	Application system down	AP Payment	F	T28	0	0	1	35	500	0	536
157	11-May-17	4.53pm	Application system down	Linkup MITI-JPJ	D	T10	0	0	1	3	500	0	504
158	11-May-17	6.21pm	Application system down	Linkup MITI-JPJ	D	T10	0	0	1	3	500	0	504
159	15-May-17		SPAM email		B	T8	0	0	1	1000	0	0	1001
160	15-May-17	11.42am	SPAM email	Email	B	T8	0	0	1	1000	0	0	1001
161	18-May-17	9.30am	Wifi can not be accessed	Wireless/Wifi Controller	D	T10	1	10	0	800	0	0	811
162	20-May-17		SPAM email		B	T8	0	0	1	1000	0	0	1001
163	22-May-17	10.30am	Wifi can not be accessed	Wireless/Wifi Controller	D	T10	1	10	0	800	0	0	811
164	24-May-17	8.40am	Power trip		F	T35	30	15	38	1000	5000	0	6083
165	24-May-17	9.40am	Wifi can not be accessed	Cable / Incoming Packet	D	T10	1	10	0	800	0	0	811
166	24-May-17	9.30pm	Firewall faulty	Firewall Server	F	T29	1	1	0	1000	0	17	1019
167	24-May-17	9.45am	Power cut at whole Data Center	Data Center	F	T35	50	40	38	1000	5000	28	6156

168	26-May-17	11.05pm	Switch faulty	Switch	F	T31	1	10	15	100	0	0	126
169	26-May-17	11.05pm	Firewall faulty	Firewall Server	F	T29	1	1	0	1000	0	17	1019
170	30-May-17	10.38am	Wifi can not be accessed	Wireless/Wifi Controller	D	T10	1	10	0	800	0	0	811
171	30-May-17	11.54pm	Email with malicious code detected by Malware Protection System	Email	A	T2	0	0	1	1000	0	0	1001
172	31-May-17	8.46am	Phishing email	Email	B	T5	0	0	1	100	0	0	101
173	31-May-17	10.00am	Wifi can not be accessed	Wireless/Wifi Controller	D	T10	1	10	0	800	0	0	811
174	1-Jun-17	11.01am	Wifi can not be accessed	Wireless/Wifi Controller & switch	D	T10	1	10	0	800	0	0	811
175	1-Jun-17	2.38pm	Wifi can not be accessed	Wireless/Wifi Controller & switch	D	T10	1	10	0	800	0	0	811
176	1-Jun-17	11.01am	Wifi can not be accessed	Wireless/Wifi Controller	D	T10	1	10	0	800	0	0	811
177	2-Jun-17		SPAM email		B	T8	0	0	1	1000	0	0	1001
178	6-Jun-17	12.12pm	Application system down	TFIS Server	F	T28	0	0	1	35	500	0	536
179	6-Jun-17	11.35am	Wifi can not be accessed	Wireless/Wifi Controller	D	T10	1	10	0	800	0	0	811
180	8-Jun-17	11.01am	Wifi can not be accessed	Wireless/Wifi Controller	D	T10	1	10	0	800	0	0	811
181	13-Jun-17	2.30pm	Phishing email	Email	B	T5	0	0	1	100	0	0	101
182	20-Jun-17	8.00am	Vendor incompetency. Service unavailability (microsoft office) at client site. Vendor did not check/test properly after updating Antivirus patches.	Antivirus Server	G	T50	1	1	38	1000	0	17	1057
183	24-Jun-17		Phishing email		B	T5	0	0	1	100	0	0	101
184	28-Jun-17		Phishing email		B	T5	0	0	1	100	0	0	101
185	28-Jun-17		Phishing email		B	T5	0	0	1	100	0	0	101
186	1-Jul-17		Phishing email		B	T5	0	0	1	100	0	0	101
187	4-Jul-17		Phishing email		B	T5	0	0	1	100	0	0	101
188	4-Jul-17	9.20am	Application system down	TFIS Server	F	T28	0	0	1	35	500	0	536
189	11-Jul-17	10.47am	Application system down	TFIS Server	F	T28	0	0	1	35	500	0	536
190	14-Jul-17	10.47am	Application system down	TFIS Server	F	T28	0	0	1	35	500	0	536
191	24-Jul-17	10.00am	Hardware malfunction	Netbackup	F	T37	1	0	1	0	0	0	2
192	31-Jul-17	11.22am	Application system down	Linkup MITI-JPJ	D	T10	0	0	1	3	500	0	504
193	31-Jul-17	4.45pm	Network congestion	ePCO Server	D	T11	0	0	1	50	1000	0	1051
194	14-Aug-17	4.45pm	Network congestion	ePCO Server	D	T11	0	0	1	50	1000	0	1051

195	15-Aug-17	8.00am	Vendor incompetency. Unavailability of VC System (misconfiguration by vendor during preventive maintenance work the day before)	VC Server	G	T50	20	5	1	100	0	17	143
196	16-Aug-17	9.54 am	Application system down	TFIS Server	F	T28	0	0	1	35	500	0	536
197	16-Aug-17	10.15 am	Application system down	TFIS Server	F	T28	0	0	1	35	500	0	536
198	16-Aug-17	10.15 am	Application system down	AP Payment	F	T28	0	0	1	35	500	0	536
199	16-Aug-17	4.58pm	Application system down	TFIS Server	F	T28	0	0	1	35	500	0	536
200	17-Aug-17	10.15 am	Application system down	AP Payment	F	T28	0	0	1	35	500	0	536
201	21-Aug-17	1.00am	Continuous attempts for intrusion/DDoS by hackers	SSO Server VPN & Load Balancer	H	T79	2	20	1	1000	5000	28	6051
202	24-Aug-17		SPAM email		B	T8	0	0	1	1000	0	0	1001
203	28-Aug-17		SPAM email		B	T8	0	0	1	1000	0	0	1001
204	28-Aug-17		SPAM email		B	T8	0	0	1	1000	0	0	1001
205	11-Sep-17	5.52pm	Application system down	TFIS Server	F	T28	0	0	1	35	500	0	536
206	11-Sep-17	5.53pm	JPJ Link-Up down		D	T10	0	0	1	3	500	0	504
207	13-Sep-17	1.13pm	Email from unknown source tried tricking user to reveal personal information	Email	B	T5	0	0	1	10	0	0	11
208	14-Sep-17		SPAM email		B	T8	0	0	1	1000	0	0	1001
209	14-Sep-17	8.54am	Continuous attempts for intrusion/DDoS by hackers	SSO Server VPN & Load Balancer	H	T79	2	20	1	1000	5000	28	6051
210	14-Sep-17	8.54am	Malware attack attempt detected		A	T2	7	10	15	1000	0	0	1032
211	15-Sep-17		SPAM email		B	T8	0	0	1	1000	0	0	1001
212	15-Sep-17	2.38pm	SANCR Server down		F	T29	0	0	1	35	500	0	536
213	19-Sep-17	14.45pm	ComServer down		F	T29	0	0	1	35	500	0	536
214	27-Sep-17	9.39am	EIS server down		F	T29	0	0	1	58	0	0	59
215	28-Sep-17	5.00pm	Connection failure to TRUST System	TRUST System Server/network	D	T10	1	0	1	20	0	28	50
216	6-Oct-17	10.04am	Crystal Report Module can't be accessed		F	T28	0	0	1	10	0	0	11
217	9-Oct-17	12.04n	System TFIS down		F	T28	0	0	1	35	500	0	536
218	14-Oct-17	9.30am	Power supply disrupted	Storage Controller	F	T40	7	10	15	1000	500	28	1560
219	14-Oct-17	11.58am	Portal can't be accessed	Server Portal	F	T27	9	0	38	1000	1500	28	2575
220	20-Oct-17	9.55am	Data Customs & Webservice JPJ Link-up down.		F	T30	0	0	1	3	500	0	504
221	24-Oct-17		SPAM email		B	T8	0	0	1	1000	0	0	1001
222	25-Oct-17	10.19am	Data Customs can't be accessed, EIS database problem		F	T38	0	0	1	58	0	0	59
223	25-Oct-17	8.41am	Consol ComServer & JPJ Link-up can't be accessed		F	T29	0	0	1	3	500	0	504

224	26-Oct-17	9.44am	System TFIS down		F	T28	0	0	1	35	500	0	536
225	28-Oct-17		SPAM email		B	T8	0	0	1	1000	0	0	1001
226	2-Nov-17		Consol ComServer & JPJ Link-up can't be accessed		F	T29	0	0	1	3	500	0	504
227	5-Nov-17		Microsoft Office unavailable - Clientside		F	T30	0	0	38	1000	0	0	1038
228	8-Nov-17	3.46pm	System TFIS down		F	T28	0	0	1	35	500	0	536
229	9-Nov-17	5.46pm	System TRUST can't be accessed		F	T28	0	0	1	20	0	28	49
230	10-Nov-17	8.00am	System TRUST can't be accessed		F	T28	0	0	1	20	0	28	49
231	10-Nov-17	3.00pm	System TRUST can't be accessed		F	T28	0	0	1	20	0	28	49
232	10-Nov-17	5.15pm	System TFIS down		F	T28	0	0	1	35	500	0	536
233	11-Nov-17		SPAM email		B	T8	0	0	1	1000	0	0	1001
234	11-Nov-17		SPAM email		B	T8	0	0	1	1000	0	0	1001
235	11-Nov-17		SPAM email		B	T8	0	0	1	1000	0	0	1001
236	11-Nov-17		Data loss - Online Saham System		T	T28	0	0	1	50	20000	28	20079
237	14-Nov-17	7.00am	Continuous attempts for intrusion/DDoS by hackers		H	T79	0	10	38	1000	5000	28	6076
238	14-Nov-17	3.00pm	Continuous attempts for intrusion/DDoS by hackers		H	T79	0	10	38	1000	5000	28	6076
239	15-Nov-17	9.00am	Continuous attempts for intrusion/DDoS by hackers		H	T79	0	10	38	1000	5000	28	6076
240	16-Nov-17	8.00am	Continuous attempts for intrusion/DDoS by hackers		H	T79	0	10	38	1000	5000	28	6076
241	16-Nov-17	2.42pm	System EIS can't be accessed		F	T28	0	0	1	58	0	0	59
242	17-Nov-17	3.36pm	System EIS can't be accessed		F	T28	0	0	1	58	0	0	59
243	24-Nov-17	4.22pm	System TRUST can't be accessed		F	T28	0	0	1	20	0	28	49
244	1-Dec-17		SPAM email		B	T8	0	0	1	1000	0	0	1001
245	3-Dec-17		SANCR Server down		F	T29	0	0	1	35	500	0	536
246	3-Dec-17		Crystal Report Module can't be accessed		F	T28	0	0	1	10	0	0	11
247	5-Dec-17		Application system down	TFIS Server	F	T28	0	0	1	35	500	0	536
248	6-Dec-17		Application system down	TFIS Server	F	T28	0	0	1	35	500	0	536
249	6-Dec-17		Application system down	AP Payment	F	T28	0	0	1	35	500	0	536
250	10-Dec-17		SPAM email		B	T8	0	0	1	1000	0	0	1001
251	22-Dec-17		Email undelivered		F	T28	0	0	1	1000	0	0	1001
252	22-Dec-17		Email undelivered		F	T28	0	0	1	1000	0	0	1001
253	22-Dec-17		Email undelivered		F	T28	0	0	1	1000	0	0	1001
254	22-Dec-17		Email undelivered		F	T28	0	0	1	1000	0	0	1001

Appendix J Letter of Verification on Application of the Proposed Risk Assessment Using Survival Analysis Technique

I) Letter from ICT Security Officer of Ministry-A

PUAN INTHRANI SHAMMUGAM
STUDENT
ADVANCED INFORMATICS SCHOOL (UTM AIS)
UNIVERSITY TECHNOLOGY MALAYSIA,
JALAN SULTAN YAHYA PETRA,
54100, KUALA LUMPUR

Date: 20 November 2019

Dear Madam,

RE: LETTER OF APPRECIATION AND VERIFICATION ON THE APPLICATION OF 'INFORMATION SECURITY RISK ASSESSMENT USING SURVIVAL ANALYSIS TECHNIQUE FOR DATA CENTERS IN MALAYSIAN PUBLIC SECTOR'

Please to confirm that the Information Security Risk Assessment using Survival Analysis technique proposed for Data Centers in The Malaysian Public Sector in your study was used in our data center environment to predict the potential threats as well as in improving our security measures in place and maintaining our ISO/IEC 27001:2013 certification. We have successfully obtained the recertification in 2019.

2) Greatly appreciate your cooperation, advice and assistance rendered during the recertification process in our department.

Yours faithfully,



(HAJI MOHD NADZRI YUSOF)
Chief ICT Security Officer
Information Management Division
Ministry of International Trade and Industry Malaysia

II) Letter from Risk Expert in Public Sector

PUAN INTHRANI SHAMMUGAM
STUDENT
ADVANCED INFORMATICS SCHOOL (UTM AIS)
UNIVERSITY TECHNOLOGY MALAYSIA,
JALAN SULTAN YAHYA PETRA,
54100, KUALA LUMPUR

Date: 15 May 2021

Dear Madam,

RE: LETTER OF VERIFICATION ON THE APPLICATION OF 'INFORMATION SECURITY RISK ASSESSMENT USING SURVIVAL ANALYSIS TECHNIQUE FOR DATA CENTERS IN MALAYSIAN PUBLIC SECTOR'

With reference to the above, please to inform that the above mentioned Risk Assessment method has been reviewed and I would like to confirm that the proposed Information Security Risk Assessment using Survival Analysis technique in this study is relevant and can be applied for Data Center environment in The Malaysian Public Sector.

Thank you,



(DR. JAYALETCHUMI A/P T. SAMBANTHA MOORTHY)
ICT Officer
Information Management Division
Public Works Department
drjaya@jkr.gov.my

III) Letter from Risk Expert in MAMPU

PUAN INTHRANI SHAMMUGAM
STUDENT
ADVANCED INFORMATICS SCHOOL (UTM AIS)
UNIVERSITY TECHNOLOGY MALAYSIA,
JALAN SULTAN YAHYA PETRA,
54100, KUALA LUMPUR

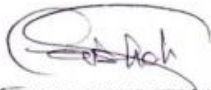
Date: 10 June 2021

Dear Madam,

RE: LETTER OF VERIFICATION ON THE APPLICATION OF THE PROPOSED 'INFORMATION SECURITY RISK ASSESSMENT USING SURVIVAL ANALYSIS TECHNIQUE FOR DATA CENTERS IN THE MALAYSIAN PUBLIC SECTOR'

Please to confirm that the proposed Information Security Risk Assessment using Survival Analysis technique for data centers in the Malaysian Public Sector in your study has been reviewed. The proposed Risk Assessment method in your study found to be suitable to apply in data center environment, in the Malaysian Public Sector to predict the potential information security threats effectively and will greatly help the information security officers.

Yours faithfully,



(AATSHAH BINTI DATO' ABU BAKAR)
Senior Principal Assistant Director
ICT Consultancy Unit
Malaysian Administrative Modernization and Management Planning Unit (MAMPU)
Prime Minister Department

**Counting Process (CP)
Event Report**

for 731 days

from 1 January 2016 to 31 December 2017

Appendix L Analysis of recorded events using counting processing format

```
> CoxModel.2 <- coxph(Surv(start, stop, status, type="counting") ~ t01 + t02 + t03 + t04 + t05 + t06 + t07 + t08 +
t09 + t10 + t11 + t12 + t13 + t14 + t15 + t16 + t17 + t18 + t19 + t20 + t21 + t22 + t23 + t24 + t25 + t26 + t27
+ t28 + t29 + t30 + t31 + t32 + t33 + t34 + t35 + t36 + t37 + t38 + t39 + t40 + t41 + t42 + t43 + t44 + t45 + t46
+ t47 + t48 + t49 + t50 + t51 + t52 + t53 + t54 + t55 + t56 + t57 + t58 + t59 + t60 + t61 + t62 + t63 + t64 + t65
+ t66 + t67 + t68 + t69 + t70 + t71 + t72 + t73 + t74 + t75 + t76 + t77 + t78 + t79 + t80 + t81 + t82 + t83 + t84
+ t85 + t86, method="efron", data=Dataset)
```

```
> summary(CoxModel.2)
```

```
Call: coxph(formula = Surv(start, stop, status, type = "counting") ~ t01 + t02 + t03 + t04 + t05 + t06 + t07 + t08 + t09
+ t10 + t11 + t12 + t13 + t14 + t15 + t16 + t17 + t18 + t19 + t20 + t21 + t22 + t23 + t24 + t25 + t26 + t27 + t28 +
t29 + t30 + t31 + t32 + t33 + t34 + t35 + t36 + t37 + t38 + t39 + t40 + t41 + t42 + t43 + t44 + t45 + t46 + t47 + t48 +
t49 + t50 + t51 + t52 + t53 + t54 + t55 + t56 + t57 + t58 + t59 + t60 + t61 + t62 + t63 + t64 + t65 + t66 + t67 + t68 + t69
+ t70 + t71 + t72 + t73 + t74 + t75 + t76 + t77 + t78 + t79 + t80 + t81 + t82 + t83 + t84 + t85 + t86, data = Dataset,
method = "efron")
```

n= 528868, number of events= 522840

	coef	exp(coef)	se(coef)	z	Pr(> z)	
t01	NA	NA	0.00	NA	NA	
t02	-1.03	0.36	0.03	-35.65	< 2e-16	***
t03	NA	NA	0.00	NA	NA	
t04	NA	NA	0.00	NA	NA	
t05	1.34	3.83	0.02	63.64	< 2e-16	***
t06	NA	NA	0.00	NA	NA	
t07	NA	NA	0.00	NA	NA	
t08	1.61	5.02	0.01	126.29	< 2e-16	***
t09	10.13	25190.00	2.47	4.10	0.00	***
t10	0.77	2.15	0.01	104.41	< 2e-16	***
t11	9.01	8218.00	1.56	5.78	0.00	***
t12	NA	NA	0.00	NA	NA	
t13	NA	NA	0.00	NA	NA	
t14	NA	NA	0.00	NA	NA	
t15	NA	NA	0.00	NA	NA	
t16	NA	NA	0.00	NA	NA	
t17	NA	NA	0.00	NA	NA	
t18	NA	NA	0.00	NA	NA	
t19	NA	NA	0.00	NA	NA	
t20	NA	NA	0.00	NA	NA	
t21	NA	NA	0.00	NA	NA	
t22	NA	NA	0.00	NA	NA	
t23	NA	NA	0.00	NA	NA	
t24	NA	NA	0.00	NA	NA	
t25	NA	NA	0.00	NA	NA	
t26	NA	NA	0.00	NA	NA	

t27	-12.07	0.00	2.97	-4.06	0.00	***
t28	-2.39	0.09	0.01	-183.91	< 2e-16	***
t29	-1.41	0.24	0.01	-100.54	< 2e-16	***
t30	10.95	57220.00	1.20	9.13	< 2e-16	***
t31	-2.14	0.12	0.04	-55.68	< 2e-16	***
t32	-16.21	0.00	3.53	-4.59	0.00	***
t33	NA	NA	0.00	NA	NA	
t34	NA	NA	0.00	NA	NA	
t35	-10.41	0.00	0.80	-12.96	< 2e-16	***
t36	NA	NA	0.00	NA	NA	
t37	-2.37	0.09	0.04	-63.90	< 2e-16	***
t38	0.01	1.01	0.03	0.39	0.70	
t39	NA	NA	0.00	NA	NA	
t40	1.93	6.91	0.06	34.88	< 2e-16	***
t41	NA	NA	0.00	NA	NA	
t42	NA	NA	0.00	NA	NA	
t43	1.13	3.10	0.06	18.25	< 2e-16	***
t44	NA	NA	0.00	NA	NA	
t45	-1.07	0.34	0.05	-22.77	< 2e-16	***
t46	NA	NA	0.00	NA	NA	
t47	NA	NA	0.00	NA	NA	
t48	NA	NA	0.00	NA	NA	
t49	NA	NA	0.00	NA	NA	
t50	-2.65	0.07	0.03	-97.95	< 2e-16	***
t51	NA	NA	0.00	NA	NA	
t52	NA	NA	0.00	NA	NA	
t53	NA	NA	0.00	NA	NA	
t54	NA	NA	0.00	NA	NA	
t55	NA	NA	0.00	NA	NA	
t56	NA	NA	0.00	NA	NA	
t57	NA	NA	0.00	NA	NA	
t58	NA	NA	0.00	NA	NA	
t59	NA	NA	0.00	NA	NA	
t60	NA	NA	0.00	NA	NA	
t61	NA	NA	0.00	NA	NA	
t62	NA	NA	0.00	NA	NA	
t63	NA	NA	0.00	NA	NA	
t64	NA	NA	0.00	NA	NA	
t65	NA	NA	0.00	NA	NA	
t66	NA	NA	0.00	NA	NA	
t67	NA	NA	0.00	NA	NA	
t68	NA	NA	0.00	NA	NA	
t69	NA	NA	0.00	NA	NA	
t70	NA	NA	0.00	NA	NA	
t71	NA	NA	0.00	NA	NA	

t72	NA	NA	0.00	NA	NA	
t73	NA	NA	0.00	NA	NA	
t74	NA	NA	0.00	NA	NA	
t75	NA	NA	0.00	NA	NA	
t76	NA	NA	0.00	NA	NA	
t77	NA	NA	0.00	NA	NA	
t78	NA	NA	0.00	NA	NA	
t79	-2.03	0.13	0.03	-62.09	< 2e-16	***
t80	NA	NA	0.00	NA	NA	
t81	NA	NA	0.00	NA	NA	
t82	NA	NA	0.00	NA	NA	
t83	NA	NA	0.00	NA	NA	
t84	NA	NA	0.00	NA	NA	
t85	NA	NA	0.00	NA	NA	
t86	NA	NA	0.00	NA	NA	

Signif. codes: 0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

	exp(coef)	exp(-coef)	lower .95	upper .95
t01	NA	NA	NA	NA
t02	0.36	2.79	0.34	0.38
t03	NA	NA	NA	NA
t04	NA	NA	NA	NA
t05	3.83	0.26	3.68	3.99
t06	NA	NA	NA	NA
t07	NA	NA	NA	NA
t08	5.02	0.20	4.90	5.15
t09	25190.00	0.00	198.30	3201000.00
t10	2.15	0.46	2.12	2.18
t11	8218.00	0.00	386.00	174900.00
t12	NA	NA	NA	NA
t13	NA	NA	NA	NA
t14	NA	NA	NA	NA
t15	NA	NA	NA	NA
t16	NA	NA	NA	NA
t17	NA	NA	NA	NA
t18	NA	NA	NA	NA
t19	NA	NA	NA	NA
t20	NA	NA	NA	NA
t21	NA	NA	NA	NA
t22	NA	NA	NA	NA
t23	NA	NA	NA	NA

t24	NA	NA	NA	NA
t25	NA	NA	NA	NA
t26	NA	NA	NA	NA
t27	0.00	175200.00	0.00	0.00
t28	0.09	10.90	0.09	0.09
t29	0.24	4.10	0.24	0.25
t30	57220.00	0.00	5446.00	601200.00
t31	0.12	8.46	0.11	0.13
t32	0.00	10950000.00	0.00	0.00
t33	NA	NA	NA	NA
t34	NA	NA	NA	NA
t35	0.00	33090.00	0.00	0.00
t36	NA	NA	NA	NA
t37	0.09	10.64	0.09	0.10
t38	1.01	0.99	0.95	1.09
t39	NA	NA	NA	NA
t40	6.91	0.14	6.20	7.70
t41	NA	NA	NA	NA
t42	NA	NA	NA	NA
t43	3.10	0.32	2.75	3.50
t44	NA	NA	NA	NA
t45	0.34	2.92	0.31	0.38
t46	NA	NA	NA	NA
t47	NA	NA	NA	NA
t48	NA	NA	NA	NA
t49	NA	NA	NA	NA
t50	0.07	14.15	0.07	0.07
t51	NA	NA	NA	NA
t52	NA	NA	NA	NA
t53	NA	NA	NA	NA
t54	NA	NA	NA	NA
t55	NA	NA	NA	NA
t56	NA	NA	NA	NA
t57	NA	NA	NA	NA
t58	NA	NA	NA	NA
t59	NA	NA	NA	NA
t60	NA	NA	NA	NA
t61	NA	NA	NA	NA
t62	NA	NA	NA	NA
t63	NA	NA	NA	NA
t64	NA	NA	NA	NA
t65	NA	NA	NA	NA
t66	NA	NA	NA	NA
t67	NA	NA	NA	NA
t68	NA	NA	NA	NA

t69	NA	NA	NA	NA
t70	NA	NA	NA	NA
t71	NA	NA	NA	NA
t72	NA	NA	NA	NA
t73	NA	NA	NA	NA
t74	NA	NA	NA	NA
t75	NA	NA	NA	NA
t76	NA	NA	NA	NA
t77	NA	NA	NA	NA
t78	NA	NA	NA	NA
t79	0.13	7.65	0.12	0.14
t80	NA	NA	NA	NA
t81	NA	NA	NA	NA
t82	NA	NA	NA	NA
t83	NA	NA	NA	NA
t84	NA	NA	NA	NA
t85	NA	NA	NA	NA
t86	NA	NA	NA	NA

LIST OF PUBLICATIONS

Index Journal

1. **Shammugam, I.**, Narayana Samy, G., Magalingam, P., Maarop, N., Perumal, S., & Shanmugam, B. (2021). Information security threats encountered by Malaysian public sector data centers. *Indonesian Journal of Electrical Engineering and Computer Science*, 21(3), 1820-1829. doi:<https://doi.org/10.11591/ijeecs.v21.i3>