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

List of Figures