



**Faculty of Information and Communication Technology**

A faded version of the UTeM logo and university name is visible in the background behind the title text.

**AN EMPIRICAL STUDY OF THE INFORMATION SECURITY  
AWARENESS MODEL IN OMAN**

**Issam Shaaban Moshaded Al Shanfari**

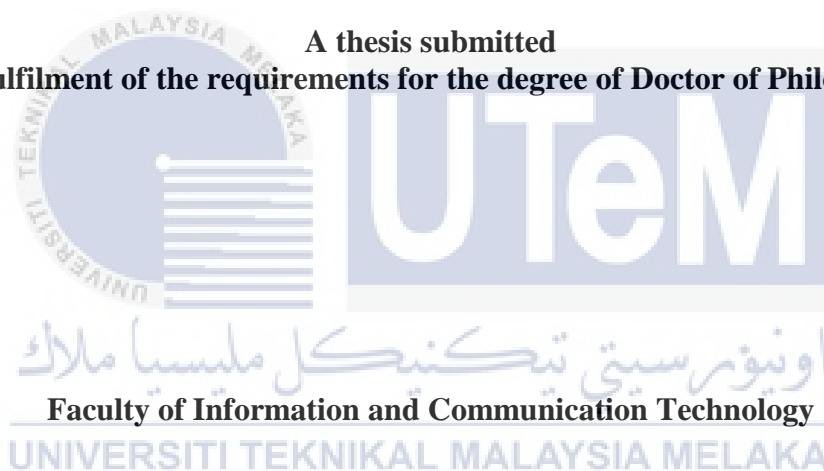
**Doctor of Philosophy**

**2023**

**AN EMPIRICAL STUDY OF THE INFORMATION SECURITY AWARENESS  
MODEL IN OMAN**

**ISSAM SHAABAN MOSHADED AL SHANFARI**

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



**UNIVERSITI TEKNIKAL MALAYSIA MELAKA**

**2023**

## DECLARATION

I declare that this thesis entitled “An Empirical Study of the Information Security Awareness Model in Oman” is the result of my own research except as cited in the references. The thesis has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.



Signature : .....

Name : .....





Issam Al Shanfari.....

Date : 25/2/2023  
اونيزور سي تي كل مليسيا ملاك

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

## APPROVAL

I hereby declare that I have read this thesis and in my opinion this thesis is sufficient in terms of scope and quality for the award of Doctor of Philosophy.

 Signature :  .....

Supervisor Name : Senior Lecturer Dr. Warusia Mohamed Yassin

Date : .....25/2/2023.....

اونيورسيتي تيكنيكل مليسيا ملاك

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

## DEDICATION

I dedicate my dissertation work to the sake of Allah, my homeland, Oman, UTeM University and its distinguished professors, my family, my beloved sons, Amer and Azzan, my beloved brothers and sisters, and many friends who inspire and support me. I will always appreciate all they have done. A special thanks to my supervisor, Dr Warusia Mohamed Yassin, who has supported me throughout my study journey. I will never forget his most wonderful cooperation with me.



## ABSTRACT

Most organisations continue to face threats to their information security. In most organisations, these threats and risks are attributed to employees' lack of information security awareness and security behaviours. As the human and technological aspects of information security are inextricably linked, reducing risks in this area also necessitates investigation into the human aspects of information security. Although the relevance of information security awareness for the human component is high, the prevalence among employees has been relatively low. Consequently, they run an increased risk of security incidents owing to a lack of threat mitigation strategies and the perception that it would never occur to them. This quantitative correlational study investigates the success factors influencing the employees' information security awareness intentions and information security behaviour adoption through questionnaires, thus developing an integrated model of the extracted success factors. The success factors utilised are derived from the Theory of Planned Behaviour (TPB), Protection Motivation Theory (PMT), and General Deterrence Theory (GDT). The study population consisted of employees from various positions in Omani public institutions. Although 480 questionnaires were handed out to participants, it was decided that the minimum sample size should be 384. The respondents were chosen using a method of proportionate stratified sampling. The main research instrument was derived from past studies, adapted according to the purpose of the study, divided into two portions, and verified by a panel of experts in the study field. SPSS version 24 and AMOS version 24 software was used to analyse the data. The structural equation modelling technique was used to examine correlations between the success factors utilised as independent variables, with the employee's intention to engage in information security awareness activities as a mediator variable towards actual information security behaviour as the dependent variable. This study's correlation analysis revealed that information security attitude ( $\beta=0.138$ ), subjective norms ( $\beta=0.146$ ), perceived behavioural control ( $\beta=0.300$ ), response efficacy ( $\beta=0.148$ ), perceived threat vulnerability ( $\beta=0.311$ ), perceived severity of sanctions ( $\beta=0.276$ ), and security education, training, and awareness ( $\beta=0.139$ ) are the significant factors affecting public institution employees' information security awareness intentions in Oman from one hand. Information security awareness's intentions ( $\beta=0.582$ ), organisational support ( $\beta=0.262$ ), and information security communication channels ( $\beta=0.187$ ) are the significant factors affecting actual information security behaviour adoption from the other. The findings enabled the development of an integrated model that includes the control and prediction, motivation, deterrence, technical-related, organisational, and communication factors of InfoSec behaviour among employees. It was verified that the model accounts for 52% of the variance (adjusted  $R^2$ ) in information security behaviour. Expert validation was performed to comprehend the analysis results better and gain expert confirmation. Several implications and recommendations were also derived from the study's findings. Thus, the developed integrated model is definitive and offers a basis for future research in relevant areas of study.

# **KAJIAN EMPIRIKAL TERHADAP MODEL KESEDARAN KESELAMATAN MAKLUMAT DI OMAN**

## **ABSTRAK**

*Kebanyakan organisasi menghadapi ancaman yang berterusan terhadap keselamatan maklumat mereka. Di dalam kebanyakan organisasi, ancaman dan risiko ini dikaitkan dengan kekurangan kesedaran keselamatan maklumat dan tingkah laku keselamatan pekerja. Memandangkan aspek manusia dan teknologi keselamatan maklumat adalah berkait rapat, pengurangan risiko di dalam bidang ini memerlukan penyiasatan terhadap aspek manusia khususnya dari sudut keselamatan maklumat. Walaupun perkaitan ISA untuk komponen manusia adalah tinggi, akan tetapi lazimnya ISA di kalangan pekerja adalah agak rendah. Mereka menghadapi insiden keselamatan yang berisiko tinggi oleh kerana kekurangan strategi pengurangan ancaman dan persepsi bahawa ia tidak akan berlaku kepada mereka. Kajian kuantitatif korelasi ini bertujuan untuk menyiasat faktor kejayaan yang mempengaruhi niat ISA pekerja dan penggunaan tingkah laku keselamatan maklumat melalui soal selidik dan membangunkan model bersepadu faktor kejayaan yang diekstrak. Teori Tingkah Laku Terancang (TPB), Teori Motivasi Perlindungan (PMT), dan Teori Pencegahan Umum (GDT). Populasi kajian terdiri daripada pekerja daripada pelbagai jawatan di institusi awam negara Oman. Sebanyak 480 soal selidik telah diedarkan kepada peserta dan saiz sampel yang diputuskan adalah sebanyak 384. Responden dipilih menggunakan kaedah persampelan berstrata berkadar. Instrumen kajian utama diperoleh daripada kajian lepas serta disesuaikan mengikut tujuan kajian semasa yang dibahagikan kepada dua bahagian, dan disahkan oleh panel pakar dalam bidang kajian. SPSS versi 24 dan AMOS versi 24 digunakan untuk menganalisis data. Teknik pemodelan persamaan struktur digunakan untuk mengkaji korelasi antara faktor kejayaan yang digunakan sebagai pembolehubah tidak bersandar, dengan niat pekerja untuk melibatkan diri dalam aktiviti ISA sebagai pembolehubah pengantara terhadap tingkah laku keselamatan maklumat sebenar sebagai pembolehubah bersandar. Analisis korelasi kajian ini mendedahkan bahawa sikap keselamatan maklumat ( $\beta=0.138$ ), norma subjektif ( $\beta=0.146$ ), kawalan tingkah laku yang dirasakan ( $\beta=0.300$ ), keberkesanan tindak balas ( $\beta=0.148$ ), kelemahan ancaman yang dirasakan ( $\beta=0.311$ ), keterukan sekatan yang dirasakan ( $\beta=0.276$ ), dan pendidikan, latihan dan kesedaran keselamatan ( $\beta=0.139$ ) adalah faktor penting yang mempengaruhi niat ISA kakitangan institusi awam di Oman, dan niat ISA ( $\beta=0.582$ ), sokongan organisasi ( $\beta=0.262$ ) dan saluran komunikasi keselamatan maklumat adalah faktor penting yang mempengaruhi penerimaan tingkah laku keselamatan maklumat sebenar daripada yang lain. Penemuan ini membolehkan pembangunan model bersepadu ( $\beta=0.187$ ) yang merangkumi kawalan dan ramalan, motivasi, pencegahan, faktor berkaitan teknikal, organisasi dan komunikasi bagi tingkah laku keselamatan maklumat di kalangan pekerja. Model ini telah disahkan dan menyumbang 52% daripada varians ( $R^2$  diselaraskan) dalam gelagat keselamatan maklumat. Pengesahan pakar telah dilakukan untuk lebih memahami keputusan analisis dan untuk mendapatkan pengesahan pakar. Beberapa implikasi dan cadangan juga diperoleh daripada dapatan kajian. Melalui pengagregatan ini, model bersepadu yang dibangunkan adalah muktamad dan menawarkan asas untuk penyelidikan masa depan dalam bidang pengajian yang berkaitan.*

## ACKNOWLEDGEMENTS

The first thing I want to say is that I want to thank Allah Almighty. He gave me the chance, patience, and help I needed to get through difficult situations, and then he helped me reach this stage's end.

From the bottom of my heart, I would like to express my sincere acknowledgement to my supervisors, Dr Warusia Mohamed Yassin and Ts. Dr Raihana Syahirah Abdullah, from the Department of Computer Systems and Communication (SKK), Faculty of Information and Communication Technology (FTMK), Universiti Teknikal Malaysia Melaka (UTeM), for providing support, guidance, and feedback throughout this research.

From the bottom of my heart, I would like to thank my loving parents, beloved family, and brothers and sisters for their support and sacrifices, which encouraged and supported me a lot during my studies.

Lastly, I would like to express my gratitude and appreciation to everyone who took part or helped me successfully finish this thesis.



## TABLE OF CONTENTS

	<b>PAGE</b>
<b>DECLARATION</b>	
<b>APPROVAL</b>	
<b>DEDICATION</b>	
<b>ABSTRACT</b>	<b>i</b>
<b>ABSTRAK</b>	<b>ii</b>
<b>ACKNOWLEDGEMENTS</b>	<b>iii</b>
<b>TABLE OF CONTENTS</b>	<b>iv</b>
<b>LIST OF TABLES</b>	<b>viii</b>
<b>LIST OF FIGURES</b>	<b>xi</b>
<b>LIST OF ABBREVIATION</b>	<b>xiii</b>
<b>LIST OF APPENDICES</b>	<b>xvii</b>
<b>LIST OF PUBLICATIONS</b>	<b>xviii</b>
<b>CHAPTER</b>	
<b>1. INTRODUCTION</b>	<b>1</b>
1.1 Introduction	1
1.2 Background	1
1.3 Background to Research Problem	5
1.4 Research Problem	7
1.5 Research Questions	10
1.6 Research Objectives	10
1.7 Scope of the Research	11
1.8 Research Significance	11
1.9 Research Contribution	12
1.10 Operational Definitions	14
1.11 Summary and Thesis Outline	17
<b>2. LITERATURE REVIEW</b>	<b>19</b>
2.1 Introduction	19
2.2 The Scope of Information Security Awareness (ISA)	20
2.3 Measurement of ISA Levels	24
2.3.1 Assessment of ISA in Omani Organisations	26
2.4 ISA Adoption/ Acceptance Models and Theories	28
2.4.1 Theory of Reasoned Action (TRA)	28
2.4.2 Theory of Planned Behaviour (TPB)	29
2.4.3 Protection Motivation Theory (PMT)	31
2.4.4 Diffusion of Innovation (DOI)	32
2.4.5 General Deterrence Theory (GDT)	32
2.4.6 Technology Acceptance Model (TAM)	33
2.5 Psychological Factors Affecting ISA	34
2.5.1 InfoSec Attitude	35
2.5.2 Subjective Norms	38
2.5.3 Perceived Behavioural Control	40
2.5.4 Response Efficacy	42

2.5.5	Perceived (Security Threat) Vulnerability	44
2.5.6	Perceived Sanction Severity and Certainty	46
2.5.7	Security Education, Training, Awareness (SETA)	50
2.5.8	Behavioural Intention	51
2.5.9	Facilitating Conditions Factors (Organisational Support)	53
2.6	Criticism of Adoption Models and Theories	55
2.7	Integrated Models in ISA	58
2.7.1	Literature Gaps	62
2.7.2	Conceptual Model	65
2.7.3	The Formulated Hypotheses	68
2.8	Summary	75
<b>3.</b>	<b>METHODOLOGY</b>	<b>76</b>
3.1	Introduction	76
3.2	Phase 1: Research Methodology, Design, and Approach	78
3.2.1	Research Philosophy	80
3.2.1.1	Positivism vs Interpretivism	81
3.2.1.2	Choice of Philosophy	82
3.2.2	Research Approach	83
3.2.2.1	Research Type	83
3.2.2.2	Quantitative vs Qualitative	84
3.2.2.3	Objective vs Subjective Research	85
3.2.2.4	Deductive vs Inductive Research	85
3.2.2.5	Choice of Research Approach	86
3.2.3	Research Strategy	87
3.2.3.1	Time Horizon	88
3.2.4	Population and Sample	89
3.3	Phase 2: ISA Level Assessment, Problem Identification and Literature Gap Analysis	93
3.3.1	ISA Level Assessment	93
3.3.2	Carry out a Literature Review	95
3.3.2.1	Factor Weight Analysis	98
3.4	Phase 3: Main Survey's Development and Implementation	100
3.4.1	Questionnaire Development	101
3.4.1.1	Translation of Questionnaire	103
3.4.1.2	Variables Measurement	105
3.4.2	Questionnaire Pre-test and Pilot Study	106
3.4.3	Validity and Reliability	111
3.4.4	Conducting the Survey	112
3.5	Phase 4: Statistical Analysis and Results	114
3.5.1	Data Preparation	114
3.5.2	Data Analysis Method	115
3.5.3	Testing of Hypotheses and Model Building	121
3.5.4	Expert Validation	121
3.6	Summary	122
<b>4.</b>	<b>ANALYSIS AND FINDING</b>	<b>123</b>
4.1	Introduction	123

4.2	Omani Public Sector Employees' Backgrounds (ISA Assessment)	123
4.2.1	General ISA Level among Omani Public Sector Employees	126
4.3	Response Rate (Main Survey)	128
4.4	Data Screening	129
4.4.1	Outliers	130
4.4.2	Normality	131
4.4.3	Linearity	133
4.4.4	Homoscedasticity Assumption	134
4.4.5	Multicollinearity Test	135
4.5	Correlation Matrix between Variables	137
4.6	Demographic Characteristics of the Respondents	139
4.7	Exploratory Factor Analysis (EFA)	146
4.7.1	KMO Test Results	147
4.7.2	Variance of Extracted Factors	148
4.7.3	Factor Loading Results	150
4.8	Descriptive Statistics for Variables	152
4.9	Confirmatory Factor Analysis (CFA)	153
4.10	Goodness of Fit Index (GOF)	154
4.11	Confirmatory Factor Analysis Results (Full Measurement)	155
4.12	Reliability and Validity Test	158
4.12.1	Reliability (Cronbach's Alpha) and Composite Reliability	158
4.12.2	Constructs Validity	158
4.12.2.1	Convergent Validity	159
4.12.2.2	Discriminant Validity	160
4.13	Assessment of Structural Model	162
4.14	Coefficient of Determination: R <sup>2</sup> value	165
4.15	Effect Size (f <sup>2</sup> )	166
4.16	Hypotheses Results	167
4.17	Expert Validation	169
4.17.1	Assessment of the Research Problem	172
4.17.2	Utilised Factors of ISA's Behavioural Intention and Actual InfoSec Behaviour	175
4.17.3	Evaluation of Relationships with ISA Intention and InfoSec Behaviour	178
4.18	Summary	181
<b>5.</b>	<b>DISCUSSION</b>	<b>182</b>
5.1	Introduction	182
5.2	Discussion of Research Findings	182
5.2.1	Information Security Awareness Level	183
5.2.2	Determination of Significant and Insignificant Factors Utilised	187
5.2.3	Relationships between Used Factors toward ISA Intention and InfoSec Behaviour among Oman's Public Sector Employees	202

5.2.4	Success Factors for ISAs in the Developed Integrated Model	208
5.2.4.1	A Comparative Evaluation of the Developed Model	210
5.2.5	Validation of the Developed Integrated Model	213
5.3	Research Implications	216
5.3.1	Theoretical Implications	216
5.3.2	Practical Implications	218
5.4	Summary	221
<b>6.</b>	<b>CONCLUSION AND RECOMMENDATIONS</b>	<b>222</b>
6.1	Introduction	222
6.2	Research Summary	222
6.3	Achieving the Research Objectives	224
6.4	Limitations of the Study	227
6.5	Recommendations	229
6.5.1	Expert Validation for Study's Recommendations	231
6.6	Future Research	234
	<b>REFERENCES</b>	<b>236</b>
	<b>APPENDICES</b>	<b>263</b>



## LIST OF TABLES

TABLE	TITLE	PAGE
1.1	Operational Definitions	14
2.1	The Percentage of Qualified Employees in Omani Institutions (MTCIT, 2021)	28
2.2	The Effect of InfoSec Attitude	36
2.3	The Effect of Subjective Norms	39
2.4	The Effect of Perceived Behavioural Control	41
2.5	The Effect of Response Efficacy	43
2.6	The Effect of Perceived Vulnerability	46
2.7	The Effect of Perceived Sanction Severity and Certainty	48
2.8	The Effect of Security, Education, Training and Awareness (SETA)	50
2.9	The Effect of Behavioural Intention	52
2.10	The Effect of Facilitating Conditions	54
2.11	Comparison with Previous ISA Models	67
3.1	Mapping Research Questions with Methodology	77
3.2	Positivism Vs Interpretivism (Easterby-Smith et al., 2012)	82
3.3	Quantitative Vs Qualitative Research (Firestone, 1987; Neville, 2007)	84

3.4	Civil Service Employees until the end of 2017- OMAN (MOCS, 2018)	89
3.5	Krejcie and Morgan’s Sample Size Determination	91
3.6	Number of Questionnaires Distributed (MOCS, 2018)	93
3.7	Most Used Relationships and Factor Weight Analysis (Approach Adapted from Rana et al., 2015)	99
3.8	The Questionnaire's Measurable Factors and Related Elements	105
3.9	Face Validity of the Questionnaire by Experts	106
3.10	Summary of Reliability of Cronbach’s Alpha from Pilot Test	111
3.11	Evaluation of Measurement Model Criteria for this Study	118
3.12	Evaluation of Structural Model Criteria for this Study	120
4.1	Demographic Characteristics (ISA Assessment Survey)	123
2.2	Frequency, Mean, and Standard Deviation of the ISA Level	126
4.3	Summary of Data Collection and Response Rate	129
4.4	Univariate Outliers	130
4.5	Skewness and Kurtosis for Variables	133
4.6	Multicollinearity Test	136
4.7	Pearson Correlation among the Variables	138
4.8	Distributions of Respondents by Gender	140
4.9	Distributions of Respondents by Age	141
4.10	Distributions of Respondents by Education Level	142
4.11	Distributions of Respondents by Position	143
4.12	Distributions of Respondents by Experience	144
4.13	Distributions of Respondents by Sector Type	145

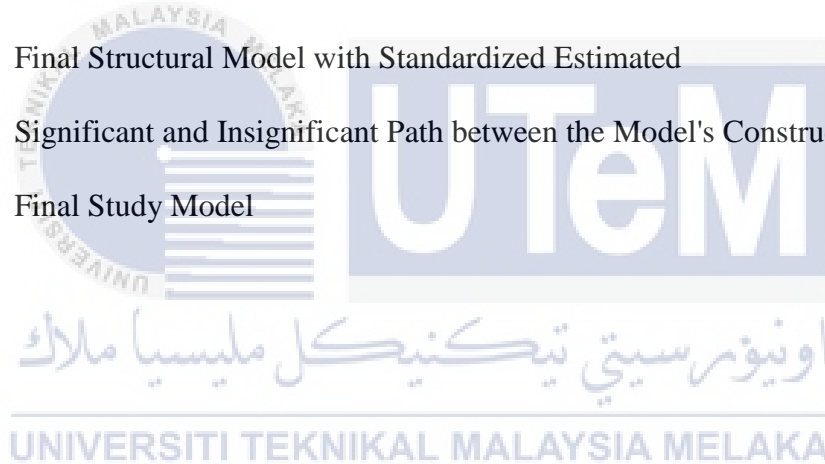
4.14	Results of the KMO and Bartlett's Test	147
4.15	Extracted Factors and Summaries of their Variance	149
4.16	Summary of Dropped Items after Exploratory Factor Analysis (EFA)	150
4.17	Factor Loading for All Variables' Items	151
4.18	All Variables and their Descriptive Statistics	153
4.19	Recommendation Values of Measurement Variables	155
4.20	Results of Fit Indices for CFA- Full Measurement Model	156
4.21	Items Loading, AVE, Cronbach's alpha and Composite Reliability (CR)	159
4.22	Discriminant Validity for Latent Variables	161
4.23	Results of Fit Indices for CFA- Full Structural Model	163
4.24	Coefficient of Determination Result $R^2$	166
4.25	Effect Size $f^2$	167
4.26	Hypotheses Testing Result of Structural Model	168
4.27	Potential Expert Validation Interviewees	171
5.1	Hypotheses Testing Result	208
6.1	Mapping between the Research Objectives, Research Questions and Accomplishment Sections	224

## LIST OF FIGURES

FIGURE	TITLE	PAGE
2.1	TRA Model	29
2.2	TPB Model	30
2.3	PMT Model	31
2.4	DOI Model	32
2.5	GDT Model	33
2.6	TAM Model	34
2.7	Most Significant Theories Used in InfoSec Domain (Kuppusamy et al., 2020)	56
2.8	The Study's Model	66
3.1	Phases of Research Methodology	77
3.2	The Research Onion (Saunders et al. 2012)	79
3.3	Research Methodology Flowchart of this Study	80
3.4	Deductive vs Inductive Approaches	86
3.5	ISA Six Focus Areas (Adopted from Parsons et al., 2017)	95
3.6	Article Selection Procedures	96
3.7	Survey Process (Burgess, 2001)	113
3.8	Model Building Steps	114
4.1	Normality Assumption for InfoSec Actual Behaviour	132



4.2	Linearity Assumption for Employees' InfoSec Actual Behaviour	134
4.3	Homoscedasticity Assumption for Employees' InfoSec Actual Behaviour	135
4.4	Distributions of Respondents by Gender	140
4.5	Distributions of Respondents by Age	141
4.6	Distributions of Respondents by Education	142
4.7	Distributions of Respondents by Position	143
4.8	Distributions of Respondents by Experience	144
4.9	Distributions of Respondents by Sector Type	146
4.10	Final Measurement Model for All Variables	157
4.11	Final Structural Model with Standardized Estimated	164
4.12	Significant and Insignificant Path between the Model's Constructs	169
5.1	Final Study Model	210



## LIST OF ABBREVIATION

AB	- Actual Behaviour
AGFI	- Adjusted Goodness of Fit Index
AMOS	- Analysis of Moment Structures
ATT	- Attitude
AVE	- Average Variance Extracted
BI	- Behavioural Intention
BYOD	- Bring-Your-Own-Device
CA	- Cronbach's Alpha
CFA	- Confirmatory Factor Analysis
CFI	- Comparative Fit Indices
CMA	- Countermeasure Awareness
COM	- Communication Channels
C.R.	- Critical Ratio for Regression Weight
CSFs	- Critical Success Factors
DOI	- Diffusion of Innovation Theory
DSB	- Desktop Security Behaviour
DV	- Dependent Variable
EFA	- Exploratory Factor Analysis
EQS	- Equations SEM program

F.C	- Facilitating Conditions Factors
GDT	- General Deterrence Theory
GFI	- Goodness-of-Fit Index
GOF	- Goodness of Fit Indicators
HAIS-Q	- The Human Aspects of Information Security Questionnaire
ICT	- Information Communications Technology
IFI	- Instrumental Fit Index
IIUM	- International Islamic University Malaysia
InfoSec	- Information Security
IP	- Information Processing framework
ISA	- Information Security Awareness
ISCCB	- Information Security-conscious Care Behaviour
ISPs	- Information Security Policies
IT	- Information Technology
ITA	- Information Technology Authority اونيورسيتي تيكنيكال ايمالاك
IV	- Independent Variable
KMO	- Kaiser-Meyer-Olkin
LISREL	- Linear Structural Relation
MI	- Modification Indices
MOCS	- Ministry of Civil Services
MOE	- Ministry of Education
MSV	- Maximum Shared Squared Variance
MT	- Motivation Theory

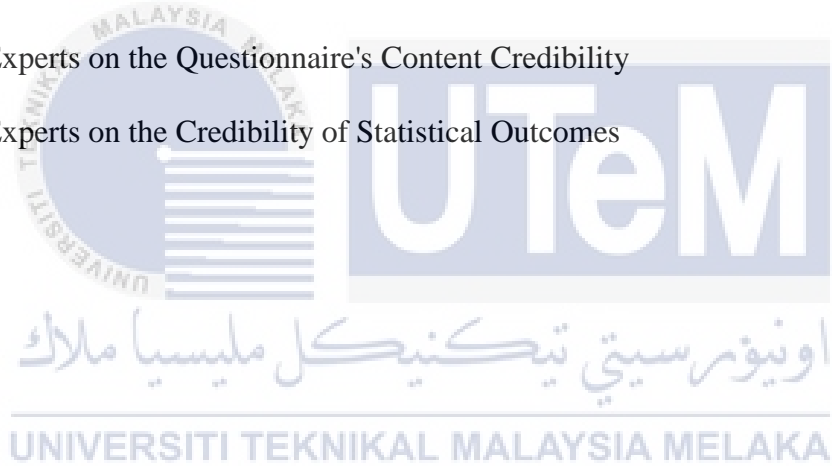
MTCIT	- Ministry of Transport, Communications and Information Technology
NFI	- Normed Fit Index
OCERT	- Oman Computer Emergency Readiness Team
OS	- Organisational Support
PBC	- Perceived Behavioural Control
PCOS	- Perceived Certainty of Sanctions
PEOU	- Perceived Ease of Use
PLS-SEM	- Partial Least Squares Structural Equation Modelling
PMT	- Protection Motivation Theory
PS	- Perceived Severity
PSOS	- Perceived Severity of Sanctions
PU	- Perceived Usefulness
PV	- Perceived Vulnerability
RC	- Response Cost
RE	- Response Efficacy
RMSEA	- Root mean Square Error of Approximation
SCPT	- Situational Crime Prevention Theory
S.D	- Standard Deviation
S.E	- Standard Error of Regression Weight
SE	- Self-Efficacy
SeBIS	- Security Behaviour Intentions Scale
SEM	- Structural Equation Modelling
SETA	- Security Education, Training and Awareness

SIEM	- Security Information and Event Management
SLT	- Social Learning Theory
SN	- Subjective Norms
SPSS	- Statistical Package for the Social Science
TA	- Threat Awareness
TAM	- Technology Acceptance Model
TLI	- Tucker-Lewis Index
TPB	- Theory of Planned Behaviour
TRA	- Theory of Reasoned Action
UISAQ	- Users' Information Security Awareness Questionnaire
VIF	- Variance Inflation Factor
VPN	- Virtual Private Network



## LIST OF APPENDICES

APPENDIX	TITLE	PAGE
A	Invitation Letter for Questionnaires	263
B	The Study's Main Questionnaire	264
C	The ISA's Assessment Questionnaire	271
D	Credential of Translators	274
E	Experts on the Questionnaire's Content Credibility	375
F	Experts on the Credibility of Statistical Outcomes	276



## LIST OF PUBLICATIONS

The following is the list of publications related to the work of this thesis:

- 1- Al-Shanfari I, Yassin W, Abdullah R., 2020. Identify of Factors Affecting Information Security Awareness and Weight Analysis Process. *International Journal of Engineering and Advanced Technology (IJEAT)*, 9(3):534- 42.
- 2- Al-Shanfari, I., Yassin, W., Abdullah, R. S. and Magrisi, G., 2020. Enhancing Information Security Awareness among Omani Public Sector Employees: A Pilot Study. *International Journal on Emerging Technologies*, 11(3): 1194–1203.
- 3- Al-Shanfari, I., Yassin, W., Abdullah, R. S., Al-Fahim, N. H. and Ismail, R., 2020. Prediction, Control, Motivation and Deterrence-based Model to Raise Information Security Awareness among Organisations' Employees. *Technology Reports of Kansai University*, 62(9): 5267-84.
- 4- Al-Shanfari, I., Yassin, W., Abdullah, R. S., Al-Fahim, N. H. and Ismail, R., 2021. Introducing A Novel Integrated Model for the Adoption of Information Security Awareness through Control, Prediction, Motivation, and Deterrence Factors: A Pilot Study. *Journal of Theoretical and Applied Information Technology*. 99(12): 2991 – 3003.
- 5- Al-Shanfari, I., Yassin, W., Tabook, N. and Ismail, R., Ismail, A., 2022. Determinants of Information Security Awareness and Behaviour Strategies in Public Sector Organizations among Employees. *International Journal of Advanced Computer Science and Applications-IJACSA*. 13(8): 479 – 490.

# CHAPTER 1

## INTRODUCTION

### 1.1 Introduction

This chapter clarifies the background of this research on information security awareness (ISA) in the Sultanate of Oman. It presents the domain of the research problem, introduces the objectives and primary research questions, and defines the scope and importance of the study. Operational definitions and thesis outlines are also included.

### 1.2 Background

According to statistics on Internet Status Worldwide (2019), the number of internet users is constantly increasing in the Sultanate of Oman, where the percentage of users increased (1.9%) of the total increase in the number of internet users in the Middle East, which exceeds 5.183%. Oman has emerged as an important e-commerce market in the Middle East, attributable to its excellent consumer protection laws. Furthermore, smartphones and the associated increase in online retailers are fuelling economic growth in Oman due to improved infrastructure and increased internet use, especially by young people (Global Data, 2015). Constant economic growth has also increased the volume of internet and mobile banking. These improvements in payment infrastructure have increased the number of electronic transactions through Omani payment cards to 1,932,224, generating a total revenue of 365 million OMR by the end of 2017 (ITA, 2018).

The growth in internet services has also led to the increasing use of payment cards to complete transactions. By the end of 2017, 34 government entities utilised e-payment