

***A User-Centric Approach to the Elicitation of Information
Security Requirements***

Dale Kleeman

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

**Doctor of Philosophy (PhD)
University of Canberra**

Canberra, Australia

February 2015

Abstract

Information security research and literature has generally followed the views from practice where users are frequently seen as a weak link in the implementation of information security measures and their role in the overall information security system should be minimised if possible. This is evident in information systems security development approaches, both in the research literature and in practice, where users generally do not have a role in the security requirements elicitation process. This situation appears contrary to the more general information systems development literature where participative practices have become more commonplace.

This study recognises the critical role that users can play in information security, from the initial conceptualisation of the security measures through to the effective operation of those measures post-implementation. Information systems security development approaches are intended to improve the specification of information security requirements with positive benefits for information security outcomes. However, user awareness of information security measures will develop during the application of information systems security development approaches if the users are actively participating in the elicitation of the information security requirements. This increased security awareness will lead to improved information security outcomes for related business processes following implementation of the developed system.

This thesis focusses on these user aspects of information security and reports research that examined a range of case studies exploring user participation in the elicitation of information security requirements within systems development. Qualitative research methods were used to consider, from several perspectives, how participative practices impact on information security of associated business processes.

An initial case study involving the implementation of an electronic document and records management system considered the propensity for a range of stakeholders to engage with information security issues during a major development project, and established that users have an interest in engaging with information security issues. The case study also examined the attitudes of IT managers and project team members to user involvement in information security and found that there were competing perspectives concerning participatory development in information security.

Drawing on literature from soft systems and control self-assessment, a Process Model for the Elicitation of Control Requirements (the PMECR) was developed as an instrument for intervention for this research effort. An objective for the PMECR was that it could be integrated into the regular

requirements elicitation practices of business analysts during systems development projects. The aim of the intervention was to consider how users engaged in these security elicitation processes and the proposed PMECR was tested in various case studies. Following these applied tests, a revised version of the PMECR was formulated and presented. The case study findings support the contention that engaging with users through mechanisms such as the PMECR are feasible during information systems development and are likely to lead to improved information security outcomes. These outcomes would be achieved through improved specification of information security requirements during the development process, and through increased information security awareness as a result of these participative practices.

A theoretical model providing a framework for the consideration of issues concerned with user participation in the elicitation of information security requirements during systems development projects is proposed based on these case study findings. The theoretical model brings together the research work that has been undertaken during this project with the discussion of the literature relating to information security, soft systems methodology, control self-assessment and general user participation in information systems development projects.

Acknowledgements

This thesis has been a journey of more than eight years and has come about with the assistance of many people along the way. I am indebted to all of these people and wish to offer my gratitude for their help and support.

First of all, I wish to thank my supervisors, Professors John Campbell and Craig McDonald, both of whom have provided experience, wisdom and guidance. John, as the primary supervisor, has been patient throughout this process and has been generous with feedback and mentoring of my efforts. He has also helped me to continue on, especially during the difficult times that can sometimes surface during such a journey. Craig has assisted with all of this, has taken over when John was away, and has provided an alternative perspective at times that has been very helpful. It has been a privilege and an inspiration working with both of them.

I am grateful to my wife Helen for her support and encouragement along the way, never doubting my ability to finish, and I warmly thank her for it. Her concurrent doctoral work has made things 'interesting' at times at home, and I thank our children, Lily and Ruby, who have been growing up in the midst of it all. I hope that my bringing this research to a productive conclusion provides them, along with my older children, Kim, Jarrah and Benita, with inspiration to achieve their own ends in life. My father and brothers, as academics themselves, have helped motivate me to continue with this work and have maintained an interest in my work. My mother always had high aspirations for me, but unfortunately, died about a month before the submission of the thesis. It is a disappointment that she was unable to see the end of this part of the journey. Both parents provided me with values that are important to me and I continue to try to put into practice.

Lourdes (Lulu) Turner provided professional editing assistance on this dissertation. Professional editorial assistance was guided by terms stipulated in the *Higher Degrees by Research Policy and Procedures*, Part 7, Section 3.3 on 'Professional Editing'.

Finally, I would like to thank the Faculty of Information Sciences and Engineering and the Faculty of Business, Government and Law and especially my colleagues within the Information Systems discipline for their generosity in allowing me time within my workload so that I could continue with, and complete these studies.

List of Abbreviations and Acronyms

BA	Business Analyst
CRSA	Control Risk Self-Assessment
CSA	Control Self-Assessment
DEST	Department of Education, Science and Technology
EDRMS	Electronic Document and Records Management System
GDSS	Group Decision Support Systems
IA	Internal Audit
ISA	Information Security Awareness
ISD	Information Systems Development
ISS	Information Systems Security
IT	Information Technology
PGP	Pretty Good Privacy
PMECR	Process Model for Elicitation of Control Requirements
SBA	Systems-Based Auditing
SRM	Security Risk Management
SSM	Soft Systems Methodology
WPP	Workplace Productivity Programme

Table of Contents

Chapter 1 Introduction	1
1.1 Introduction.....	1
1.2 Research origins	2
1.3 Research aims.....	6
1.4 Research contribution	7
1.5 Outline of the thesis	7
1.5.1 Chapter 1 – Introduction	7
1.5.2 Chapter 2 – Literature review and discussion of key concepts.....	8
1.5.3 Chapter 3 – Research methodology.....	8
1.5.4 Chapter 4 – The DocMan case study.....	8
1.5.5 Chapter 5 – Implementing the Process Model for Eliciting Control Requirements.....	8
1.5.6 Chapter 6 – A theoretical model of user participation with information security issues within information systems development projects.....	9
1.5.7 Chapter 7 – Conclusion.....	9
1.5.8 Appendices	9
1.6 Conclusion	9
Chapter 2 Literature review and discussion of key concepts	11
2.1 Introduction.....	11
2.1.1 Information security requirements and user requirements	12
2.2 User involvement in systems development requirements	13
2.3 Information Security.....	16
2.3.1 Information security and user participation	16
2.3.2 Information systems security development approaches.....	19
2.3.3 Information security user involvement and awareness.....	21
2.3.4 Risk assessment and risk management.....	24
2.3.5 Control Self-Assessment and internal audit methodologies.....	32
2.4 Soft Systems Methodology.....	37
2.4.1 Some key SSM concepts.....	38
2.4.2 Developing SSM activity models	43
2.4.3 Why SSM might be useful to the CSA context?.....	45
2.5 Conclusion	47
Chapter 3 Research Methodology	49
3.1 Introduction.....	49
3.2 Research aims and research purpose.....	49
3.3 Research approaches within the information systems discipline	50
3.4 Research design.....	55
3.4.1 The DocMan case study.....	57
3.4.2 The PMECR case studies.....	59
3.5 The process model for eliciting control requirements (PMECR)	60
3.6 Conclusion	63
Chapter 4 The DocMan Case Study	65
4.1 Background.....	65

4.2	Timeline of significant events in the DocMan project.....	66
4.2.1	General project history.....	66
4.2.2	Researcher involvement in the DocMan Project	68
4.2.3	Documents considered.....	70
4.2.4	Stakeholder analysis and organisational units considered	70
4.3	Interviews	73
4.3.1	General awareness of information security issues	74
4.3.2	Previous experience in participating in the specification of requirements generally, and information security requirements in particular	76
4.4	Data analysis.....	77
4.4.1	Motivations of users to be involved with information security.....	77
4.4.2	Competing objectives for information security between senior IT managers and project team members.....	80
4.4.3	User engagement with information security during requirements gathering and developer resistance	85
4.4.4	General perceptions on information security	88
4.4.5	Information security measures adversely interfering with the performance of work	89
4.5	Concluding remarks about the DocMan case study.....	92
Chapter 5 Implementing the Process Model for Eliciting Control Requirements.....		95
5.1	Introduction.....	95
5.2	Background.....	95
5.2.1	Phase 1 testing of the PMECR	97
5.2.2	Phase 2 testing of the PMECR	99
5.3	Research tasks with the application of the PMECR to IT projects.....	100
5.3.1	Criteria for evaluating the application of the PMECR	101
5.4	Case studies	103
5.4.1	Case study 1 – Canberra Times mobile application	103
5.4.2	Case study 2 – Taxi booking application.....	105
5.4.3	Case study 3 – Trusted Access Security System	107
5.4.4	Case 4 – All in One e-Commerce Solution.....	109
5.4.5	Case 5 – Risk Treatment Database (RTD)	110
5.4.6	Case 6 – Riding School Administration.....	110
5.5	Summary evaluation.....	111
5.6	Analysis of case study outcomes	116
5.6.1	Difficulties engaging users.....	116
5.6.2	Use of the activity models	118
5.6.3	Adaption of tools within the PMECR.....	120
5.6.4	Source of materials used to define information security control requirements	121
5.7	The revised PMECR.....	122
5.8	Conclusion	123
Chapter 6 A theoretical model of user participation with information security issues within information systems development projects		125
6.1	Introduction.....	125
6.2	The developed theoretical model	125

6.2.1	Improved information security outcomes	126
6.2.2	The theoretical model of user participation with information security issues within information systems development projects	126
6.2.3	User awareness of information security measures.....	128
6.2.4	Participants.....	129
6.2.5	Business analysts and project managers.....	131
6.2.6	Types of involvement	132
6.2.7	Choice of participation methods.....	134
6.3	The theoretical model and information systems theory.....	135
6.4	Conclusion	136
Chapter 7	Conclusion	139
7.1	Summary of key issues	139
7.2	Fulfilment of objectives and research contribution	142
7.2.1	Summary of the contribution to knowledge	144
7.3	Study limitations.....	145
7.4	Future research	146
7.4.1	Issues from the development and application of the PMECR.....	147
7.4.2	Issues from the theoretical model of user participation with information security within information systems development projects, as presented in Chapter 6.....	148
7.5	Concluding remarks.....	149
References	151
Appendices	159
2.1	Australian standards and key texts relating to risk management and information security.....	161
3.1	Process model for eliciting control requirements (PMECR).....	167
3.2	Revised version of the PMECR.....	177
4.1	Ethics committee documentation for the DocMan research.....	189
4.2	Raw data analysis of the DocMan interviews	197
5.1	Information security issues in ITP projects – 2011.....	205
5.2	Chapter 5, Case Study 1 details and information security related artefacts	217
5.3	Chapter 5, Case Study 2 details and information security related artefacts	223
5.4	Chapter 5, Case Study 3 details and information security related artefacts	233

List of Figures

Figure 2.1 Updated IS participation theory elements.....	15
Figure 2.2 Risk management process	26
Figure 2.3 The history and development of CSA.....	34
Figure 2.4 The conventional seven-stage model of SSM	39
Figure 2.5 The process of SSM	40
Figure 2.6 The LUMAS model: Learning for a User by a Methodology-informed Approach to a problem Situation	42
Figure 2.7 A generic conceptual model	44
Figure 2.8 A generic activity model.....	45
Figure 3.1 The IS field: a pragmatic model of aspects relevant to describing it and researching in it	51
Figure 3.2 An overview of the processes involved in this research project	55
Figure 4.1 Simplified organisational chart	71
Figure 6.1: A proposed theoretical model connecting participation by stakeholders with information security issues in systems development situations to improved information security outcomes.....	127