UNIVERSITY OF SOUTHERN QUEENSLAND

PSYCHOLOGICAL THEORIES AND THEIR APPLICABILITY IN RESOLVING ISSUES WITH UNAUTHRORISED COMPUTER ACCESS

A Dissertation submitted by

Angela A M Howard

For the award of

Master of Business Research

2011

Abstract

Literature has shown that technical solutions are not completely successful in securing information systems from intruders. Previous attempts to develop hacker profiles are still incomplete and time consuming to apply. Prior studies in social engineering and expectancy theory have shown that they can address some of the issues organisations are encountering, especially in employees disclosing sensitive organisational data. Therefore, using these studies in an organisational context may provide clues to how the disclosure of information can be contained. This aspect was posited in the main research question:

How can education affect the process of preventing social engineering to minimise the success of unauthorised intrusion?

While answering the main research question, due to time constraints, this study focussed only on social engineering as the main cause of disclosing organisational data. This aspect was determined using psychological theories and their applicability in resolving issues with unauthorised computer access. Qualitative approach was used as the main data collection technique and two focus groups were employed in collecting data. The University of Southern Queensland was used as the case organisation and suitable samples were drawn for a 2 x 90-minute focus group sessions. The qualitative data were analysed using two prominent text analysis applications, namely, Leximancer 3.5 and NVivo 8.

This qualitative data analysis identified 5 crucial themes. These themes are security awareness, unauthorised access, social engineering, policies and procedures, and education. It is inferred from the data that changes in the way policies and procedures implemented can have marked improvement in security aspects, especially in containing the leakage of organisational data. Thus, this research can assert that a change in policies and procedures can have an impact on unauthorised access.

New findings of the study include that staff are proactively looking for more secure ways in their processing and creating new procedures as they go, and that there seems to be a disconnect between access to information systems and the organisational data. Future research can expand on the model created for this research and focus on expectancy theory as well as quantitative methodology so that outcomes can be generalised.

CERTIFICATION OF DISSERTATION

I certify that the ideas, data collection, data analysis, discussion and conclusion reported in this dissertation are entirely my own effort, except where otherwise acknowledged. I also certify that the work is original and has not been previously submitted for any other award, except where otherwise acknowledged.

_____ _____

Signature of Candidate Date

ENDORSEMENT

_____ _____

Signature of Supervisor Date

_____ _____

Signature of Associate Supervisor Date

Acknowledgements

I would like to use this opportunity to thank those people who have assisted me throughout this research dissertation.

My first appreciation goes to my supervisor Professor Raj Gururajan. It is through his support and expertise that I was able to make it through this dissertation. Guiding me through the early stages to find my feet, making the call to the Chief Information Officer was a first step in finding participants for the data collection, and answering the many questions I had. Raj's reassurance, that I was on the right track with my dissertation, gave me the confidence to continue and complete this dissertation.

I would also like to thank my Associate supervisor Dr Abdul Hafeez-Baig, who was always there to provide support and encouragement, sharing his experience with focus groups and sitting in on the focus groups to support me.

Both my supervisors have allowed me the freedom to find my way while making sure that I did not get lost and have nurtured my growth in developing my research skills.

I would like to thank all staff members and students, whom I cannot name due to privacy and confidentiality, who have participated in the focus groups, for their generosity of sharing their experience and taking the time to participate.

I would like to thank Liz Whatson, for providing all administrative guidelines and kind reminders to keep me enrolled each semester.

I would like to thank Chris O'Reilly who, with her proof reading and feedback, has supported me in the last fiddly steps of completing this dissertation.

I would also like to thank Dr Dave Roberts, who planted the seeds for this study and encouraged me to combine my two passions, Information Technology and Psychology. My thanks also go to Dr Wui-Gee Tan, who pointed me towards books for my literature review.

However, much appreciation goes to my husband, Srecko Howard, who has fully supported my decision to undertake this study and endured the stressful times when I did not think I could keep going. I am very lucky to have had his support – without that I would have never started this research. It was his believe in me being able to complete this study that got me this far.

Table of Contents

1 INTRODUCTION 1

1.1 BACKGROUND TO THE STUDY 1
1.1.1 Description of the problem 1
1.1.2 Problems with current solutions 2
1.1.3 Importance of the study 3
1.1.4 Justification for the research 3
1.2 RESEARCH APPROACH 4
1.3 BRIEF OVERVIEW OF THESIS LAYOUT 4

2 LITERATURE REVIEW 5

2.1 INTRODUCTION 5
2.2 HISTORICAL OVERVIEW OF THE THEORY AND RESEARCH LITERATURE 5
2.2.1 The Internet and information systems 5
2.2.2 The problem with unauthorised access 6
2.2.3 How organisations mitigate hacking 7
2.2.3.1 Technical solutions 7
2.2.3.1.1 Intrusion detection systems 7
2.2.3.1.1.1 How IDS works 8
2.2.3.1.1.2 Shortcomings 9
2.2.3.1.1.3 Conclusion 9
2.2.3.1.2 Intrusion prevention systems 10
2.2.3.1.2.1 How IPS works 10
2.2.3.1.2.2 Shortcomings 10
2.2.3.1.2.3 Conclusion 11
2.2.3.1.3 Summary 11
2.2.3.2 Manual solution 11
2.2.3.3 Staff involvement 11
2.2.3.4 Problems in the contemporary environment 12
2.2.3.5 Summary 12
2.3 THE THEORY AND RESEARCH LITERATURE SPECIFIC TO THE TOPIC 13
2.3.1 Source of the problem – the hacker 13
2.3.1.1 Early days 13
2.3.1.2 Hackers 14
2.3.1.3 Ethical or Grey Hackers 14
2.3.1.4 Profiling hackers 15
2.3.1.4.1 Detection and prosecution 17
2.3.1.4.2 The problem with hacker profiling 17
2.3.1.5 Security awareness 17
2.3.2 What is social engineering? 18
2.3.3 How does social engineering relate to unauthorised access? 19
2.4 CRITIQUE OF THE VALIDITY OF APPROPRIATE THEORY AND RESEARCH LITERATURE 21
2.5 SUMMARY OF WHAT IS KNOWN AND UNKNOWN ABOUT THE TOPIC 21
2.6 THE CONTRIBUTION TO THE LITERATURE 22
2.7 CHAPTER SUMMARY 23

3 RESEARCH MODEL 24

3.1 INTRODUCTION 24
3.2 THE RESEARCH MODEL 24

3.3 THE MODEL 25
3.3.1 Social engineering 25
3.3.2 System 25
3.3.2.1 Procedures manual 25
3.3.2.2 Policies 26
3.3.2.3 Procedures 26
3.3.2.4 Risk management 26
3.3.3 Users 26
3.3.4 Behavioural change 27
3.4 THE RESEARCH QUESTION AND PROPOSITIONS 27
3.5 CHAPTER SUMMARY 29

4 RESEARCH METHODOLOGY 30

4.1 INTRODUCTION 31
4.2 QUALITATIVE RESEARCH PHILOSOPHIES 31
4.3 FOCUS GROUPS 33
4.3.1 Ethical clearance 33
4.3.2 Invitation document and consent form 33
4.3.3 Purpose of a focus group 34
4.3.4 What is a focus group? 34
4.3.5 Reason for using a focus group 35
4.3.6 Role of the moderator 35
4.3.7 Preparation 36
4.3.8 How many groups and saturation level 36
4.3.9 Selection of participants 37
4.3.10 Ensuring participation 37
4.3.11 Guiding questions 38
4.4 LEXIMANCER 3.5 38
4.4.1 Processing steps 40
4.5 NVIVO 8 47
4.6 CHAPTER SUMMARY 48

5 DATA COLLECTION 50

5.1 INTRODUCTION 51
5.2 OBTAINING PERMISSION FROM DEPARTMENT HEADS 51
5.3 OBTAINING PARTICIPANTS AND COMPOSITION OF THE FOCUS GROUPS 52
5.4 ARRANGING THE VENUE 54
5.5 SECURING PARTICIPANTS 54
5.6 ENSURING PARTICIPANTS' ATTENDANCE 55
5.7 CONDUCTING THE FOCUS GROUPS 55
5.7.1 Validity 55
5.7.2 Length 55
5.7.3 Consent 56
5.7.4 Recording 56
5.7.5 Moderator 56
5.7.6 Completion 56
5.7.7 Reflections 57
5.7.8 Transcription 57
5.8 CHAPTER SUMMARY 57

6 DATA ANALYSIS 59

6.1 INTRODUCTION 60
6.2 VALIDITY 60
6.2.1 Content validity 61
6.2.2 Face validity 61
6.2.3 Saturation of themes 61
6.2.4 Descriptive validity 62
6.2.5 Interpretive validity 62
6.3 CONCEPTS 62
6.3.1 How literature was used to arrive at the concepts 62
6.3.2 Propositions 63
6.4 FOCUS GROUP ONE 64
6.4.1 Using Leximancer 3.5 64
6.4.1.1 First analysis run 65
6.4.1.2 Second analysis run 66
6.4.1.2.1 Theme 'people' 66
6.4.1.2.2 Theme 'credentials' 70
6.4.1.2.3 Theme 'password' 73
6.4.1.2.4 Theme 'systems' 74
6.4.1.2.5 Theme 'information' and concept 'data' 76
6.4.1.2.6 Summary 78
6.4.2 NVivo 8 80
6.4.2.1 Education – Change procedures 81
6.4.2.2 Education – IT competency 82
6.4.2.3 Education – Passwords 84
6.4.2.4 Education – Using encryption 85
6.4.2.5 Existing improvements 85
6.4.2.6 Existing improvements to secure practice 88
6.4.2.7 Existing policy 88
6.4.2.8 Opportunities to improve security 88
6.4.2.9 Reasons for sharing credentials – staff 89
6.4.2.10 Risk – Bluetooth 91
6.4.2.11 Risk – Copyright 91
6.4.2.12 Risk – Email content unprotected 92
6.4.2.13 Risk – Glitches 92
6.4.2.14 Risk – Graduates still have access 93
6.4.2.15 Risk – New mobile devices outside purchasing cycle 94
6.4.2.16 Risk – Not using encryption 94
6.4.2.17 Risk – Security 94
6.4.2.18 Risk – Social engineering 95
6.4.2.19 Risk – Staff sharing credentials 97
6.4.2.20 Risk – Students sharing credentials 98
6.4.2.21 Risk – Unauthorised access occurring 99
6.4.2.22 Risk – USB keys 99
6.4.2.23 Trust 100
6.4.2.24 Summary 100
6.5 FOCUS GROUP TWO 103
6.5.1 Using Leximancer 3.5 103
6.5.1.1 First analysis run 104
6.5.1.2 Second analysis run 104
6.5.1.2.1 Theme 'student' 105

6.5.1.2.2 Theme 'information' 110
6.5.1.2.3 Theme 'system' 113
6.5.1.2.4 Theme 'looking' 115
6.5.1.2.5 Theme 'induction' 116
6.5.1.2.6 Summary 118
6.5.2 NVivo 8 119
6.5.2.1 Education – Change procedures 120
6.5.2.2 Education – Induction 125
6.5.2.3 Education – IT competency 127
6.5.2.4 Education – Passwords 128
6.5.2.5 Existing improvements 129
6.5.2.6 Existing improvements to secure practice 131
6.5.2.7 Existing policy 131
6.5.2.8 Opportunities to improve security 132
6.5.2.9 Reasons for sharing credentials – staff 136
6.5.2.10 Risk – Email content unprotected 137
6.5.2.11 Risk – Incorrect access levels 139
6.5.2.12 Risk – Personal information available 141
6.5.2.13 Risk – Social engineering 142
6.5.2.14 Risk – Staff sharing credentials 145
6.5.2.15 Risk – Students sharing credentials 145
6.5.2.16 Risk – Unauthorised access occurring 146
6.5.2.17 Trust 147
6.5.2.18 Summary 148
6.6 COMBINED ANALYSIS 153
6.7 CHAPTER SUMMARY 155

7 DISCUSSION, LIMITATIONS, FUTURE RESEARCH AND CONCLUSION 156

7.1 DISCUSSION 156
7.2 LIMITATIONS 160
7.3 FUTURE RESEARCH 160
7.4 CONCLUSION 162
7.5 SUMMARY 162

8 REFERENCES 164

APPENDIX A - ETHICAL CLEARANCE 173

APPENDIX B – INVITATION DOCUMENT AND CONSENT FORM 175

Table of Figures

Figure 1: Model - minimize intrusion with propositions (P1a, P1b, P1c, P2a, P2b, and P2c) 24

Figure 2: Chapter 4 Research Methodology 30

Figure 3: Leximancer - Project Control 41

Figure 4: Leximancer - Load Data 42

Figure 5: Leximancer - Pre-process 43

Figure 6: Leximancer - Concept Seeds Identification 43

Figure 7: Leximancer - Edit Emergent Concept Seeds 44

Figure 8: Leximancer - Develop Concept Thesaurus 45

Figure 9: Leximancer - Create Compound Concepts 45

Figure 10: Leximancer - Code Concepts into Text 46

Figure 11: Leximancer - Generate Outputs 47

Figure 12: Chapter 5 Data Collection 50

Figure 13: Chapter 6 Data Analysis 59

Figure 14: Leximancer concept map - Focus group one - visible concepts 66

Figure 15: NVivo tree nodes - Focus group one 81

Figure 16: Leximancer concept map - Focus group two - visible concepts 105

Figure 17: NVivo tree nodes - Focus group two 119

Figure 18: NVivo - Free nodes for both focus groups 154

Table of Tables

Table 1: University department heads contacted 52

Table 2: Participants present at the focus groups 53

Table 3: Leximancer thematic summary from Figure 14 - Focus group one 67

Table 4: Leximancer ranked concepts - Focus group one 68

Table 5: Leximancer thematic summary - Focus group two 106

Table 6: Leximancer ranked concepts - Focus group two 107

Table 7: Combined concepts 155

Table 8: Refined combined concepts 157