

**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	5
DECLARATION	7
ACKNOWLEDGMENTS	8
ACRONYMS USED IN THIS THESIS	9
LIST OF FIGURES	10
LIST OF TABLES	11
CHAPTER 1: INTRODUCTION	12
1.1 AIM OF THIS STUDY AND THE RESEARCH QUESTION	15
1.2 SIGNIFICANCE OF THIS STUDY	15
1.3 SCOPE OF THIS RESEARCH	17
1.4 CONCEPTUAL FRAMEWORK	17
1.5 THE STRUCTURE OF THIS THESIS	20
CHAPTER 2: LITERATURE REVIEW OF PERCEPTIONS OF RISKS TO INFORMATION SYSTEMS	22
2.1 KEY TERMS AND DEFINITIONS	24
2.1.1 <i>Information Security (InfoSec)</i>	24
2.1.2 <i>Risks and Threats</i>	26
2.1.3 <i>Information System (IS) Risk</i>	28
2.1.4 <i>IS Risk Perception</i>	28
2.1.5 <i>Factors that Influence IS Risk Perceptions</i>	29
2.1.6 <i>Computer Users</i>	30
2.2 GENERAL RISK	32
2.2.1 <i>Perceptions of General Risk</i>	34
2.2.2 <i>Factors that Influence Perceptions of General Risk</i>	37
2.2.3 <i>Summary of General Risk Research</i>	38
2.3 INFORMATION SECURITY (INFOSEC)	38
2.3.1 <i>Behavioural Aspects of InfoSec</i>	41
2.3.2 <i>IS Risks and Perceptions</i>	46
2.3.3 <i>Factors that Influence IS Risk Perceptions</i>	48
2.3.4 <i>Summary of InfoSec Research</i>	49

2.4	DATA COLLECTION AND ANALYSIS TECHNIQUES	50
2.4.1	<i>Repertory Grid Technique (RGT)</i>	51
2.4.2	<i>Structured Interviews</i>	56
2.4.3	<i>Coding and Categorisation</i>	57
2.4.4	<i>Content Analysis</i>	57
2.4.5	<i>Principal Component Analysis (PCA)</i>	58
2.4.6	<i>Summary of Data Collection and Analysis Techniques Research</i>	59
2.5	CHAPTER SUMMARY	59
CHAPTER 3: RESEARCH METHODOLOGY		61
3.1	THE NATURE OF THE RESEARCH PROBLEM	61
3.2	THE RESEARCH PROCESS	63
3.2.1	<i>Nomothetic or Idiographic Approach</i>	65
3.3	EPISTEMOLOGY	66
3.3.1	<i>Constructionism</i>	67
3.3.2	<i>Constructive Alternativism</i>	67
3.4	THEORETICAL PERSPECTIVE	67
3.4.1	<i>Interpretivism</i>	68
3.5	METHODOLOGY	69
3.5.1	<i>Two-stage Hybrid Approach</i>	70
3.6	METHODS	71
3.6.1	<i>Repertory Grid Technique (RGT)</i>	72
3.6.2	<i>Structured Interviews</i>	73
3.6.3	<i>Coding and Categorisation</i>	74
3.6.4	<i>Content Analysis</i>	75
3.6.5	<i>Principal Component Analysis (PCA)</i>	75
3.7	RISKS, LIMITATIONS AND KEY ASSUMPTIONS	76
3.8	TRUSTWORTHINESS	78
3.9	CHAPTER SUMMARY	78
CHAPTER 4: STAGE 1: DEVELOPMENT OF THE REPERTORY GRID INSTRUMENT		80
4.1	JUSTIFICATION	80
4.1.1	<i>“Supplied” versus Elicited Elements</i>	82
4.2	DATA COLLECTION	82
4.2.1	<i>Choice of RGT Elements</i>	83
4.2.2	<i>Interviewees</i>	85
4.2.3	<i>Semi-structured Interviews</i>	86

4.3	DATA ANALYSIS	86
4.3.1	<i>Transcription</i>	87
4.3.2	<i>Coding</i>	87
4.3.3	<i>Categorisation</i>	87
4.3.4	<i>Selection of Elements</i>	90
4.4	CHAPTER SUMMARY	93

CHAPTER 5: STAGE 2: DATA COLLECTION AND ANALYSIS **95**

5.1	BACKGROUND	95
5.2	DATA COLLECTION	96
5.2.1	<i>Interviewees</i>	97
5.2.2	<i>Structured Interviews</i>	98
5.2.3	<i>Miscellaneous</i>	106
5.3	DATA ANALYSIS	108
5.3.1	<i>Type of Data</i>	109
5.3.2	<i>Qualitative and Quantitative Analyses</i>	110
5.3.3	<i>Repertory Grid Analysis Software</i>	111
5.3.4	<i>Identification of IS Risk Perceptions</i>	111
5.3.5	<i>Identification of Threat Perceptions</i>	128
5.3.6	<i>Identification of Situational Factors</i>	130
5.4	CHAPTER SUMMARY	138

CHAPTER 6: FINDINGS AND DISCUSSION **140**

6.1	FINDINGS PERTAINING TO IS RISK PERCEPTIONS	140
6.1.1	<i>IS Risk Perceptions and Individual InfoSec Awareness</i>	146
6.1.2	<i>IS Risk Perceptions and Organisational Level</i>	154
6.1.3	<i>IS Risk Perceptions and Gender</i>	160
6.2	FINDINGS PERTAINING TO THREAT PERCEPTIONS	164
6.2.1	<i>Threat Perceptions and Individual InfoSec Awareness</i>	165
6.2.2	<i>Threat Perceptions and Organisational Level</i>	167
6.2.3	<i>Threat Perceptions and Gender</i>	168
6.3	FINDINGS PERTAINING TO SITUATIONAL FACTORS	169
6.4	FINDINGS PERTAINING TO THE USE OF THE RGT	175
6.5	LIMITATIONS	177
6.6	CHAPTER SUMMARY	180

CHAPTER 7: CONCLUSIONS	183
7.1 OVERVIEW	184
7.2 IMPLICATIONS FOR RESEARCH	185
7.3 IMPLICATIONS FOR THE MANAGEMENT OF INFOSEC	186
7.4 OPPORTUNITIES FOR FURTHER RESEARCH	186
7.5 CHAPTER SUMMARY	187
REFERENCES	189
APPENDICES	204
1. STAGE 1 INTERVIEW STRUCTURE	204
2. STAGE 2 INTERVIEW STRUCTURE	206
3. CONTACT SUMMARY FORM	208

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 identifying 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

1 - 1	InfoSec Input-Process-Output Model	14
1 - 2	Conceptual Framework of this Research	19
2 - 1	Scope of Literature Review	23
2 - 2	InfoSec Model	25
3 - 1	How InfoSec Maps onto Burrell <i>et al</i> (1979) Four Sociological Paradigms	62
3 - 2	The Research Process of this Thesis	65
4 - 1	Types of Grids	81
4 - 2	Categories of Threats	92
4 - 3	RGT Interview Sheet Showing the “Supplied” Elements Common to every Interview	94
5 - 1	Filled-in Sample Repertory Grid Interview Form	101
5 - 2	IS Risk Perception Categories (Version 1)	114
5 - 3	IS Risk Perception Categories (Version 2)	117
5 - 4	IS Risk Perception Categories (Version 3)	118
5 - 5	IS Risk Perception Categories (Final Version)	120
5 - 6	Sample Grid Calculations	122
5 - 7	Content Analysis of All Interviewees	127
5 - 8	Threat Perception Analysis for a Sample Interviewee	129
5 - 9	Sample Text File for Input into GRIDSTAT	131
5 - 10	Principal Component Analysis Results	132
6 - 1	Content Analysis of All Interviewees	144
6 - 2	Content Analysis of Interviewees with High InfoSec Awareness	147
6 - 3	Content Analysis of Interviewees with Medium InfoSec Awareness	149
6 - 4	Content Analysis of Interviewees with Low InfoSec Awareness	151
6 - 5	Content Analysis of Interviewees at Senior Management Level	155
6 - 6	Content Analysis of Interviewees at Operational Level	156
6 - 7	Content Analysis of Interviewees at Transactional Level	158
6 - 8	Content Analysis of Male Interviewees	161
6 - 9	Content Analysis of Female Interviewees	162

LIST OF TABLES

2 - 1	Psychometric Paradigm	35
2 - 2	A Selection of Computer User Behaviours	42
2 - 3	The 11 Corollaries of Kelly's Personal Construct Theory (PCT)	52
3 - 1	Justification for Using an Interpretive Approach for this Study	69
3 - 2	Features of Quantitative vs. Qualitative Research	
	Approaches to Analysing RGT Grids	73
4 - 1	Categorised Items in Order of Number of Times Referenced	89
4 - 2	The 17 Threats Showing Selected Threats Shaded	91
5 - 1	Interviewee Profile	98
5 - 2	Percentage Similarity Look-up Table	123
5 - 3	Varimax Rotated Construct Factor Loadings	134
5 - 4	Retained Components	135
5 - 5	Situational Factor Labels	137
6 - 1	Allocation of Constructs to Categories and Themes	142
6 - 2	IS Risk Perceptions Relating to InfoSec Awareness	152
6 - 3	IS Risk Perceptions Relating to Organisational Level	159
6 - 4	IS Risk Perceptions Relating to Gender	163
6 - 5	Overall Threat Perceptions	165
6 - 6	Threat Perceptions and InfoSec Awareness	166
6 - 7	Threat Perceptions and Organisational Level	167
6 - 8	Threat Perceptions and Gender	168
6 - 9	Retained Components	169
6 - 10	Situational Factor Labels	170
6 - 11	Summary of Principal Component Analyses	
	Showing Labelled Components	172
6 - 12	Major Situational Factors	173