The development and evaluation of an
Information Security Awareness Capability Model:
Linking ISO/IEC 27002 controls with
Awareness Importance, Capability and Risk.

Submitted in fulfilment of the requirements
of the degree of
Doctor of Philosophy

School of Management and Enterprise
Faculty of Business, Education, Laws and Arts
The University of Southern Queensland

Robert Poepjes
Master of Information Systems (University of Southern Queensland, 2004)
Graduate Diploma of Applied Finance & Investment
(Securities Institute of Australia, 2000)
Bachelor of Business (Economics) (Edith Cowan University, 1996)
(Information Systems Audit and Control Association)

2015
ABSTRACT

This research examines the role that awareness has on the effectiveness of information security within an organisation. There is a lack of understanding as to what is an appropriate level of awareness for information security controls across an organisation. Without understanding the required awareness importance and demonstrated awareness capability, an organisation may not be able to determine whether a lack of knowledge poses information security related risks.

This study refers to Awareness Importance as how important awareness is, or how influential awareness is, in the success of a process or control. For example, when crossing a busy street it would be important to be aware of oncoming traffic before crossing. This study also refers to Awareness Capability as how aware or capable a person is when faced with a decision. It relates to the comprehension of a current situation and, for example, before a person crosses a street, are they aware or capable of comprehending the situation of the oncoming traffic? This capability will influence how successful the street crossing would be. Awareness Risk is the gap that results from the required amount of awareness (Awareness Importance) being greater than that actually being displayed (Awareness Capability).

This research is motivated by the primary question of “to what extent does the relationship between awareness importance and awareness capability predict the risks associated with an organisation’s current state of information security awareness of their information security controls?” This study suggests that by identifying the potential risks posed by any awareness gap, it is likely that improvements to the capability and posture of information security in organisations could be achieved.

There is little empirical research on how awareness influences the effectiveness of information security controls. Furthermore, scant research has been conducted on how successful or effective these education and training programs are on organisational awareness. Moreover, do they raise the perception, comprehension and decision-making of individuals and organisations in relation to potential threats? In bridging this literature gap, this current research builds and tests a theoretical
framework and model that combines aspects of ISO/IEC 27002 standard with theories of situation awareness and risk management. The resultant model is an information security awareness capability model (ISACM).

In the first phase of this research, survey data was collected from information security professionals in order to establish a benchmark Awareness Importance rating for each of the 39 main security categories and their associated control objectives in the ISO/IEC 27002 standard. These ratings, established for three stakeholder groups (IT staff, senior management, end users) within organisations, formed the first component of this study’s ISACM. In the second phase survey, situation awareness theory guided the development of an Awareness Capability instrument to capture the second component of ISACM. This instrument was used to survey two separate populations to measure awareness capability of end users against the top 10 security categories of Awareness Importance determined in phase one. Phase two survey data was used to calculate the third component of the ISACM, Awareness Risk - the gap between required awareness (Importance) and demonstrated awareness (Capability).

This research extends existing literature by contributing an approach and empirical model for measuring the required importance and capability of information security awareness within an organisation, thus identifying potential information security risks. The key findings illustrate that the required importance of awareness of information security controls differs from control to control, and differs depending on which stakeholder is involved. Finally, the study’s model calculates Awareness Risk, allowing organisations to establish where awareness is sufficient; as well as where awareness is lacking and likely to present risks.

The researcher concludes that the model developed will assist organisations in identifying awareness gaps and associated risks for specific information security control objectives across an organisation. ISACM will provide a better understanding of the level of information security awareness that exists in an organisation and where risks exist due to lower than desirable levels of awareness of information security controls. This will subsequently allow organisations to invest in the appropriate areas where unacceptable levels of risk exist.
CERTIFICATION OF DISSERTATION

The work presented in this thesis is, to the best of my knowledge and belief, original except as otherwise indicated in the text. I hereby declare that I have not submitted this material, in whole or in part, for a degree at this or any other institution.

Signed:
Robert Poepejes
Date: 01 November 2015

Signed:  M Lane
Dr Michael Lane (principal supervisor)
Date: 01 November 2015

Signed:
Associate Professor Jianming Yong (associate supervisor)
Date: 01 November 2015
ACKNOWLEDGEMENTS

My deepest and most sincere gratitude is owed to Dr Michael Lane for his limitless guidance, patience, encouragement and insight throughout the duration of my doctoral studies. Michael’s commitment and belief in the research I was undertaking has been immense and it is to a great degree that I thank him for helping me get to the finish line. Michael’s ability to provide me with academic and subject matter guidance will be life lasting for me, and his enormous capacity to help me is very much appreciated. Thank you Michael.

I would also like to thank Chris O’Reilly for her final proof read of my thesis and her suggested grammatical changes.

Finally, I would also like to thank my wife Michele, who not only displayed boundless understanding and patience with my studies, but kept me going by continuing to study herself and helped me see this through to the end. Thank you for all your support ShellBell.
# Table of Contents

1.0 Introduction ................................................................................................................. 1

1.1 Background to the research ......................................................................................... 1

1.2 Research problem, research questions and contributions ........................................ 4
  1.2.1 Research Questions ........................................................................................................ 5
  1.2.2 Contributions .................................................................................................................. 6

1.3 Justification for the research ....................................................................................... 8
  1.3.1 The Importance of the Study .......................................................................................... 8

1.4 Methodology ................................................................................................................ 9

1.5 Outline of the thesis .................................................................................................... 10

1.6 Definitions of Key Terms ........................................................................................... 13

1.7 Delimitations of scope and key assumptions, and their justifications ......................... 14

1.8 Conclusion .................................................................................................................. 15

2.0 Research Issues ........................................................................................................... 16

2.1 Introduction .................................................................................................................. 16

2.2 Parent theories and classification models .................................................................... 17
  2.2.1 Information security ....................................................................................................... 17
  2.2.2 ISO/IEC 27000 framework .......................................................................................... 22
    2.2.2.1 How aspects of ISO/IEC 27002 help contribute to better security ..................... 23
  2.2.3 Information security awareness .................................................................................... 24
    2.2.3.1 Importance of information security awareness to organisations ..................... 26
    2.2.3.2 Conducting information security awareness training ......................................... 27
    2.2.3.3 Measuring information security awareness .......................................................... 28
  2.2.4 Situation Awareness (SA) and Capability Measurement ........................................ 29
    2.2.4.1 Level 1 situation awareness - perception ............................................................. 30
    2.2.4.2 Level 2 situation awareness - comprehension ..................................................... 31
    2.2.4.3 Level 3 situation awareness - projection .............................................................. 31
    2.2.4.4 Measuring situation awareness .............................................................................. 31
    2.2.4.5 Capability measurements ...................................................................................... 32
  2.2.5 Risk management and performance gaps ............................................................... 34

2.3 ISO/IEC 27002 Standard ............................................................................................. 35
  2.3.1 Security Policy ............................................................................................................. 36
  2.3.2 Organisation of Information Security ......................................................................... 39
  2.3.3 Asset Management ....................................................................................................... 42
  2.3.4 Human Resources Security ......................................................................................... 45
  2.3.5 Physical and Environmental Security ......................................................................... 48
  2.3.6 Communications and Operations Management ........................................................ 50
  2.3.7 Access Control ............................................................................................................ 54
  2.3.8 Information Systems Acquisition, Development and Maintenance ....................... 57
  2.3.9 Information Security Incident Management .............................................................. 61
  2.3.10 Business Continuity Management .......................................................................... 64
  2.3.11 Compliance ............................................................................................................... 66

2.4 Research problem theory: analytical, theoretical frameworks and related research issues or propositions .................................................................................................................. 68
  2.4.1 Awareness Importance and the ISO/IEC 27002 standard ........................................ 69
  2.4.2 Awareness Capability and Situation Awareness ......................................................... 70
  2.4.3 Awareness Risk and the risk management standards .................................................. 72

2.5 Theoretical and conceptual model – ISACM ................................................................. 73
  2.5.1 Elements of the ISO/IEC 27002 Standard that underpin ISACM ............................ 75
  2.5.2 Elements of Situation Awareness that underpin ISACM ........................................... 76

2.6 Conclusion ................................................................................................................... 79

3.0 Methodology I .............................................................................................................. 81
3.1 Introduction

3.2 Justification for the research paradigm

3.3 Justification for the research methodology

3.3.1 The use of surveys .................................................. 84
3.3.2 Two-phased research approach .................................. 84

3.4 Phase 1 - Developing the Awareness Importance component

3.5 Survey Population Phase 1 – Awareness Importance component

3.6 Survey Development – Awareness Importance component

3.6.1 Pre-test to verify the appropriateness of each survey question 89
3.6.2 Survey Questionnaire design ....................................... 89
3.6.2.1 Survey Questionnaire layout ................................... 90
3.6.2.2 Considerations to increase response rate of the survey .... 90
3.6.2.3 Survey Questionnaire content .................................. 91
3.6.2.4 Scale used for the survey questions ............................ 92
3.6.2.5 Coding questions in Qualtrics ................................. 92
3.6.3 Pilot testing the survey questionnaire ........................... 93
3.6.4 Final survey questionnaire steps prior to survey launch ..... 93

3.7 Survey Administration

3.8 Data analysis procedures for phase 1 Survey

3.8.1 Descriptive data analysis ........................................... 94
3.8.2 Relevance for research phase 2 survey .......................... 95

3.9 Conclusion

4.0 Methodology II ................................................................ 96

4.1 Introduction

4.2 Phase 2 – Developing the Awareness Capability component

4.3 Survey Development – Awareness Capability component

4.3.1 Existing measures relevant to the research constructs ........ 97
4.3.2 Survey Questionnaire design ....................................... 98
4.3.2.1 Survey questionnaire layout .................................... 98
4.3.2.2 Considerations to increase response rate of the survey .... 99
4.3.2.3 Survey Questionnaire content .................................. 100
4.3.2.4 Scale used for awareness capability questions ............... 111
4.3.2.5 Coding questions in Qualtrics ................................. 112
4.3.3 Pre-test to verify the appropriateness of each survey question .... 112
4.3.4 Final survey questionnaire steps prior to survey launch ....... 113
4.3.5 Survey population design – Awareness Capability component . 113
4.3.5.1 Target population .................................................. 113
4.3.5.2 Population unit ..................................................... 113
4.3.5.3 Survey Population frame ....................................... 113
4.3.5.4 Population size .................................................... 114
4.3.6 Survey Administration .................................................. 114

4.4 Data analysis procedures for phase 2 survey

4.4.1 Descriptive data analysis ............................................. 116

4.5 Phase 2 – Developing the Awareness Risk component

4.6 Limitations of the methodology

4.7 Special and unusual treatment of data prior to analysis

4.8 Computer programs used to analyse data

4.9 Ethical considerations

4.10 Conclusion

5.0 Data Analysis – Research phase 1 and 2 ................................ 120

5.1 Introduction

5.2 Descriptive Statistics - Phase 1 Survey

5.2.1 Survey completion rate ............................................. 122
5.2.2 Identifying usable responses ....................................... 123
5.2.3 Demographics of Survey 1 Respondents
5.3 Deriving the Awareness Importance ratings
5.3.1 Rating Awareness Importance by stakeholder groups
5.3.2 Patterns of data for Awareness Importance
5.3.2.1 Security control clause 1: Security Policy
5.3.2.2 Security control clause 2: Organisation of Information Security
5.3.2.3 Security control clause 3: Asset Management
5.3.2.4 Security control clause 4: Human Resources Security
5.3.2.5 Security control clause 5: Physical and Environmental Security
5.3.2.6 Security control clause 6: Communications and Operations
5.3.2.7 Security control clause 7: Access Control
5.3.2.8 Security control clause 8: Information System Acquisition, Development & Maintenance
5.3.2.9 Security control clause 9: Information Security Incident Management
5.3.2.10 Security control clause 10: Business Continuity Management
5.3.2.11 Security control clause 11: Compliance
5.4 Descriptive Statistics - Phase 2 Survey
5.4.1 Survey completion rates and usable responses
5.4.2 Demographics of Survey 2 Respondents
5.4.2.1 Australian university population
5.4.2.2 MyOpinions panel population
5.5 Deriving the Awareness Capability scores
5.5.1 Pattern awareness profile of responses
5.5.2 Patterns of data for Awareness Capability
5.6 Deriving the Awareness Risk scores
5.6.1 In-depth analysis of areas of highest Awareness Risk
5.6.1.1 Awareness Capability question 1
5.6.1.2 Awareness Capability question 2
5.6.1.3 Awareness Capability question 3
5.7 Conclusion
6.0 Discussion of data analysis and findings
6.1 Introduction
6.2 Discussion of data analysis results - Research phase 1
6.2.1 Awareness Importance ratings
6.2.1.1 Security control clause 1: Security Policy
6.2.1.2 Security control clause 2: Organisation of Information Security
6.2.1.3 Security control clause 3: Asset Management
6.2.1.4 Security control clause 4: Human Resources Security
6.2.1.5 Security control clause 5: Physical and Environmental Security
6.2.1.6 Security control clause 6: Communications and Operations Management
6.2.1.7 Security control clause 7: Access Control
6.2.1.8 Security control clause 8: Information System Acquisition, Development & Maintenance
6.2.1.9 Security control clause 9: Information Security Incident Management
6.2.1.10 Security control clause 10: Business Continuity Management
6.2.1.11 Security control clause 11: Compliance
6.2.1.12 Summary of security control clauses
6.3 Discussion of data analysis results - Research phase 2
6.3.1 Awareness Capability scores
6.3.2 Awareness Risk ratings
6.3.2.1 Q1 Access Control - User Responsibilities
6.3.2.2 Q3 Access Control - Mobile computing and teleworking
6.4 The overall ISACM model
6.5 Conclusion
7.0 Conclusions and Implications
7.1 Introduction
List of Figures

Figure 1-1 Structure of Chapter 1 ........................................................................................................... 1
Figure 1-2: Model incorporating ISO/IEC 27002, Awareness Importance, Awareness Capability, and Awareness Risk .................................................................................................................. 10
Figure 2-1 Structure of Chapter 2 ........................................................................................................... 16
Figure 2-2 Relationship between the parent theories and research problem theory, and between the research problem and the research issues or propositions ..... 17
Figure 2-3 Structure of the ISO/IEC 27002 Standard ........................................................................... 35
Figure 2-4 Adapted model of Situation Awareness in dynamic decision-making.... 71
Figure 2-5 Calculating level of risk ......................................................................................................... 72
Figure 2-6 Adapted Awareness Risk matrix related to information security awareness ......................... 73
Figure 2-7 Example of risk evaluation rule set ....................................................................................... 73
Figure 2-8 Combined SALIANT model influencing Awareness Capability................. 77
Figure 2-9: Demonstration of the results from assessment of awareness importance, capability and risk ........................................................................................................................................... 78
Figure 3-1 Structure of Chapter 3 ........................................................................................................... 81
Figure 3-2: Summary of Research Design Phases 1 and 2 ................................................................. 85
Figure 3-3 Example ISO/IEC 27002 guidance material ...................................................................... 88
Figure 3-4 Example ISO/IEC 27002 Standard ..................................................................................... 91
Figure 3-5 Scale used for phase 1 Survey ............................................................................................. 92
Figure 4-1 Structure of Chapter 4 .......................................................................................................... 96
Figure 4-2 Example of scoring for survey question............................................................................... 115
Figure 4-3 Adapted Awareness Risk matrix related to information security awareness ..................... 117
Figure 5-1 Structure of Chapter 5 ........................................................................................................ 120
Figure 5-2 Summary of Awareness Importance rating by stakeholder group ..................... 127
Figure 5-3 Heatmap ranking in descending order of survey responses by Security Control Clauses .................................................................................................................................................. 129
Figure 5-4 Awareness Importance survey question scale ............................................................. 130
Figure 5-5 Attainment of SA levels ...................................................................................................... 147
Figure 5-6 Respondents showing some level of SA ........................................................................... 148
Figure 5-7 Awareness Capability Question 1.1 .................................................................................... 156
Figure 5-8 Awareness Capability Question 1.2 ................................................................................... 157
Figure 5-9 Awareness Capability Question 1.3 ................................................................................... 157
Figure 5-10 Awareness Capability Question 3.1 .................................................................................. 158
Figure 5-11 Awareness Capability Question 3.2 .................................................................................. 158
Figure 5-12 Awareness Capability Question 3.3 ............................................................................... 159
Figure 6-1: ISACM incorporating Awareness Importance, Awareness Capability, and Awareness Risk ........................................................................................................................................... 160
Figure 6-2 Structure of Chapter 6 ....................................................................................................... 160
Figure 6-3 Awareness Risk heat map.................................................................................................. 175
Figure 7-1 Structure of Chapter 7 ......................................................................................................... 180
Figure 7-2 Summary of research questions supported in this study ......................................... 181
Figure 7-3 Awareness Capability versus Situation Awareness levels ........................................... 184
Figure 7-4 High level implementation guide for the ISACM ....................................................... 193
List of Tables

Table 1-1: General Research Questions and Specific Research Questions .................. 5
Table 2-1 Eleven security control clauses of ISO/IEC 27002 .................................. 24
Table 2-2: Information Security Awareness related Literature .................................. 25
Table 2-3: Situation Awareness measurement literature ......................................... 31
Table 2-4: Karokola’s Proposed Information Security Maturity Model ....................... 33
Table 2-5 Senior management awareness aspects of communications and operations management ........................................................................................................ 52
Table 2-6 IT staff awareness aspects of communications and operations management .................................................................................................................. 52
Table 2-7 End user awareness aspects of communications and operations management .................................................................................................................. 53
Table 2-8 Senior management awareness aspects for access control ......................... 55
Table 2-9 IT staff awareness aspects for access control .......................................... 56
Table 2-10 End user awareness aspects for access control ...................................... 56
Table 2-11 Senior management awareness aspects for information systems acquisition, development and maintenance ................................................................. 59
Table 2-12 IT staff awareness aspects for information systems acquisition, development and maintenance .......................................................................................... 60
Table 2-13 End user awareness aspects for information systems acquisition, development and maintenance .......................................................................................... 60
Table 2-14 Senior management awareness of compliance aspects ............................. 67
Table 2-15 IT staff awareness of compliance aspects .............................................. 68
Table 2-16 Mapping SA levels to SA function ...................................................... 70
Table 2-17: List of security control clauses and their main security categories ....... 75
Table 3-1 Basic beliefs in inquiry paradigms .......................................................... 82
Table 3-2 Summary of research paradigms .............................................................. 83
Table 3-3: High-level steps for phase one – Develop Awareness Importance survey instrument and seek ratings for each ISO/IEC 27002 control objective based on expert knowledge and experience (RQ1) ................................................. 86
Table 3-4: High-level steps for phase two – Develop a measurement instrument for Awareness Capability (RQ2) and Awareness Risk (RQ3) ............................ 87
Table 3-5 Extract of survey responses ..................................................................... 93
Table 3-6 Analysis conducted on Phase 1 Survey data ......................................... 94
Table 4-1 Top 10 end user Awareness Importance questions from phase 1 survey .... 100
Table 4-2 Security Awareness Training Topics ..................................................... 101
Table 4-3 Extract of survey responses ..................................................................... 112
Table 4-4 Analysis to be conducted on phase 2 survey data ................................ 116
Table 5-1 Summary of Awareness Importance ratings ........................................ 121
Table 5-2 Countries of survey participants ............................................................. 122
Table 5-3 Respondents’ experience level ................................................................. 122
Table 5-4 Completion rate by Question number and Experience level .................... 123
Table 5-5 Anyone who answered Question 1 ....................................................... 124
Table 5-6 Only those who fully completed the survey .......................................... 124
Table 5-7 Experience levels of those who completed the survey ............................ 125
Table 5-8 What field of IT do they work in ............................................................. 125
Table 5-9 Final breakdown of survey respondents ................................................. 126
Table 5-10 Survey completion rate ........................................................................ 143
Table 5-11 Australian university survey – Demographics ...................................... 144
Table 5-12 Australian university survey – Digital literacy .................................. 144
Table 5-13 MyOpinions panel respondents – Demographics ................................ 144
Table 5-14 MyOpinions panel respondents – Digital literacy ................................ 145
Table 5-15 MyOpinions panel – Sector count of responses ............................... 145
Table 5-16 MyOpinions panel – Sector percentage of digital literacy ................. 145
Table 5-17 Awareness Capability extract .................................................................. 146
Table 5-18 Overall Awareness Capability – Summary by survey population ......... 147
Table 5-19 User Responsibilities .............................................................................. 149
Table 5-20 Reporting Information security events and weaknesses ....................... 149
Table 5-21 Mobile computing and teleworking ...................................................... 150
Table 5-22 Exchange of information ........................................................................ 150
Table 5-23 Media handling ...................................................................................... 151
Table 5-24 Information classification ....................................................................... 151
Table 5-25 Business requirements for access control ............................................ 152
Table 5-26 Compliance with legal requirements ..................................................... 152
Table 5-27 Responsibility for assets ......................................................................... 152
Table 5-28 Equipment security ................................................................................ 153
Table 5-29 Awareness Risk measure for end users ............................................... 154
Table 6-1 Awareness Capability – Summary by survey population ..................... 174
Table 6-2 Awareness Risk ratings ........................................................................... 176
Table 7-1 ISACM – Awareness importance, capability and risk comparison matrix .............................................................................................................. 186