INFORMATION SECURITY MANAGEMENT: AN EMPIRICAL ANALYSIS OF ITS CONSTITUTION

By

Daniel John Oost

A thesis submitted for the Degree of Doctor of Philosophy

School of Management, Faculty of Business

University of Technology, Sydney

August, 2009

CERTIFICATE OF AUTHORSHIP/ORIGINALITY

I certify that the work in this thesis has not previously been submitted for a degree nor has it been submitted as part of requirements for a degree except as fully acknowledged within the text.

I also certify that the thesis has been written by me. Any help that I have received in my research work and the preparation of the thesis itself has been acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis.

Signature of candidate

Production Note:
Signature removed prior to publication.

ACKNOWLEDGMENTS

I would like to acknowledge the ongoing support and encouragement provided by my supervisor Professor Stewart Clegg and co-supervisor Professor Eng Chew. As the reader will shortly become aware, the support was provided not only in person but in book and journal form. I am greatly indebted to Professor Stewart Clegg's expert writings on the topic of power. Professor Eng Chew's wealth of experience as a practitioner provided an invaluable complement to this theoretical assistance.

Further, the coursework subjects led by Professor Carl Rhodes were an excellent preparation for my PhD work. I also valued the advice and support provided by Professor Carl Rhodes and Associate Professor Alison Pullen outside of the formal coursework setting.

I also need to express my gratitude for the generosity of the members of the participant organisation. The level of assistance provided and interest shown was a tremendous help.

Finally, I would like to thank my father, Jacob, and my Brother, Ben, for their proofreading efforts.

TABLE OF CONTENTS

CERTIFICATE OF AUTHORSHIP/ORIGINALITY ii
ACKNOWLEDGMENTS iii
TABLE OF CONTENTS iv
LIST OF FIGURES AND TABLES vi
Figures vi
Tables vi
ABSTRACT vii
ABSTRACT vii
INTRODUCTION 1
Outline of the thesis 1
What is information security and why is it important? 2
CHAPTER ONE: LITERATURE REVIEW 12
Threats to the security of organizational information environments 12
Means of controlling threats to organizational information environments 30
CHAPTER TWO: A REVIEW AND CRITIQUE OF INFORMATION SECURITY CULTURE RESEARCH 52
What does information security culture add to the understanding of information security? 55
An oversimplified link between culture and behaviour 58
Ease with which to change a culture exaggerated 61
Conclusion 66
CHAPTER THREE: COMPLEXITIES OF CULTURE AND POWER 68
The gap between intent and actualisation 68
Lukes' three dimensions of power 70
A history and classification of organizational research on power 77
Changing concepts of power, changing concepts of politics 83
Identity manipulation and resistance 86
Power as it is understood in this thesis 90
Conclusion 92
CHAPTER FOUR: RESEARCH QUESTION AND APPROACH 94
Research question 94
Research design 95
Methodology 98
Empirical data and its interpretation 101
Reflexive interpretation 104
Linguistic context 110
Final comments on reflexive interpretation 112
Coding 114
CHAPTER FIVE: ANALYSING THE DATA 117
Setting the scene 119
The data 122
Policy deviations and socialisation 124
Socialisation 131
Tracking 133
Consistent decisions 138

Outside normal process 147
Responsibility for risk 152
'Power to' and 'Power over' 163
Outsourcing 171
Cultural change 175
Responsibility in the context of undecidability 182
Conclusion 190
CHAPTER SIX: THE DATA AS (ANTE)NARRATIVE 193
Analysis of the first section of data 196
Analysis of the second section of data 203
Analysis of the third section of data 205
Analysis of the fourth section of data 214
Different positions in the polyphony 219
Narrative and antenarrative 221
CHAPTER SEVEN: CONCLUSION, SIGNIFICANCE, AND LIMITATIONS 224
Implications for theory 228
Implications for practice 232
Limitations 235
Suggestions for further research 235
APPENDIX A: TEXT FOR INITIAL IDEAS ON THEMES AND THEIR LINKAGES WITH THE DATA COLLECTED 237
APPENDIX B: TEXT FOR PRELIMINARY IDEAS ABOUT HOW FOCUSED DATA THEMES INTERRELATE 241
APPENDIX C: KEY EXTRACT WITH LINE NUMBERS 244
APPENDIX D: COMPLETE TRANSCRIPT OF THE FIRST WEEKLY MANAGEMENT MEETING ATTENDED 263
REFERENCES 312

LIST OF FIGURES AND TABLES

Figures

Figure 4.1 Initial ideas on themes and their linkages with the data collected.... 102
Figure 4.2 Preliminary ideas about how focused data themes interrelate.... 105

Tables

Table 1.1 Information security issues and their importance from Knapp et al. (2006b).... 13
Table 1.2 External information security breaches from Deloitte Touche Tohmatsu (2008).... 14
Table 1.3 Internal information security breaches from Deloitte Touche Tohmatsu (2008).... 15
Table 1.4 Types of attack or misuse respondents suffered from Computer Security Institute (2008).... 16
Table 1.5 Percentage of losses from insider threats from Computer Security Institute (2008).... 17
Table 1.6 Types of breaches suffered by UK businesses from PricewaterhouseCoopers (2008).... 18
Table 1.7 Worst security incident suffered from PricewaterhouseCoopers (2008).... 18
Table 1.8 Respondents' answers to the question 'What drives information security expenditure?' from PricewaterhouseCoopers (2008).... 19
Table 1.9 Percentage of UK businesses that have suffered from staff misuse of information systems from PricewaterhouseCoopers (2008).... 20
Table 1.10 Respondents' answers to the question 'What type of staff misuse did UK businesses suffer?' from PricewaterhouseCoopers (2008).... 20
Table 1.11 Respondents' answer to the question 'If experienced electronic attacks, how many from the outside?' from Australian Computer Emergency Response Team (2006).... 21
Table 1.12 Respondents' answer to the question 'If experienced electronic attacks, how many from the inside?' from Australian Computer Emergency Response Team (2006).... 21
Table 1.13 Respondents' answer to the question 'Which of the following types of electronic attack, computer crime, or computer access misuse or abuse did your organization detect in the last 12 months?' from Australian Computer Emergency Response Team (2006).... 22
Table 1.14 Respondents' answer to the question 'In terms of the threat faced by your organization, what factors may have contributed to those electronic attacks which harmed the confidentiality, integrity or availability of your network data or systems in the last 12 months?' from Australian Computer Emergency Response Team (2006).... 23
Table 1.15 Respondents' answer to the question 'In terms of your organization's potential vulnerabilities, what factors may have contributed to those electronic attacks which harmed the confidentiality, integrity or availability of your network data or systems in the last 12 months?' from Australian Computer Emergency Response Team (2006).... 24
Table 1.16 Respondents' answer to the question 'What aspects of computer security management does your organization find most challenging or problematic?' from Australian Computer Emergency Response Team (2006).... 25
Table 1.17 Taxonomy of security behaviours from Stanton et al. (2005).... 45
Table 3.1 Three dimensions of power from Hardy (1996).... 74
Table 3.2 Mobilizing the dimensions of power from Hardy (1996).... 75
Table 4.1 Reasons for refusal to participate in pilot study conducted by Kotulic and Clark (2004).... 96
Table 4.2 Top four reasons for non-response to survey conducted by Kotulic and Clark (2004).... 96
Table 5.1 'Power to' and 'power over' from Göhler (2009).... 169
Table 5.2 'Transitive' and 'intransitive' power from Göhler (2009).... 169
Table 6.1 Analysis of the first section of data.... 196
Table 6.2 Analysis of the second section of data.... 203
Table 6.3 Analysis of the third section of data.... 205
Table 6.4 Analysis of the fourth section of data.... 214

ABSTRACT

This thesis addresses the following research questions:

> *How does analysis of the everyday discursive work of information security managers inform us about the phenomena that they constitute as 'information security?' What does it mean to 'do' information security?*

These questions are worth asking given the importance of information to organizations (Hong et al. 2003), the extent of current information security problems (Knapp et al. 2006a), a lack of empirical research on information security (Kotulic and Clark 2004), and a preponderance of research on technical solutions to information security problems conceived in technical terms (Dhillon and Backhouse 2001). In response to this situation some scholars propose simplistic 'cultural' solutions, without empirical basis.

To answer the research questions, and help address the abovementioned problems, I observed and recorded three months of weekly meetings of a group of information security managers at a large organization. The analysis of the data in order to develop answers to the research questions followed the reflexive interpretation approach advocated by Alvesson and Sköldberg (2000). The interpretive repertoire drawn upon to interpret the data and its relationship to my research questions centred on writings on power by Clegg (1989), Clegg et al. (2006a), Haugaard (1997), Hayward and Lukes (2008) and Lukes (2005), complemented by other resources.

The reflexively interpreted data, informed by the abovementioned writings on power, suggested that an integral part of the managers' 'doing' of information security involves the management of excess responsibility relative to their power to achieve a secure state. This is an inevitable dilemma given that a fundamental information security management problem, aside from the damage breaches cause for organizations, is that its very definition implies an unrealisable state. No system is completely secure (Straub and Welke 1998; Stewart 2004).

The management of responsibility took the form of devising authorised processes constituted by rules. The decision as to whether to act or not in relation to a potential information security problem is envisioned by the managers as a result of an application of rules, rather than individual agency. If an information security breach were to result (an ever present threat) the process would ideally be to blame, in effect absorbing the responsibility. However, rules require interpretation by agents (Clegg 1989) and are potentially subject to multiple interpretations. Agency and the management of its requisite responsibility cannot be escaped. A number of implications are developed as a result of this reflexive interpretation of the data, both theoretical and practical.