

**UNINTENTIONAL INSIDER THREATS COUNTERMEASURE
MODEL (UITCM) IN REDUCING INTERNAL THREAT
ENVIRONMENT**

ZAINAB. A. A. ABDELSADEQ

UNIVERSITI SAINS ISLAM MALAYSIA

**UNINTENTIONAL INSIDER THREATS COUNTERMEASURE
MODEL (UITCM) IN REDUCING INTERNAL THREAT
ENVIRONMENT**

Zainab. A. A.Abdelsadeq

Thesis submitted in partial fulfilment for the degree of
DOCTOR OF PHILOSOPHY IN
SCIENCE AND TECHNOLOGY

UNIVERSITI SAINS ISLAM MALAYSIA

March 2023

AUTHOR DECLARATION

I hereby declare that the work in this thesis is my own except for quotations and summaries which have been duly acknowledged.

Date: 15 March, 2023

Signature :

Name : Zainab.A.A.Abdelsadeq

Matric No: 4140262

Address : Halaka alsharqiah. Box
9680, Sianah district, Taif
26551,3025,Saudi.A
Suleiman Al-Rajhi Street

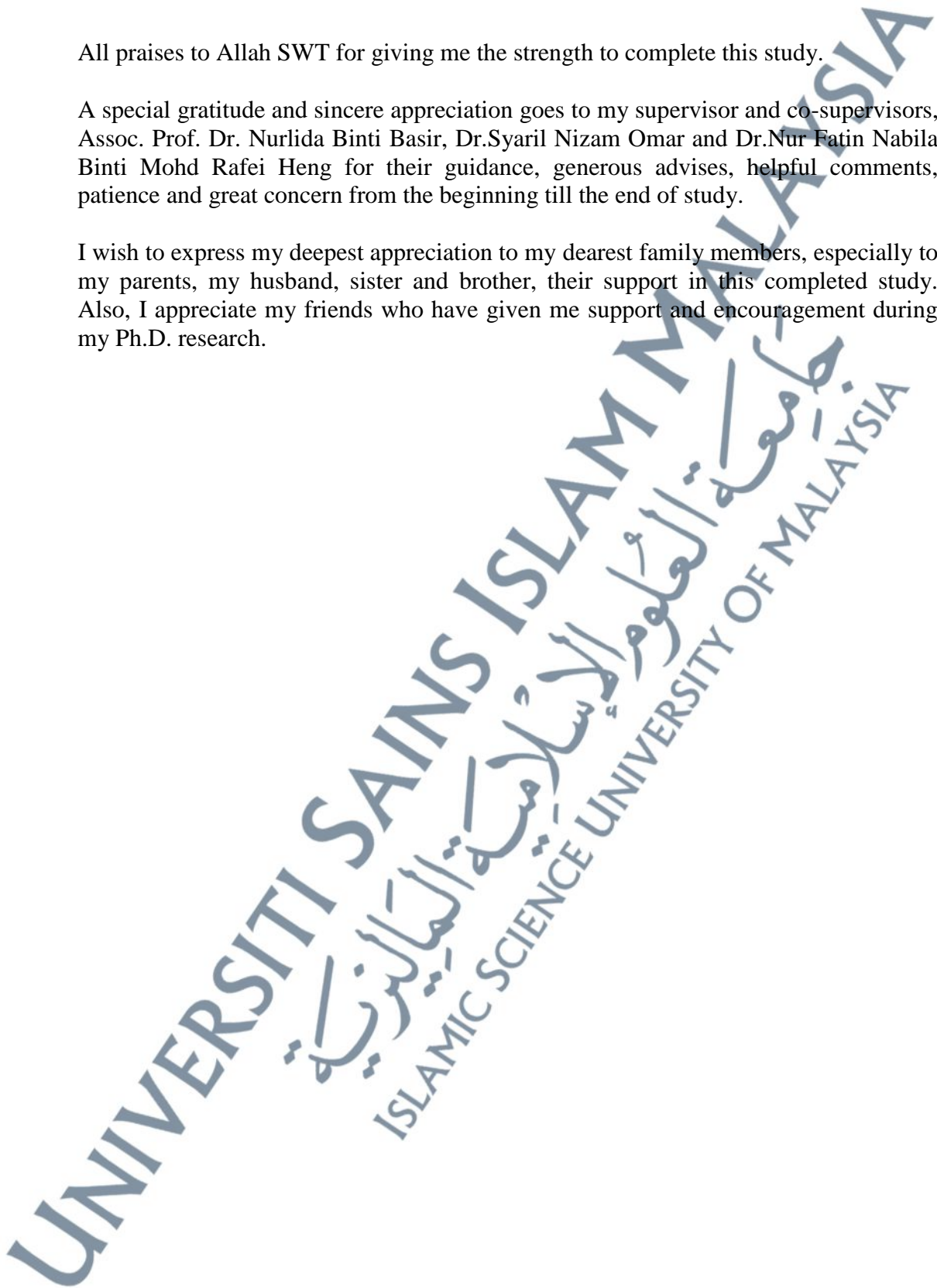
UNIVERSITI SAINS ISLAM MALAYSIA
جامعة العلوم الإسلامية
ISLAMIC SCIENCE UNIVERSITY OF MALAYSIA

ACKNOWLEDGEMENTS

All praises to Allah SWT for giving me the strength to complete this study.

A special gratitude and sincere appreciation goes to my supervisor and co-supervisors, Assoc. Prof. Dr. Nurlida Binti Basir, Dr.Syaril Nizam Omar and Dr.Nur Fatin Nabila Binti Mohd Rafei Heng for their guidance, generous advises, helpful comments, patience and great concern from the beginning till the end of study.

I wish to express my deepest appreciation to my dearest family members, especially to my parents, my husband, sister and brother, their support in this completed study. Also, I appreciate my friends who have given me support and encouragement during my Ph.D. research.



ABSTRAK

Ancaman orang dalam yang tidak disengajakan adalah salah satu isu terbesar yang boleh melemahkan pertahanan keselamatan organisasi. Kajian telah menunjukkan bahawa langkah balas keselamatan teknikal sedia ada sahaja tidak mencukupi terutamanya apabila ia berkaitan dengan kesilapan manusia. Oleh itu, dalam penyelidikan ini sebanyak 311 soal selidik telah dikumpul daripada Eksekutif Teknologi Maklumat Perusahaan Kecil Sederhana (PKS) di Malaysia untuk menentukan faktor penyumbang dan kemungkinan Ancaman Orang Dalam (UIT) yang tidak disengajakan. Data kuantitatif dianalisis menggunakan SPSS. Hasil analisis menunjukkan majoriti responden mendakwa organisasi mereka berkemungkinan besar menghadapi ancaman dengan 634 (34.2%), 442 (23.9%) percaya bahawa organisasi mereka berkemungkinan menghadapi ancaman jenis ini manakala 172 (9.3%) berkemungkinan besar telah menghadapi ancaman sedemikian. Di samping itu, kejahilan dan kecuiaan (27%), kesedaran situasi (26%) dan kesilapan manusia (22%) merupakan faktor yang paling menyumbang kepada UIT dalam PKS Malaysia. Berdasarkan tinjauan, ia menunjukkan bahawa pendekatan defensif berbilang lapisan termasuk dasar, prosedur, kawalan teknikal, kesedaran, perhatian kepada sosiologi, aspek psikologi bersama dengan alat pertahanan automatik adalah penting bagi organisasi untuk melawan "isu rakyat". Pendekatan tunggal bagi tindakan balas hanya boleh menangani beberapa aspek kesilapan manusia tetapi bukan semua. Oleh itu, objektif kajian ini adalah untuk mencadangkan satu model yang terdiri daripada pendekatan campuran yang boleh digunakan sebagai langkah balas terhadap UIT terutamanya dalam PKS Malaysia. Model ini dibangunkan melalui beberapa peringkat. Versi pertama model yang dicadangkan telah dibangunkan dengan menggabungkan langkah balas sedia ada yang telah dicadangkan dalam literatur sedia ada. Pada peringkat kedua, model yang dicadangkan selanjutnya dinilai dengan menggunakan pertimbangan berasaskan pakar melalui kaedah Delphi dengan tujuan untuk mencapai tahap konsensus yang boleh diterima di kalangan pakar dan menghapuskan sebarang ketidakpastian dalam model. Lima (5) pakar dengan komposisi 3 pengamal dan 2 ahli akademik telah menilai model dengan soal selidik dua pusingan. Berdasarkan penilaian, keputusan menunjukkan bahawa pakar telah mencapai kata sepakat bersama dengan skor min melebihi 75% dari segi kesahan teori, kebolegunaan dan kebolehbacaan dan kebolehfahaman model. Memandangkan tindakan balas ialah kawalan keselamatan yang digunakan untuk melindungi kerahsiaan, integriti, dan ketersediaan data dan sistem maklumat dan ia harus tersedia di setiap lapisan timbunan, diharapkan model itu boleh digunakan sebagai garis panduan oleh organisasi untuk menambah baik langkah balas UIT sedia ada mereka dan secara tidak langsung mengukuhkan strategik, operasi serta kewangan organisasi mereka.

ABSTRACT

Unintentional insider threats (UITs) are one of the biggest issues that can weaken the security defence of the organization. Studies have shown existing technical security countermeasures alone are insufficient especially when it deals with human errors. A total of 311 questionnaires were collected from Information Technology Executives of the Small Medium Enterprises (SMEs) in Malaysia to determine the contributing factors and the likelihood of UITs. Quantitative data was analyzed using SPSS. The results showed majority of the respondents alleged that their organizations were very likely to have faced threats with 634 (34.2%), 442 (23.9%) believed that their organizations were likely to confront this threats. While 172 (9.3%) were most likely to have faced such threats. Ignorance and negligence (27%), situation awareness (26%) and human error (22%) were the most contributing factors of UIT in Malaysian SMEs. The survey showed that multi layered defensive approaches including policies, procedures, awareness, attention to sociology, psychology aspects together with automated defence tools are important to fight with the “people issue. Single approach of countermeasure can only addresses some aspects of human errors but not all. Thus the objective of this study is to propose a model that consists of mixed approaches that can be used as countermeasures to UITs in Malaysian’s SMEs. The initial version of the proposed model was developed by combining the existing countermeasures that have been suggested in the literatures. In the second stage, the proposed model was evaluated by expert-based judgement through Delphi method to reach acceptable level of experts’ consensus and remove any uncertainty in the model. Five (5) experts with the composition of 3 practitioners and 2 academicians have evaluated the model with two-round questionnaire. Based on the evaluation, the results indicated that the experts have reach mutual consensus with mean scores more than 75% in term of the theoretical validity, usability and readability and understandability of the model. Since countermeasure is a security control used to protect the confidentiality, integrity, and availability of data and information systems and it should be available at every layer of the stack, it is hoped that the model can be used as a guideline by the organizations to improve their existing UIT countermeasures and indirectly strengthen their strategic, operational as well as financial of the organization.

الملخص

تعتبر التهديدات الداخلية غير المقصودة من أكبر المشكلات التي يمكن أن تضعف الدفاع الأمني للمنظمة. أظهرت الدراسات أن التدابير الأمنية التقنية المضادة الحالية وحدها غير كافية خاصة عندما تتعامل مع الأخطاء البشرية. لذلك ، في هذا البحث ، تم جمع ما مجموعه 311 استبياناً من مدراء تكنولوجيا المعلومات في الشركات الصغيرة والمتوسطة (SMEs) في ماليزيا لتحديد العوامل المساهمة واحتمالية التهديدات الداخلية غير المقصودة (UITs) تم تحليل البيانات الكمية باستخدام برنامج SPSS. تظهر نتائج التحليل أن غالبية المستجيبين زعموا أن منظماتهم كانت على الأرجح قد واجهت تهديدات ، حيث اعتقد 634 (34.2٪) ، 442 (23.9٪) أن منظماتهم كانت عرضة لمواجهة هذا النوع من التهديدات بينما 172 (9.3٪) كانوا على الأرجح قد واجهوا مثل هذه التهديدات. بالإضافة إلى ذلك ، كان الجهل والإهمال (27٪) والوعي بالموقف (26٪) والخطأ البشري (22٪) من أكثر العوامل المساهمة في UIT في الشركات الماليزية الصغيرة والمتوسطة. بناءً على الاستطلاع ، يُظهر أن الأساليب الدفاعية متعددة الطبقات بما في ذلك السياسات والإجراءات والضوابط الفنية والوعي والاهتمام بعلم الاجتماع والجوانب النفسية جنباً إلى جنب مع أدوات الدفاع الآلي مهمة للمؤسسة لمحاربة "قضية الأشخاص". يمكن للنهج الفردي للتدابير المضادة أن يعالج فقط بعض جوانب الأخطاء البشرية ولكن ليس كلها. وبالتالي ، فإن الهدف من هذه الدراسة هو اقتراح نموذج يتكون من مناهج مختلطة يمكن استخدامها كإجراءات مضادة تجاه الوحدات التي تعتمد على الروبوتات وخاصة في الشركات الصغيرة والمتوسطة في ماليزيا. تم تطوير النموذج عبر عدة مراحل. تم تطوير النسخة الأولى من النموذج المقترح من خلال الجمع بين التدابير المضادة الحالية التي تم اقتراحها في الأدبيات الحالية. في المرحلة الثانية ، يتم تقييم النموذج المقترح بشكل أكبر باستخدام الحكم القائم على الخبراء من خلال طريقة دلفي بهدف الوصول إلى مستوى مقبول من الإجماع بين الخبراء وإزالة أي عدم يقين في النموذج. قام خمسة (5) خبراء مع تكوين 3 ممارسين وأكاديميين بتقييم النموذج باستخدام استبيان من جولتين. بناءً على التقييم ، أشارت النتائج إلى أن الخبراء قد توصلوا إلى إجماع متبادل بمتوسط درجات أكثر من 75٪ من حيث الصلاحية النظرية وسهولة الاستخدام وقابلية القراءة والفهم للنموذج. نظراً لأن الإجراء المضاد هو عنصر تحكم أمني يستخدم لحماية السرية والنزاهة وتوافر البيانات وأنظمة المعلومات ويجب أن يكون متاحاً في كل طبقة من المكس ، فمن المأمول أن يتم استخدام النموذج كمبدأ توجيهي من قبل المنظمات لتحسين تدابيرها المضادة الحالية UIT وتعزز بشكل غير مباشر الاستراتيجية والتشغيلية وكذلك المالية للمنظمة.

TABLE OF CONTENTS

CONTENT	PAGE
AUTHOR DECLARATION	i
ACKNOWLEDGEMENTS	ii
ABSTRAK	iii
ABSTRACT	iv
MULAKHKHAS AL-BaHTH (ARABIC)	v
TABLE OF CONTENTS	vi
LIST OF TABLES	ix
LIST OF FIGURES	xi
LIST OF APPENDICES	xiii
LIST OF ABBREVIATIONS	xiv
CHAPTER 1- INTRODUCTION	
1.1 Introduction	1
1.2 Problem Statement	4
1.3 Research Questions	9
1.4 Research Objectives	9
1.5 Research Scope	10
1.6 Thesis Structure	11
1.7 Summary	12
CHAPTER 2- LITERATURE REVIEW	
2.1 Introduction	13
2.2 Role of Human in Information Security	13
2.3 Insider Threats in an Organization	16
2.3.1 Difference Between Internal and External Threats	18
2.3.2 Motives behind Insider Threat	20
2.4 Unintentional Insider Threats	21
2.4.1 Features of Unintentional Insiders	21
2.4.2 Categories of Unintentional Insider Threats	22
2.5 Contributing Factors of Unintentional Insider Threat	23
2.5.1 Direct Factors	25
2.5.2 Indirect Factors	38
2.6 Likelihood and Consequences of Unintentional Insider Threats	44
2.7 Unintentional Insider Threats Issue in Malaysia	50
2.8 Existing Countermeasure of UIT	55
2.8.1 Automation	55
2.8.2 Standard Operating Procedure (SOP)	56
2.8.3 Trust Model	56
2.8.4 Brown's Solutions to Human Error	57
2.8.4.1 Error Avoidance	57
2.8.4.2 Spatial Replication	58
2.8.4.3 Temporal Replication	58
2.8.4.4 Temporal Replication with Re-execution	59
2.8.5 Framework for Human Factors in Information Security	60
2.8.6 A Generic Model of Human Factor Management	62

2.8.7 Collaborative Reinforcement Model	64
2.8.8 Generic Mitigation Strategies for Information Leaks (2019)	66
2.8.9 UIT Mitigation Strategies and Countermeasures (Greitzer et al,2014)	68
2.9 Limitation of Existing Countermeasure	69
2.10 Unintentional Insider Threats Countermeasure Model in SMEs	73
2.11 Component Investigation	73
2.12 Small and Medium Enterprises	80
2.13 Model, Framework, Theoretical Framework and Conceptual Model	81
2.14 Appropriateness, Suitability and Usability	84
2.15 Summary	85

CHAPTER 3-RESEARCH METHODOLOGY

3.1 Introduction	86
3.2 Research Design	86
3.3 Operational Model	87
3.4 Research Framework	88
3.4.1 Conceptual Analysis	90
3.4.2 UITs in Malaysian SMEs as a case study	90
3.4.2.1 Survey Study	91
3.4.3 Conceptual Model Development	96
3.4.4 Conceptual Model Validation	99
3.4.4 .1 Validation and Reliability	99
3.4.4 .2 Approaches to Model Validation	99
3.5 Summary	107

CHAPTER4-UNINTENTIONAL INSIDER THREATS COUNTERMEASURE MODEL (UITCM) DEVELOPMENT

4.1 Introduction	109
4.2 Development Process of UIT Countermeasure Model (UITCM)	109
4.3 Step 1: Development of Initial Version of UITCM	112
4.4 Step 2: Development of Second Version of UITCM	116
4.4.1 Phase 1: Identification of Contributing Factors and Likelihood of UIT	116
4.4.1.1 Pilot Study	117
4.4.1.2 SMEs Survey	125
4.4.1.2.1 Response Rate and Data Adequacy	125
4.4.1.2.2 Instrument of Study	126
4.4.2 Phase 2: Development of Second Version of the model	138
4.4.2.1 Model Validation based on Survey Results	139
4.4.2.2 Model Development based on Component Validation	148
4.4.2.3 Relations for the Second Version of (UITCM)	151
4.5 Step 3: Development of Final Version of UITCM	162
4.5.1 Expert Validation and Expert Review	163
4.5.1.1 Selection of Experts	163
4.5.1.2 Expert Questionnaire	168
4.5.1.3 Results of Round I Delphi Method	170
4.5.1.4 Results of Round II Delphi Method	178
4.6 Summary	189

CHAPTER 5-CONCLUSION AND RECOMMENDATION

5.1 Introduction	191
5.2. Research Recapitulation	191
5.3 Unintentional Insider Threats Countermeasure Model (UITCM) In Reducing Internal Threat Environment	194
5.4 Research Contributions	196
5.4.1 Theoretical Contributions	196
5.4.2 Practical Implications	198
5.5 Limitation and Recommendation for Future Studies	200
5.6 Summary	201
REFERENCES	204
APPENDICES	235

UNIVERSITI SAINS ISLAM MALAYSIA
جامعة العلوم الإسلامية
ISLAMIC SCIENCE UNIVERSITY OF MALAYSIA

LIST OF TABLES

TABLES	PAGE
Table 2. 1: The difference Between Internal and External Threats	19
Table 2. 2: Categories of UIT Threat Vectors	22
Table 2. 3: Summary of Studies and surveys on UITs (2007-2021)	47
Table 2. 4: Summary of studies and surveys on UITs in Malaysia (2010-2021)	53
Table 2. 5: UIT Mitigation Strategies and Countermeasures by (Greitzer et al., 2014)	69
Table 2. 6: Advantages and Disadvantages of the Existing Countermeasures of the Human Error	69
Table 2. 7: The Organizational Countermeasures Components	74
Table 2. 8: The Human Factor's Countermeasures Components	75
Table 2. 9: The Automated Defence Tools Countermeasures Components	76
Table 2. 10: The Selected UIT Mitigation Strategies and Countermeasures Recommended	76
Table 2. 11: C01 Against the Second Version of UITCM	77
Table 2. 12: C02 Against the Second Version of UITCM	77
Table 2. 13: C03 Against the Second Version of UITCM	78
Table 2. 14: C04 Against the Second Version of UITCM	79
Table 2. 15: Comparison of Model, Framework, Conceptual Model and Theoretical Framework	83
Table 3. 1: Operational Model	88
Table 3. 2: Number of Questions for Each Factor	93
Table 3. 3: List of the Reviewed Conceptual Model Validation Approaches	100
Table 4. 1: (UITCM) / Initial Version development activities	112
Table 4. 2: List of References for UITCM Components	112
Table 4. 3: (UITCM) / Second Version development activities	116
Table 4. 4: Cronbach Alpha Reliability Test (Actual Study)	118
Table 4. 5: Correlations of the likelihood items (Actual Study)	120
Table 4. 6: Correlations of contributing factors of UITs (Actual Study)	123
Table 4. 7: Summary of Data Collection and Response Rate	125
Table 4. 8: Calculation Result of Sample Adequacy	125
Table 4. 9: Gender of Respondents	126
Table 4. 10: Age of Respondents	127
Table 4. 11: Respondents' Working Experience in IT Industry	128
Table 4. 12: Respondent s' Awareness of Unintentional Insider Threats	129
Table 4. 13: Policy of Organization Addressing the UIT	130
Table 4. 14: The Questions That Were Asked to Determine Likelihood of UITs.	130
Table 4. 15: Likelihood of UITs based on Six Questions	133
Table 4. 16: Mean and Standard Deviation of the likelihood of UITs	134
Table 4. 17: Question That Was Provided to Identify UITs Leading Variables.	134
Table 4. 18: The Contributing Factors of UITs	137
Table 4. 19: Mean and Standard Deviation of UITs Contributing Factors	137

Table 4. 20: The selected UIT Mitigation Strategies and Countermeasures Recommended	140
Table 4. 21: UITCM Groups and Components	148
Table 4. 22: (UITCM) / Final Version development activities	161
Table 4. 23: Profile of Experts	162
Table 4. 24: Participants' Information.	164
Table 4. 25: The comment /suggestion of the experts	170
Table 4. 26: The proposed components of UITCM with its IDs	177
Table 4. 27: Experts' answers on relevancy of the proposed components of the UITCM	179
Table 4. 28: Usability Questions with its IDs	182
Table 4. 29: Results of usability of the UITCM	183
Table 4. 30: The readability and understandability questions with its IDs	184
Table 4. 31: Results of readability and understandability of the UITCM	184

LIST OF FIGURES

FIGURES	PAGE
Figure 2. 1: Linking the Human Factor	14
Figure 2. 2: Insider Definition	17
Figure 2. 3: Insider threat characteristics	18
Figure 2. 4: Conceptual model of the insider threat problem	18
Figure 2. 5: Insider Threat profiles	21
Figure 2. 6: Insider Threats Taxonomy (The Branch of Interest of the Study Highlighted)	23
Figure 2. 7: Contributing Factors of UIT Extracted from Literatures	24
Figure 2. 8: Average Number of Internal Incidents per Year	33
Figure 2. 9: Negligence percentage among Insider Threats	34
Figure 2. 10: Percentage of accidents	45
Figure 2. 11: The distribution of accidents reported attacks	46
Figure 2. 12: Comparison of replication approaches	59
Figure 2. 13: Temporal replication with re-execution	60
Figure 2. 14: Causal loop diagram of security dynamics under the influence of risk perception	61
Figure 2. 15: A generic model of human factor management for security policy	64
Figure 2. 16: Generic Mitigation Strategies for Information Leaks (2019)	68
Figure 3. 1: Research Framework	89
Figure 3. 2: Design Science Research Method (DSRM)	97
Figure 3. 3: Model Validation Using Delphi Technique	106
Figure 3. 4: Expert's Validation Activities	107
Figure 4. 1: Summary of Activity	111
Figure 4. 2: Initial Version of UIT Countermeasure Model (UITCM)	115
Figure 4. 3: Gender of Respondent	126
Figure 4. 4: Age of Respondents	127
Figure 4. 5: Respondents' Working Experience in IT Industry	128
Figure 4. 6: Respondent s' Awareness of Unintentional Insider Threats	129
Figure 4. 7: Policy of Organization Addressing the UIT	130
Figure 4. 8: The Likelihood of UITs	133
Figure 4. 9: Second Version of UIT Countermeasure Model (UITCM)	149
Figure 4. 10: Relevancy of the proposed components of the UITCM	182
Figure 4. 11: Usability of UITCM in organization	183
Figure 4. 12: Understanding of the terms, flows, connections, and readability of the UITCM.	184
Figure 4. 13: The Final Version of unintentional insider threats countermeasures model (UITCM)/ Validated Model	186
Figure 5. 1: Final version of UITCM	

LIST OF APPENDICES

APPENDICES	PAGE
APPENDIX A: INITIAL VERSION OF UITCM/ COMPONENTS DESCRIPTION	230
APPENDIX B: UITs ONLINE QUESTIONNAIRE	237
APPENDIX C: DATASET OF THE UITs QUESTIONNAIRE	241
APPENDIX D: TABLES	242
APPENDIX E: SECOND VERSION OF UITCM/ COMPONENTS DESCRIPTION AND RELATIONS	247
APPENDIX F: MODEL VALIDATION QUESTIONNAIRES	285
APPENDIX G: SAMPLES OF EXPERT RESPONSE VIA EMAIL	293
APPENDIX H: QUESTIONNAIRES RESPONSE SAMPLES	294
APPENDIX I: FINAL VERSION OF UITCM / COMPONENTS DESCRIPTION AND RELATIONS	300
APPENDIX J: RESEARCH PUBLICATIONS	3471

ABBREVIATIONS

IT	Information Technology
UIT	Unintentional Insider Threats
PDA's	Personal Digital Assistants
CERT	The Computer Emergency Response Team
CAS	Computerized Accounting Information Systems
GDP	Gross Domestic Product
I-O	Industrial-Organizational
SETA	Security Education Training Awareness
IS	Information System.
SME	Small and Medium Enterprise
ICT	Information and Communication Technology
ISM	Information Security Management.
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
DLP	Data Loss Prevention
APT	Advanced Persistent Threat
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
RF	Radio Frequency
P2P	Peer-to-Peer networks
WPAN	Wireless Personal area network
BYOD	Bring Your Own Device
EAPs	Employee Assistance Programs
CRT	The Cognitive Reflection Test
UI	User-System Interface
UITCM	Unintentional Insider Threats Countermeasure Model