

**CYBER SECURITY CAPABILITY MATURITY MODEL
USING MAQASID AL-SHARI‘AH APPROACH**

BY

NADWIYAH BINTI MOHAMED RIDZA

**A thesis submitted in fulfilment of the requirement for the
degree of Master of Computer Science**

**Kulliyyah of Information and Communication Technology
(KICT)
International Islamic University Malaysia**

FEBRUARY 2020

ABSTRACT

Knowing how vulnerable an organisation or a country is towards cyberattacks, is referred to as Cyber Security Index or Maturity Level. Such an index is important to evaluate one's level of vulnerability to cyber threats and its defense readiness. Various cyber security models are initiated and applied across the globe as tools towards measuring the mentioned index. These models in particular provide us with indicators as to how ready an organisation or a country react to attacks and what are the steps to be taken to alleviate the situation. However, although most of the existing cyber security models excel in determining one's cyber security maturity level, the results produced only indicated the degree of practice based on the evidence presented by a country or an organisation for each criterion underlined in each model. It stops short from further explaining what the fundamental problem is: the human factor. Human beings play a very important role in cyber security. Unlike policy, technology and process which are deterministic in nature, human beings are by nature random and complex. Consequently, this unpredictable nature of people and morality issue causes humans to be regarded as the major factor affecting the level of cyber security readiness. Maqasid Al-Shari'ah supports the objectives of Shari'ah through the preservation of five elements: (1) Protection of Deen (faith), (2) Protection of Nafs (life), (3) Protection of 'Aql (intellect), (4) Protection of Nasl (lineage) and (5) Protection of Mal (wealth). Preservation of these five elements is significant for cyber security maturity. Therefore, this research is proposing the use of Maqasid Al-Shari'ah to address the human factor centred on morality as described above. Results will be categorised into the aforementioned five elements. Based on this approach, an organisation will not only be able to determine its maturity level, but interestingly the result will reveal to what extent the organisation's decision making to protect its assets comply with Islamic morality. This work aims to develop a Cyber security Capability Maturity Model guided by Maqasid Al-Shari'ah (known as MS-C2M2) which comprehensively covers both moral and physical aspects of human beings. Its success will undoubtedly demonstrate the usefulness of Maqasid Al-Shari'ah principle, as well as benefiting cyber security maturity models. The MS-C2M2 will be manifested through the development of a prototype system known as Maqasid al Shari'ah Cyber Security Barometer that captures organisations' input which later produces the corresponding cyber security maturity levels. A few subject matter experts in both areas i.e. Cyber security and Maqasid Al-Shari'ah were referred to, to evaluate and validate the reliability of the prototype's content and functionality. After being validated, eighteen organisations from various industries and backgrounds were approached to test the prototype tool. However, only three organisations had gotten back and participated. Coincidentally, the participating organisations were those with good cyber security readiness. For the purpose of comparison, two additional mock organisations were created with poor performances (after going through the barometer) to give ideas on what results do organisations with poor cyber security readiness produced. The feedback received from the survey circulated afterwards showed that the respondents are satisfied with the results produced by the Maqasid al Shari'ah Cyber Security Barometer.

خلاصة البحث

يُشار إلى معرفة مدى تأثير أي منظمة أو بلد بالهجمات الإلكترونية ، كمؤشر أمان الإنترنت أو مستوى النضج. مثل هذا الفهرس مهم لتقييم مستوى تعرض الفرد للتهديدات السيبرانية واستعداده للدفاع. يتم إطلاق نماذج أمان الإنترنت المختلفة وتطبيقها في جميع أنحاء العالم كأدوات لقياس الفهرس المذكور. تزودنا هذه النماذج على وجه الخصوص بمؤشرات حول مدى استعداد منظمة أو دولة للرد على الهجمات وما هي الخطوات التي يجب اتخاذها لتخفيف الضرر من هذه الهجمات. ومع ذلك ، على الرغم من أن معظم نماذج الأمان السيبراني الحالية تتفوق في تحديد مستوى نضج الأمان السيبراني ، فإن النتائج التي تم الحصول عليها تشير فقط إلى درجة الممارسة القائمة على الأدلة المقدمة من بلد أو مؤسسة لكل معيار تم التأكيد عليه في كل نموذج . توقف - باختصار- عن شرح المشكلة الأساسية: هو العامل البشري. يلعب البشر دوراً مهماً جداً في مجال الأمان السيبراني. على عكس السياسة والتكنولوجيا والعملية الحتمية في الطبيعة ، فإن البشر بطبيعتهم عشوائيون ومعدون. وبالتالي ، فإن هذه الطبيعة غير المتوقعة للأشخاص وقضية الأخلاق تجعل البشر يعتبرون العامل الرئيسي الذي يؤثر على مستوى استعداد الأمان السيبراني. يدعم "مقاصد الشريعة" أهداف الشريعة من خلال الحفاظ على خمسة عناصر: (1) حماية الدين ، (2) حماية النفس، (3) حماية العقل ، (4) حماية النسل (5) حماية المال. الحفاظ على هذه العناصر الخمسة مهم لنضج الأمان السيبراني. لذلك ، يقترح هذا البحث استخدام مقاصد الشريعة لمعالجة العامل البشري المتمركز حول الأخلاق كما هو موضح أعلاه. سيتم تصنيف النتائج في العناصر الخمسة المذكورة أعلاه. بناءً على هذا النهج ، لن تكون المنظمة قادرة على تحديد مستوى نضجها فحسب ، ولكن المثير للاهتمام أن النتيجة ستكشف إلى أي مدى يتوافق قرار المنظمة لحماية أصولها مع الأخلاق الإسلامية. يهدف هذا العمل إلى تطوير نموذج نضج القدرة على الأمان السيبراني يسترشد بمقاصد الشريعة (المعروفة باسم MS-C2M2) والتي تغطي بشكل شامل الجوانب المعنوية والمادية للبشر. مما لا شك فيه أن نجاحها سوف يُظهر فوائد لمبادئ المقاصد الشرعية ، وكذلك الاستفادة من نماذج نضج الأمان السيبراني. سوف يتجلى نموذج MS-C2M2 من خلال تطوير نظام نموذجي أولي يعرف باسم مقاصد الشريعة للأمان السيبراني الذي يلتقط مدخلات المنظمات التي تنتج فيما بعد مستويات نضج الأمان السيبراني. تمت الإشارة إلى عدد قليل من خبراء الموضوعات في كلا المجالين ، أي الأمان السيبراني ومقاصد الشريعة ، لتقييم وموثوقية محتوى النموذج الأولي ووظائفه. بعد التحقق من صحتها ، تم الاتصال بثمانية عشر منظمة من مختلف الصناعات والخلفيات لاختبار أداة النموذج الأولي. ومع ذلك ، فإن ثلاث منظمات فقط قد عادت وشاركت. من قبيل الصدفة ، كانت المنظمات المشاركة هي تلك التي لديها استعداد جيد للأمان السيبراني. لغرض المقارنة ، تم إنشاء منطمتين وهميتين إضافيتين بأداء ضعيف (بعد المرور بالمقياس) لإعطاء أفكار حول النتائج التي تنتجها المؤسسات ذات الاستعداد السيئ للأمان السيبراني. أظهرت التعليقات التي تم تلقيها من الاستطلاع الذي تم توزيعه بعد ذلك أن المشاركين راضون عن النتائج التي تم الحصول عليها من مقياس الأمان الشرعي في مقاصد الشريعة.

APPROVAL PAGE

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

.....
Normaziah Binti Abdul Aziz
Supervisor

.....
Aznan Zuhid Bin Saidin
Co-Supervisor

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

.....
Noor Hasrul Nizan Bin
Mohammad Noor
Internal Examiner

.....
Omar Bin Zakaria
External Examiner

This thesis was submitted to the Department of Computer Science and is accepted as a fulfilment of the requirement for the degree of Master of Computer Science.

.....
Raini Binti Hassan
Head, Department of Computer
Science

This thesis was submitted to the Kulliyah of Information and Communication Technology (KICT) and is accepted as a fulfilment of the requirement for the degree of Master of Computer Science.

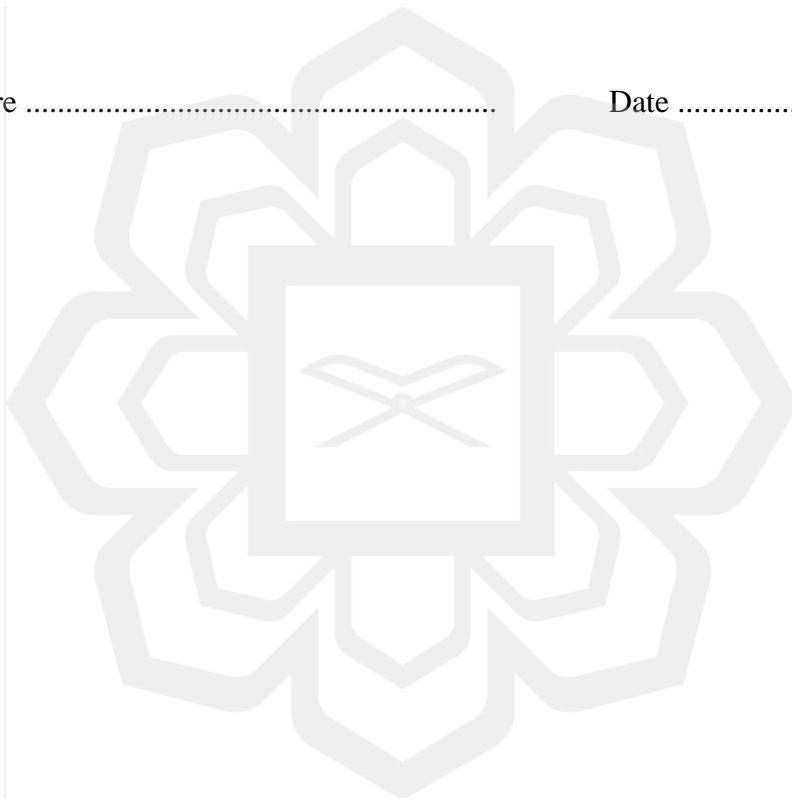
.....
Abdul Wahab Bin Abdul Rahman
Dean, Kulliyah of Information
and Communication Technology
(KICT)

DECLARATION

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

Nadwiyah binti Mohamed Ridza

Signature Date



INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

**DECLARATION OF COPYRIGHT AND AFFIRMATION OF
FAIR USE OF UNPUBLISHED RESEARCH**

**CYBER SECURITY CAPABILITY MATURITY MODEL USING
MAQASID AL-SHARI‘AH APPROACH**

I declare that the copyright holders of this thesis are jointly owned by the student and IIUM.

Copyright © 2020 Nadwiyah binti Mohamed Ridza and International Islamic University Malaysia.
All rights reserved.

No part of this unpublished research may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without prior written permission of the copyright holder except as provided below

1. Any material contained in or derived from this unpublished research may be used by others in their writing with due acknowledgement.
2. IIUM or its library will have the right to make and transmit copies (print or electronic) for institutional and academic purposes.
3. The IIUM library will have the right to make, store in a retrieved system and supply copies of this unpublished research if requested by other universities and research libraries.

By signing this form, I acknowledged that I have read and understand the IIUM Intellectual Property Right and Commercialization policy.

Affirmed by Nadwiyah binti Mohamed Ridza

.....
Signature

.....
Date



This thesis is dedicated to my parents

Mohamed Ridza and Latifah.

Thank you for supporting and believing in me.

Alhamdulillah, I did it!

ACKNOWLEDGEMENTS

First and foremost, I express my gratitude to Allah s.w.t for through His blessings I managed to complete this Thesis.

My utmost appreciation to my principal supervisor Dr. Normaziah binti Abdul Aziz and co-supervisor Dr. Aznan Zuhid bin Saidin for their continuous guidance and supervision. Thank you also to my parents (Mohamed Ridza & Latifah), close family (siblings Sulaiman and Nasuha; sister-in-law Nurul 'Amirah; nephews Naqib Rayyan, Naufal Rifqi, Najmi Rayqal and grandmother Halijah) and friends (Siti Aisyah Ismail and Narieta Bukhari) for being there for me.



TABLE OF CONTENTS

Abstract	ii
Abstract in Arabic	iii
Approval Page.....	iv
Declaration	v
Copyright Page.....	vi
Dedication	vii
Acknowledgements	viii
List of Tables	xiii
List of Figures	xv
List of Abbreviations	xix
CHAPTER ONE: INTRODUCTION	1
1.1 Background.....	1
1.1.1 The Need for Cyber security	1
1.1.2 Reasons for the Use of Maqasid Al-Shari‘ah.....	6
1.2 Statement of the Problem.....	9
1.3 Research Objectives (RO)	11
1.4 Research Questions (RQ)	11
1.5 Research Hypothesis.....	12
1.6 Scope of the Research.....	13
1.7 Significance of the Study.....	15
1.8 Thesis Structure	15
1.9 Chapter Summary	17
CHAPTER TWO: LITERATURE REVIEW	18
2.1 Chapter Introduction	18
2.2 Capability Maturity Model (CMM).....	18
2.3 Maturity Models Of Different Industries.....	21
2.3.1 Game Maturity Model.....	21
2.3.2 eTourism Communication Maturity Model (eTcoMM)	23
2.3.3 Financial Management Maturity Model	25
2.3.4 Summary of the Aim of Maturity Models used in Different Industries	26
2.4 Maturity Models in Cyber security: for Measuring a Country’s Cyber security Readiness	26
2.4.1 Cyber security Capacity Maturity Model for Nations (CMM)	29
2.4.2 Cyber Maturity in the Asia-Pacific Region.....	30
2.4.3 Cyber Readiness Index 2.0.....	31
2.4.4 Comparison of Several Existing C2M2 (Country Level)	32
2.5 Maturity Models in Cyber security: for Measuring an Organisation’s Cyber security Readiness	35
2.5.1 Cyber Security Culture Barometer.....	36
2.5.2 Cybersecurity Posture Assessment	38
2.5.3 NIST Maturity Self-Assessment Survey.....	42
2.5.4 Comparison of Several Existing C2M2 (Organisation Level).....	46

2.6	The Principle of Maqasid Al-Shari'ah.....	49
2.7	Application of Maqasid Al-Shari'ah in Different Industries	53
2.7.1	Islamic Finance	53
2.7.2	Islamic Tourism	54
2.8	The MS-C2M2: a New Perspective of C2M2	55
2.9	Chapter Summary	56
CHAPTER THREE: RESEARCH METHODS AND DESIGN		58
3.1	Chapter Introduction	58
3.2	Research Methodology	58
3.2.1	Literature Review Phase	59
3.2.2	Design and Development Phase.....	60
3.2.3	Testing Phase	60
3.2.4	Results Analysis Phase.....	61
3.2.5	Research Completion Phase.....	61
3.3	Design of the Prototype Tool.....	61
3.3.1	Functional Requirements	61
3.3.1.1	The Initial Designs of the Prototype Tool	63
3.3.1.2	The System Architecture Design	66
3.3.1.3	The Data Flow Diagram	67
3.3.2	Security Requirements in the Prototype Tool	68
3.3.2.1	Admin Login.....	69
3.3.2.2	Hyper Text Transfer Protocol Secure (HTTPS).....	69
3.3.2.3	Input/output Validation.....	69
3.3.2.4	On Screen Results Display Time Limit.....	69
3.4	Content Design of the MS-C2M2.....	70
3.4.1	The Identification of All Attributes Necessary in the Making of the MS-C2M2 Framework	70
3.4.2	A Possible Relationship Between the Three Main Attributes.....	71
3.4.3	Relating Maqasid Al- Shari'ah to Cyber security	71
3.4.4	Questionnaire in the Prototype Tool	72
3.4.5	A Compilation of the Existing Cyber security Maturity Models' Questionnaires	75
3.4.6	The Structure of the Questionnaire	77
3.5	Chapter Summary	78
CHAPTER FOUR: FRAMEWORK OF MAQASID AL-SHARI'AH IN CYBER SECURITY READINESS AND ITS IMPLEMENTATION.....		79
4.1	Chapter Introduction	79
4.2	The MS-C2M2 Framework	79
4.2.1	The Inclusion of the Maqasid Al-Shari'ah Elements in the Questionnaire	79
4.2.2	The Calculation of the Results	81
4.2.3	The Cyber security Maturity Level	81
4.2.4	Daruriyyat, Hajiyyat and Tahsiniyyat in Organisations.....	86
4.3	The Formula.....	88
4.3.1	The Formula for Calculating the Percentage for Reaching Agile	88

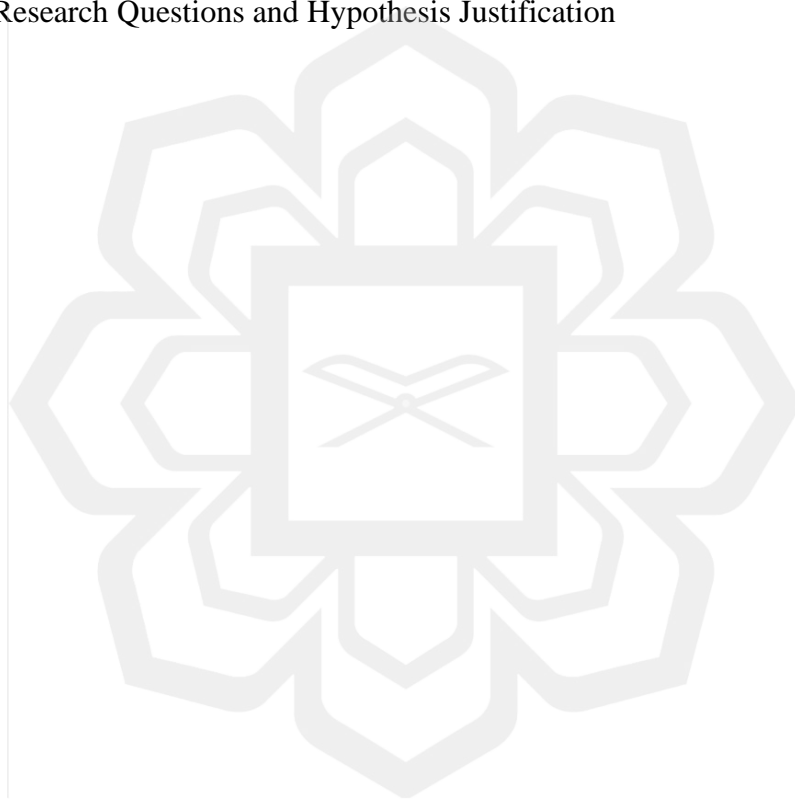
4.3.2 The Formula of Determining the Range of a Cyber security Maturity Level	90
4.3.2.1 Step by Step for Determining Range for Dimension 1,2,3 and 5.....	90
4.3.2.2 Step by Step for Determining Range for Dimension 4.....	92
4.3.3 The Formula of Determining the Colour Representing Maturity levels of a Dimension	93
4.4 Features of the Maqasid al Shari‘ah Cyber Security Barometer	96
4.4.1 Features that are Accessible and Manageable Only by the Administrators	96
4.4.1.1 The Main Menu	96
4.4.1.2 A Form to Add Details of a New Organisation	97
4.4.1.3 A Record of All Participated Organisations	98
4.4.1.4 A Form to Add a New Question	98
4.4.1.5 A Record of All Questions	99
4.4.1.6 A Form to Add a New Checklist	100
4.4.1.7 A Record of All Checklist	100
4.4.1.8 A List of Results	101
4.4.2 Features that are Visible to Both Administrators and Respondents.....	101
4.4.2.1 The Dashboard.....	101
4.4.2.2 The Main Menu	102
4.4.2.3 Organisation Info Tab.....	103
4.4.2.4 Questionnaire Tab.....	104
4.4.2.5 Results and Maturity Level Tab	105
4.5 The Security Features of the Barometer	105
4.5.1 The Log In Menu	105
4.5.2 The SSL Certificate.....	106
4.5.3 The Time Limit Error Page.....	106
4.6 The Questionnaire.....	107
4.7 The Checklist	108
4.8 Validation by Subject Matter Experts.....	109
4.9 Pilot Test in Organisations.....	110
4.10 Chapter Summary	110
CHAPTER FIVE: RESULTS AND DISCUSSIONS.....	112
5.1 Chapter Introduction	112
5.2 Understanding the Results Display.....	112
5.3 Results and Analysis.....	114
5.3.1 Results for ORG-1	116
5.3.1.1 Cyber security Maturity Level.....	116
5.3.1.2 Results with Regard to the Core Elements of Maqasid Al-Shari‘ah (by Dimensions).....	118
5.3.2 Results for ADD-1	133
5.3.2.1 Cyber security Maturity Level.....	133
5.3.2.2 Results with Regard to the Core Elements of Maqasid Al-Shari‘ah (by Dimensions).....	135
5.3.3 Results for ORG-2	150
5.3.3.1 Cyber security Maturity Level.....	150

5.3.3.2 Results with Regard to the Core Elements of Maqasid Al-Shari‘ah (by Dimensions).....	152
5.3.4 Results for ORG-3	160
5.3.5 Results for ADD-2	160
5.3.6 Summary of the Results	160
5.4 Additional Matters	164
5.4.1 Organisations Participation	164
5.4.2 Satisfaction Level of Respondents	164
5.4.2.1 Experts Responses	165
5.4.2.2 Organisations Responses	165
5.4.2.3 Overall Response Evaluation.....	166
5.4.2.4 Experts Testimony on the Maqasid al Shari‘ah Cyber Security Barometer	167
5.5 Chapter Summary	168
CHAPTER SIX: CONCLUSION AND MOVING FORWARD.....	169
6.1 Chapter Introduction	169
6.2 Summary of Findings	170
6.3 Contribution.....	176
6.4 Limitation and Future Work	177
CONFERENCES, PUBLICATIONS & RECOGNITIONS	178
REFERENCES.....	179
APPENDIX 1: LITERATURE REVIEW MAP	185
APPENDIX 2: USER’S GUIDE.....	186
APPENDIX 3: THE QUESTIONNAIRE.....	198
APPENDIX 4: A LIST OF HOW THE QUESTIONNAIRE CAN BE RELATED TO THE MAQASID AL-SHARI‘AH CORE ELEMENTS, TOGETHER WITH THEIR GENERAL EXPLANATIONS	208
APPENDIX 5: CYBER SECURITY MATURITY LEVELS EXPLAINED IN THE CONTEXT OF AN ORGANISATION (IN GENERAL).....	220
APPENDIX 6: THE CHECKLIST	226
APPENDIX 7: THE INVITATION LETTER (DRAFT)	229
APPENDIX 8: THE PRIVACY STATEMENT.....	230
APPENDIX 9: RESULTS OF ORG-3 AND ADD-2	231
APPENDIX 10: MALAYSIA TECHNOLOGY EXPO (MTE 2019).....	246

LIST OF TABLES

<u>Table No.</u>		<u>Page No.</u>
1.1	Examples of Terminologies Used to Describe the Nature of Cyber Threats with their Definitions	3
1.2	Linking the Research Questions to the Research Objectives	12
2.1	A Summary of How Each Level of Maturity is Defined (Paulk, 2009)	19
2.2	The Five Levels of the Capability Maturity Model Integrated (Carnegie Mellon 1999) (White, 2018)	20
2.3	The Four Perspectives of the Game Maturity Model, Each with their Five Maturity Levels (Boer et al., 2013)	22
2.4	The Five Operational Areas of eTcoMM with their Five Maturity Levels and Attributes (Marchiori, Pavese, & Cantoni, 2012)	23
2.5	The Five Aspects of Financial Management Maturity Model ("Financial Management Maturity Model - National Audit Office (NAO)", 2012)	25
2.6	Summary of the Aim of Maturity Models used in Different Industries	26
2.7	Comparison of Several Existing C2M2 (Country Level)	33
2.8	The Phases of Cybersecurity Posture Assessment (Hitachi Systems Security Inc., n.d.)	39
2.9	The Ultimate Cybersecurity Posture Checklist (Hitachi Systems Security Inc., n.d.)	40
2.10	Comparison of Several Existing C2M2 (Organisation Level) inclusive of MS-C2M2	47
2.11	Several Definitions of Maqasid Al- Shari'ah as Defined by Muslim Scholars (Dusuki & Bouheraoua, 2011)	49
3.1	Possible Relation between Maqasid Al-Shari'ah and Cyber security	72
3.2	The Chosen Factors from the Cybersecurity Capacity Maturity Model for Nations (CMM) (Revised edition) by The Global Cyber Security Capacity Centre (2017)	74
3.3	A Compilation of the Existing Cyber security Maturity Models' Questionnaires that is Relevant to Dimension 1; Factor 1.1	76

3.4	The Structure of the Questionnaire	77
4.1	Relevancy of Maqasid Al-Shari'ah Elements in the Context of an Organisation	80
4.2	Maturity Level and its Range of Marks (for Dimension 1,2,3 and 5)	91
4.3	Modified Maturity Level and its Range of Marks (for Dimension 1,2,3 and 5)	92
4.4	Maturity Level and its Range of Marks (for Dimension 4)	93
5.1	Summary of Cyber Security Maturity Levels Obtained by All Organisations	161
6.1	Research Questions and Hypothesis Justification	175



LIST OF FIGURES

<u>Figure No.</u>		<u>Page No.</u>
1.1	A Graph of Impact Against Likelihood (Collins, 2019)	2
1.2	Reported Incidents in Malaysia 2018 (MyCERT - The Malaysian Computer Emergency Response Team, 2019)	5
1.3	Reported Incidents in the World, 2018 (Passeri, 2019)	5
1.4	The Thesis Overall Outline	16
2.1	The Five Maturity Levels of CMM (Paulk, 2009)	18
2.2	The Ten Aspects of Cyber security Culture Barometer, Together with the Descriptors (Nagan Research Group LLC., 2017)	37
2.3	The Five Maturity Levels of Cyber Security Culture (Nagan Research Group LLC., 2017)	38
2.4	The Five Maturity Levels of Cybersecurity Posture (Hitachi Systems Security Inc., n.d.)	41
2.5	The Five Dimensions of NIST Maturity Self-Assessment Survey (Cipher, n.d.)	42
2.6	The Elements that Define the Dimensions of NIST Maturity Self-Assessment Survey (Cipher, n.d.)	43
2.7	Example of How the Dimensions of NIST Maturity Self-Assessment Survey are Evaluated (Cipher, n.d.)	44
2.8	The Five Maturity Levels of NIST Maturity Self-Assessment Survey (Cipher, n.d.)	45
2.9	Shaya'a Othman Islamic Management Model (Othman et al., 2015)	55
3.1	A Flowchart of How the Research will be Carried Out	59
3.2	The Processes Involved within the Prototype Tool	62
3.3	A Flowchart Depicting the Processes Involved in Developing the Prototype Tool	63
3.4	An Initial Prototype Tool's Design for Recording the Organisation's Background Details	64

3.5	An Initial Prototype Tool's Design for Displaying Questions to Evaluate the Cyber security Maturity Level	64
3.6	An Initial Prototype Tool's Design for Displaying Results of the Organisation	65
3.7	An Initial Prototype Tool's Design for Displaying General Guidelines to Achieve Agile Level	65
3.8	The System Architecture Design of the Prototype Tool	66
3.9	The Data Flow Diagram of the Prototype Tool	67
3.10	The Main Attributes of the Proposed Model's Framework	70
3.11	A Table that Relates Maqasid Al-Shari'ah, Cyber security Maturity Levels and the Dimensions (Example: Dimension 1; Factor 1.1)	71
3.12	The Dimensions and Factors of the Prototype Tool for the MS-C2M2	73
4.1	The Process of Assigning Maqasid Al-Shari'ah Elements to a Question (Example 1)	80
4.2	The Process of Assigning Maqasid Al-Shari'ah Elements to a Question (Example 2)	81
4.3	The Cyber security Maturity Levels of Maqasid al Shari'ah Cyber Security Barometer	82
4.4	The Mappings of Daruriyyat, Hajiyyat, Tahsiniyyat onto Functional, Tactical & Strategic and Agile Cyber security Maturity Level Respectively	85
4.5	The Formula for Calculating the Percentage for Reaching Agile	89
4.6	The Formula of Determining the Range of a Cyber security Maturity Level	90
4.7	Step-by-step Examples of Determining the Colour of the Cyber security Maturity Levels (Example 1)	94
4.8	Step-by-step Examples of Determining the Colour of the Cyber security Maturity Levels (Example 2)	95
4.9	The Prototype Tool's Main Menu	97
4.10	An Organisation's Details Form	97
4.11	A List to Record the Organisations	98
4.12	A Form for Adding a New Question	99

4.13	A List to Record all Questions	99
4.14	A Form to Add a Checklist	100
4.15	A Record of all Checklist	100
4.16	A List to Record the Results	101
4.17	The Prototype Tool's Dashboard	102
4.18	The First Form Main Menu	102
4.19	The Second Form Main Menu	103
4.20	The Organisation Info Tab	103
4.21	The First Form of the Questionnaire Tab	104
4.22	The Second Form of the Questionnaire Tab	104
4.23	The Administrative Log in Page	105
4.24	A Screenshot of the SSL Certificate of the Prototype Tool	106
4.25	The Error Page for Security Purposes	107
4.26	Example of the Questionnaire	108
4.27	Example of the Checklist	108
5.1	Cyber Security Maturity Levels (example)	112
5.2	Results with Regard to the Core Elements of Maqasid Al-Shari'ah for a Dimension (example)	113
5.3	A Detailed Explanation on How to Read Results in Figure 5.2	114
5.4	Cyber security Maturity Levels of ORG-1	116
5.5	Maqasid Al-Shari'ah Perspective of ORG-1 (Dimension 1)	119
5.6	Maqasid Al-Shari'ah Perspective of ORG-1 (Dimension 2)	121
5.7	Maqasid Al-Shari'ah Perspective of ORG-1 (Dimension 3)	124
5.8	Maqasid Al-Shari'ah Perspective of ORG-1 (Dimension 4)	127
5.9	Maqasid Al-Shari'ah Perspective of ORG-1 (Dimension 5)	130
5.10	Cyber security Maturity Levels of ADD-1	133
5.11	Maqasid Al-Shari'ah Perspective of ADD-1 (Dimension 1)	135

5.12	Maqasid Al-Shari'ah Perspective of ADD-1 (Dimension 2)	138
5.13	Maqasid Al-Shari'ah Perspective of ADD-1 (Dimension 3)	141
5.14	Maqasid Al-Shari'ah Perspective of ADD-1 (Dimension 4)	145
5.15	Maqasid Al-Shari'ah Perspective of ADD-1 (Dimension 5)	147
5.16	Cyber security Maturity Levels of ORG-2	151
5.17	Maqasid Al-Shari'ah Perspective of ORG-2 (Dimension 1)	152
5.18	Maqasid Al-Shari'ah Perspective of ORG-2 (Dimension 2)	153
5.19	Maqasid Al-Shari'ah Perspective of ORG-2 (Dimension 3)	155
5.20	Maqasid Al-Shari'ah Perspective of ORG-2 (Dimension 4)	157
5.21	Maqasid Al-Shari'ah Perspective of ORG-2 (Dimension 5)	159
5.22	Summary of Maqasid Al-Shari'ah Results Obtained by All Organisations for Dimension 1	161
5.23	Summary of Maqasid Al-Shari'ah Results Obtained by All Organisations for Dimension 2	162
5.24	Summary of Maqasid Al-Shari'ah Results Obtained by All Organisations for Dimension 3	162
5.25	Summary of Maqasid Al-Shari'ah Results Obtained by All Organisations for Dimension 4	163
5.26	Summary of Maqasid Al-Shari'ah Results Obtained by All Organisations for Dimension 5	163

LIST OF ABBREVIATIONS

ASPI	Australian Strategic Policy Institute
BSA	Business Software Alliance
C2M2	Cyber security Capability Maturity Model
CI	Critical Infrastructure
CIO	Chief Information Officer
CMM	Capability Maturity Model
CMMI	Capability Maturity Model Integrated
CRI	Cyber Readiness Index
DMO	Destination Management Organisation
DOS	Denial-of-Service
eTcoMM	eTourism Communication Maturity Model
GCI	Global Cybersecurity Index
GDP	Gross domestic products
HTTPS	Hyper Text Transfer Protocol Secure
IUM	International Islamic University Malaysia
ISMS	Information Security Management System
ITU	International Telecommunication Union
MCMC	Malaysian Communications and Multimedia Commission
MMO	Massively Multiplayer Online
MS-C2M2	Cyber security Capability Maturity Model guided by Maqasid Al-Shari'ah
MyCERT	The Malaysian Emergency Response Team
NAO	National Audit Office
NSA	National Security Agency
NACSA	National Cyber Security Agency
NGO	Non-Governmental Organisation
NHS	National Health Service
NIST	National Institute of Standards and Technology
PDPA	Personal Data Protection Act
PHP	Hypertext Preprocessor (A Programming Language)
R&D	Research and Development
SEI	Software Engineering Institute
SOP	Standard Operating Procedure
SSL	Secure Sockets Layer
URL	Uniform Resource Locator
WEF	World Economic Forum

CHAPTER ONE

INTRODUCTION

1.1 BACKGROUND

1.1.1 The Need for Cyber security

Cyber security is a term referring to efforts and counter measures used to safeguard and protect cyber users as well as their data and work from criminal hackers (Stallings & Brown, 2012). This is undeniably important especially in an era where most of our work and assets are carried out in the cyber world using latest technologies that the world has to offer. In any security matters, threats that relate to the asset to be protected, are a major concern. Threats are anything or anyone that can bring harm to our assets (Stallings & Brown, 2012).

In the 14th edition Global Risks Report 2019, an annual initiative done by World Economic Forum (WEF), it was found that cyberattacks were among the top 10 risks in term of its likelihood to harm us and our assets as well as its impact (Collins, 2019). Likelihood here refers to the chances or probability that a risky incident (as defined by WEF) to occur in our everyday life and impact refers to how severe the effects are. Both are measured in the scale of 1 to 5 which the latter indicates the highest probability or severity. See Figure 1.1. Cyberattacks (the one circled in red) was ranked number 5 and 7 in terms of its likelihood and impact respectively. This signifies the need to address the risk with high importance, and not lightly.

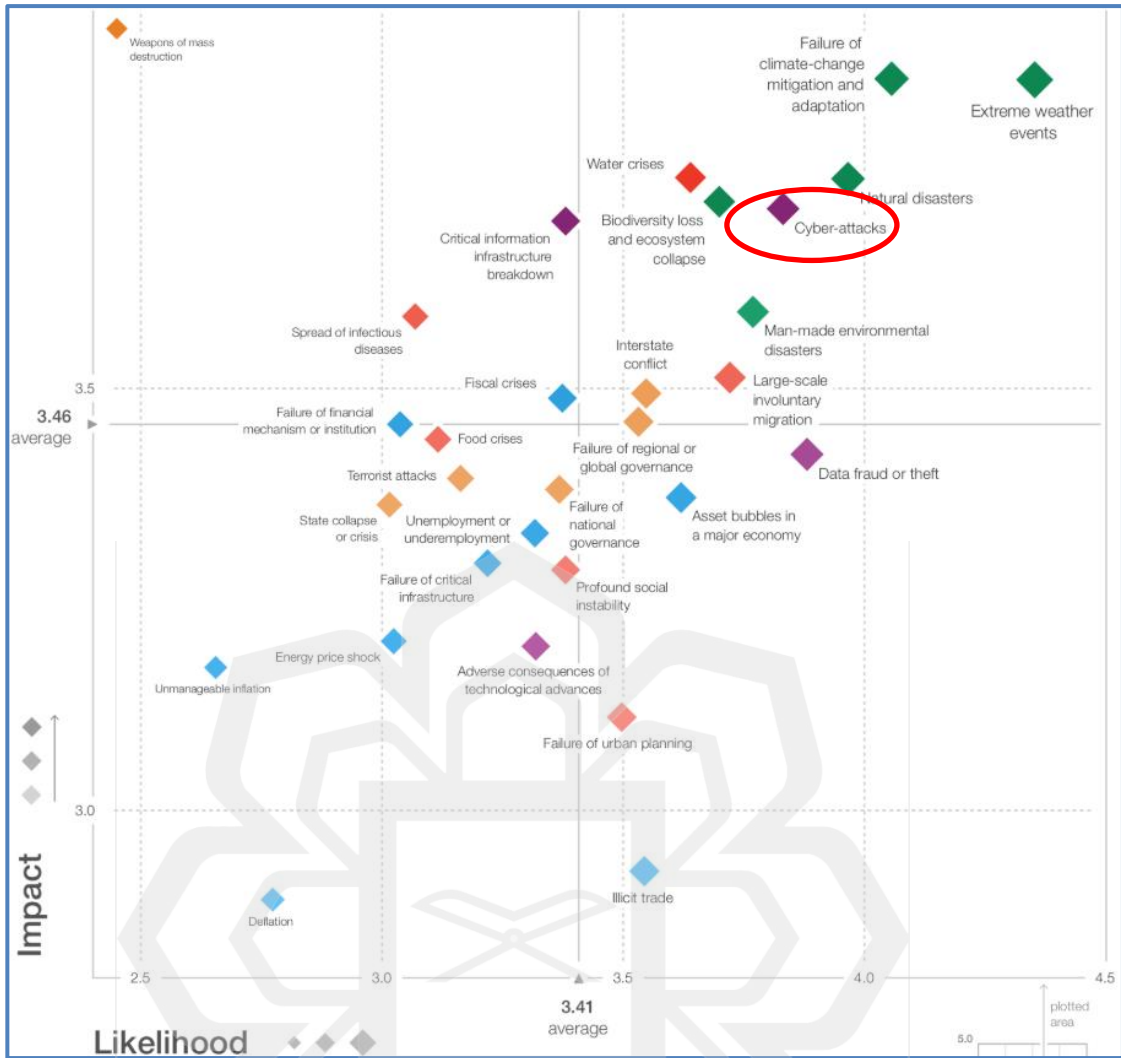


Figure 1.1: A Graph of Impact Against Likelihood (Collins, 2019)

The criminals who perform these threats usually have financial gain and individual satisfaction as their core motivation. There are many terminologies used to classify threats, such as (1) cyber-warfare, (2) cyber-espionage, (3) cybercrime, (4) cyber-terrorism and (5) etc. Table 1.1 gives an overview of their definitions.

Table 1.1: Examples of Terminologies Used to Describe the Nature of Cyber Threats with their Definitions

Terminology	Definition
cyberwar/ cyber-warfare	<ul style="list-style-type: none"> • Operations done on rival nation-state by the military in the cyber space. It is for the benefit of the state (Brenner, 2006). • Civilians are not supposed to be targeted (Brenner, 2006).
cybercrime	<ul style="list-style-type: none"> • Unauthorised infiltration into computer networks, usually for economic gains (Morag, 2014). • Similar to cyberwar but differs in term of scale. Cybercrime has a much smaller scale than cyberwar (Elkus, 2011). • Crimes that are committed using technologies (Brenner, 2006).
cyberattack	<ul style="list-style-type: none"> • The use of malicious codes to take advantage of other people's computer network, computer information system, etc. (Gangadeen, 2016) • 2 types: <ul style="list-style-type: none"> ✚ (1) Syntactic (the use of malicious software). Example: Virus, Worms, Trojan Horses, Spyware, Malware (Gangadeen, 2016) ✚ (2) Semantic (misleading information for the purpose of covering your track). Example: Phishing, Denial-of-Service (DOS) and Spoofing. (Gangadeen, 2016)
cyber-terrorism	<ul style="list-style-type: none"> • Similar to cybercrime, but in cyber-terrorism it is for reasons other than personal gains i.e. political (Brenner, 2006). • It targets civilians as opposed to cyber-warfare (Brenner, 2006).
cyber related crime	<ul style="list-style-type: none"> • Crimes that does not necessarily require the use of technologies. • Sometimes referred to as social engineering. • Social engineering is simply a skill harnessed in order to trick victim into giving their valuable information just by talking or impersonating someone else (Peters, 2015).
cyber-sabotage	<ul style="list-style-type: none"> • The act of causing a disturbance to the computer network (Morag, 2014). • Similar to cyber-terrorism but in cyber-sabotage, it does not harm people directly (Morag, 2014).
cyber-espionage	<ul style="list-style-type: none"> • Usually associated with the involvement of spies to devise a strategy in order to retrieve a government or an organisation's sensitive information by the means of breaking the computer system or network (Morag, 2014).

From Table 1.1, one would be able to understand that cyber threats can exist in many different forms and each form may differ in terms of its scale, purpose and methods of attacking.

Just as much technology is improving, the cyber threats are also continuing to evolve. In May 2017, about 150 countries were attacked by a Wannacry Ransomware virus (Dwoskin & Adam, 2017). Once infected, a computer for example, would have all data and information stored within it encrypted and unless the owner of the computer paid the demanded ransom, nothing can be done to retrieve them. The National Health Service (NHS) in United Kingdom was one of the organisations that fell victim to this phenomenon. Due to the attack, X-Ray imaging was unable to be carried out causing delay for patients to get treatment (Rawlinson, 2017). Experts had also warned that it is still highly unlikely that the data would be decrypted once the ransom had been paid (Collins, 2017; Yalburgi, 2017).

In January 2018, the disclosure of Meltdown and Spectre vulnerabilities has practically put every operating system and device at risk ("10 Must-Know 2018 Cybersecurity Statistics", 2018). These vulnerabilities allow attackers to get access to data previously considered completely protected in computing device (Fruhlinger, 2018).

The year 2019 falls nothing short of the cyberattacks when in January, a bug was discovered in iPhone FaceTime application (Mayo, 2019). The bug allowed a caller to hear the recipient's audio even though he or she has yet to answer or reject the call. The following figures (Figure 1.2 and 1.3) depicted the various forms of cyber threats in Malaysia as well as international in 2018.

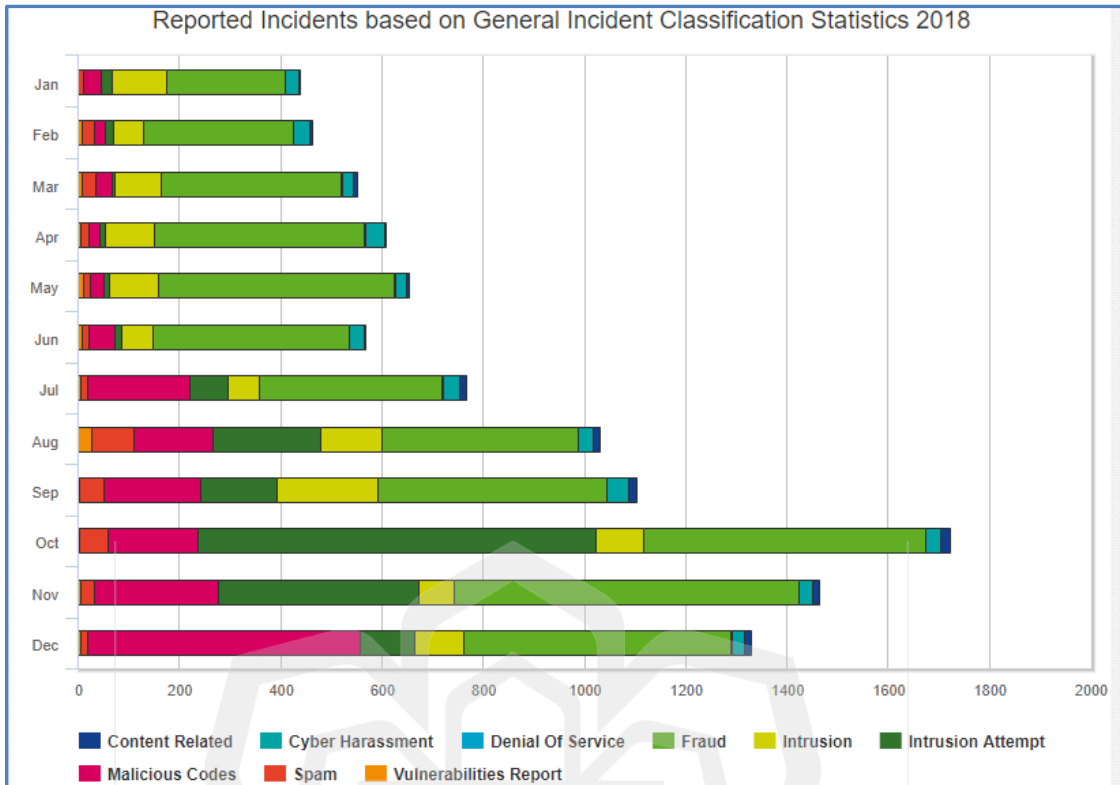


Figure 1.2: Reported Incidents in Malaysia 2018 (MyCERT - The Malaysian Computer Emergency Response Team, 2019)

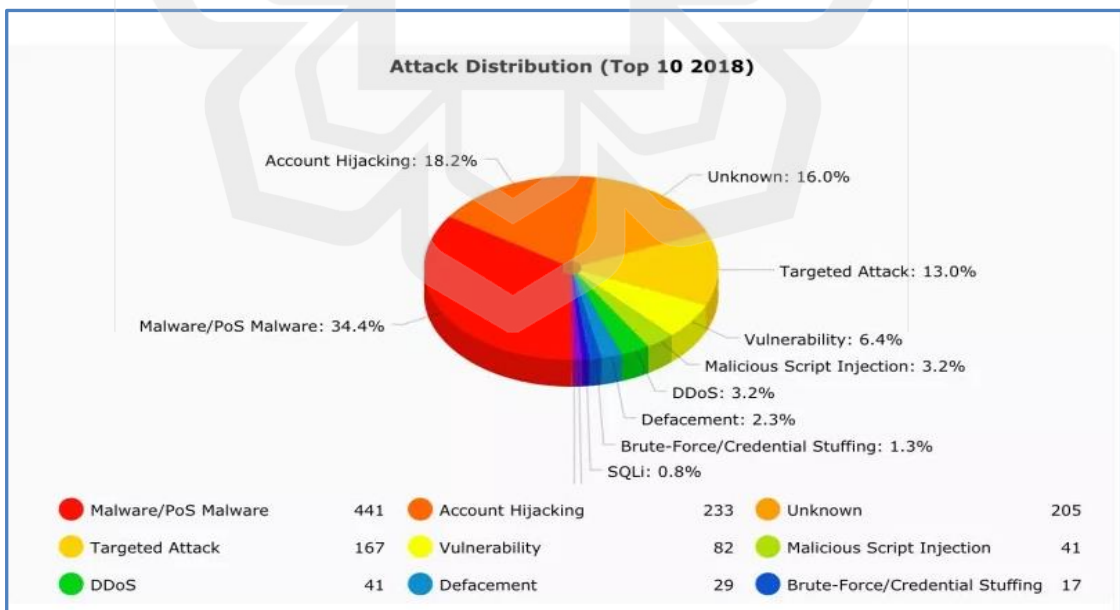


Figure 1.3: Reported Incidents in the World, 2018 (Passeri, 2019)