An Examination of Information System Risk Perceptions Using the Repertory Grid Technique

by

MALCOLM R PATTINSON

B. App. Sc. (South Australian Institute of Technology)

M. Comm. (Research) (Flinders University)

Submitted in total fulfilment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

in

Business School, Faculty of The Professions

University of Adelaide

Date Submitted: April 2012

TABLE OF CONTENTS

ABSTRACT

The increasing dependence on information systems (ISs) together with the emergence of new technologies, threats and risks has reinforced the need for a higher level of information security (InfoSec) within most organisations. The traditional management approach to mitigating such IS risks has been to implement hardware and software solutions. However, academics and practitioners are beginning to appreciate that solutions relating to the human behavioural aspects of InfoSec are an equally, if not more, effective solution. For example, if management know how their computer users perceive the risks to their organisation's ISs and what situational factors influence these perceptions, they can use this information to design and instigate intervention strategies to improve user behaviour.

The aim of this research is to contribute to the knowledge pertaining to InfoSec behaviour by examining the perceptions that computer users have of the risks to their organisation's ISs and by indentifying the major situational factors that influence these perceptions.

Due to the human cognitive aspect of this aim, the research design necessitated a qualitative component and therefore a two-stage hybrid qualitative-quantitative approach was adopted. Stage 1 involved a series of semi-structured interviews with typical computer users from a variety of organisations for the purpose of developing a Repertory Grid Technique (RGT) interviewing instrument to be used in the next stage. Stage 2 of this research involved a series of structured interviews, embedded with this instrument to elicit IS risk perceptions of computer users. This raw data was then analysed both qualitatively and quantitatively to generate research findings.

The findings of these analyses indicate that, in general, computer users perceive that the most serious IS risks are:

- damage to an organisation's reputation and credibility
- an increase in costs; systems becoming unavailable and inaccessible, and
- the inability to do their job properly.

The situational factors that have a major impact on these IS risk perceptions are:

- the type of loss suffered
- the extent of personal impact, and

- the severity and scope of the impact.

When these findings are combined, the types of loss that are perceived as being most significant are:

- loss of productivity (due to systems being unavailable and the inability to access data)
- loss of reputation, credibility and image, and
- financial loss (due to the need for additional resources to recover systems and data).

This research also implies that:

- Computer users with a high level of InfoSec awareness perceive reputation damage and loss of credibility as the most serious risk compared to those with less awareness of InfoSec who are more concerned about their own welfare, rather than the impact to their organisation.
- The more InfoSec-aware computer users are, the more they believe that the existing controls and safeguards are the reason that InfoSec breaches will occur and will have a wide-ranging impact.
- The higher an employee is within their organisational structure, the more concerned he or she is about organisational risks as compared to personal risks.
- Male computer users identify damage to their organisation's reputation as a serious risk, however, they are more concerned about "why" the organisation is at risk.
- Female computer users, on the other hand, seem to have a far more balanced view of the IS risks than their male counterparts, but do not recognise that damage to their organisation's reputation is a serious risk.

Armed with these research findings, InfoSec managers are better placed to design human behavioural solutions, such as InfoSec awareness seminars, into their InfoSec management plans. Furthermore, this research demonstrates that the RGT is a highly appropriate technique to elicit IS risk perceptions of computer users and that management would benefit from its use if they needed to evaluate their own employees.

DECLARATION

This work contains no material which has been accepted for the award of any other degree or diploma in any university or other tertiary institution to Malcolm Robert Pattinson and, to the best of my knowledge and belief, contains no material previously published or written by another person, except where due reference has been made in the text.

I give consent to this copy of my thesis, when deposited in the University Library, being made available for loan and photocopying, subject to the provisions of the Copyright Act 1968.

I also give permission for the digital version of my thesis to be made available on the web, via the University's digital research repository, the Library catalogue, the Australasian Digital Theses Program (ADTP) and also through web search engines, unless permission has been granted by the University to restrict access for a period of time.

Signed:…….. Date: ……

Malcolm R Pattinson

ACKNOWLEDGMENTS

The author expresses his sincere appreciation to his Principal Supervisor, Dr Cate Jerram of the Business School, Faculty of the Professions, The University of Adelaide. Despite going through a difficult time for her family and the enormous workload she always takes on, somehow she made the time to ensure that this thesis met the highest of standards. She was responsible for introducing me to qualitative research and although I initially resisted due to my positivist background, I am a better person for it.

Thanks also to Dr Marcus Butavicius and Kathryn Parsons, both from the DSTO, for lending me their expertise; to my good friend Dr David Ayre for his valuable comments; and to a fellow PhD student, Dr Melanie Smans, for sharing the same frustrations and issues associated with the PhD process.

There was also a small cohort of ex-colleagues from the University of South Australia who acted as great sounding boards as we all strove to finish PhD's late in life. Thanks to each of you, especially Dr Don Falconer and Chris Stewart.

And finally, I wish to acknowledge my wonderful partner Maureen, for having faith in me by letting me do what I wanted to do and for supporting me superbly along the way.

ACRONYMS USED IN THIS THESIS

CEO	Chief Executive Officer
CFO	Chief Financial Officer
CIA	Confidentiality, Integrity and Availability
CIO	Chief Information Officer
CISO	Chief Information Security Officer
DR	Disaster Recovery
HCI	Human Computer Interaction
ICT	Information and Communications Technology
IFS	Index of Factorial Simplicity
InfoSec	Information Security
IP	Internet Protocol
IS	Information System
ISs	Information Systems
IT	Information Technology
MIS	Management Information System (s)
NIST	National Institute of Standards and Technology
PCA	Principal Component Analysis
PCAs	Principal Component Analyses
PCP	Personal Construct Psychology
PCT	Personal Construct Theory
RGT	Repertory Grid Technique
USB	Universal Serial Bus

LIST OF FIGURES

LIST OF TABLES