

**The human element in information security: An analysis of social engineering
attacks in the greater Tshwane area of Gauteng, South Africa**

by

SHANDRÉ KIM JANSEN VAN RENSBURG

submitted in accordance with the requirements for
the degree of

DOCTOR OF LITERATURE AND PHILOSOPHY

in the subject

CRIMINOLOGY

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: PROF JH PRINSLOO

June 2017

COPYRIGHT

All rights reserved jointly by the University of South Africa (Unisa) and Ms SK Jansen van Rensburg. In terms of the **Copyright Act 98 of 1978**, no part of this material may be reproduced, be stored in any retrieval system, be transmitted in any form or be published, redistributed or screened by any means (electronic, mechanical, photocopying, recording or otherwise) without prior written permission from Unisa and Ms SK Jansen van Rensburg. However, permission to use in these ways any material in this work that is derived from other sources must be obtained from the original source. For academic and research purposes, original information may be used and referred to on condition that it is properly referenced and the sources acknowledged as such.

DECLARATION

Student Number: 49128507

I, **Shandré Kim Jansen van Rensburg**, declare that this dissertation: **“The human element in information security: An analysis of social engineering attacks in the greater Tshwane area of Gauteng, South Africa”**, submitted in accordance with the requirements for the PhD degree in Criminology, at Unisa, is my original work and all the sources cited or quoted in this research study have been indicated and acknowledged in the comprehensive list of references.

SIGNATURE:

.....

SK JANSEN VAN RENSBURG

DATE:

.....

DEDICATION

For Rachel and every little girl who has a dream.

She is clothed with strength and dignity, and she laughs without fear of the future
(Proverbs 31: 25).

ACKNOWLEDGEMENTS

I give God my Father all the honour and praise for the completion of this dissertation. Your grace is sufficient and my weakness is perfected through Your strength.

I would like to thank my beloved husband for all of your support and encouragement. Thank you for never allowing me to give up on this dream and for walking every step of this journey with me.

To my loving and supportive parents, parents-in-law, sister and brother-in-law, I would like to thank you for your continuous prayers, generosity and understanding.

To an exceptional supervisor and mentor, Professor JH Prinsloo, I thank God for the day you decided to take me under your wing. I will forever be grateful for the influence you have in my work and on my life.

I would sincerely like to thank Professor NP Dastile, my Chair of Department and mentor, for all of the support and interest that you have shown in my work and academic development.

To my fellow colleagues at the Department of Criminology and Security Science, thank you for your encouragement and guidance.

Finally, to all the research participants who took part in this study – thank you for availing your time, knowledge and experiences to this study.

Title : **The human element in information security:
An analysis of social engineering attacks in
the greater Tshwane area of Gauteng, South
Africa**

Name : Shandré Kim Jansen van Rensburg

Supervisor : Professor JH Prinsloo

Department : Criminology and Security Science
University of South Africa

Degree : Doctor of Literature and Philosophy

EXECUTIVE SUMARY

The notion of property has advanced to include abstract assets such as ideas, artistic works or information. As technology continues to expand, innovative minds increasingly discover opportunities for exploitation. Social engineering is the use of manipulative and deceptive techniques against human nature in order to access sensitive and confidential information as a means to achieve some sort of illicit action or omission of action.

This study sought to provide an exploration, description, explanation and analysis of social engineering attacks. The research was guided by a multi-inter-transdisciplinary (MIT) approach as a means to better understand, measure and explain such attacks, in order to formulate a protective strategy. Furthermore, the contextual role of social engineering attacks - within the disciplines of criminology, security science, computer science, psychology and law - was ascertained in order to design and develop a MIT social engineering prevention model.

The study was navigated by a mixed methods approach as data were collected through the use of semi-structured interviews, questionnaires and workshops. Data triangulation

was attained as data were collected in three ways to achieve mutual collaboration and detailed insight into the phenomenon under investigation.

The study generated comprehensive findings as the aim and objectives were realised. It was found that social engineering for illicit purposes is indeed occurring significantly within a South African context. Although the research respondents were aware of the behaviours associated with social engineering, the terminology and complexities associated with it confirms unfamiliarity. Furthermore, it was determined that businesses and individuals are at risk to social engineering attacks and that social engineering cannot be analysed in a single discipline; it is thus multi-inter-transdisciplinary (MIT) in nature. Finally, the need for a MIT social engineering model was identified and such a model was consequently designed and developed to assist in the protection of businesses and individuals.

The findings of the study informed the recommendations for preventative and response mechanisms outlined in the final chapter of the study. The study strongly campaigns for additional academic inquiries into social engineering to further expand the knowledge base on it.

KEY TERMS: criminological theories; hacking; impersonation; information security; multi-inter-transdisciplinary (MIT); personal information; phishing; privacy; risk; social engineering; social networks; threat; vulnerability

LIST OF ABBREVIATIONS

ATM	Automated Teller Machine
CIA	Confidentiality, Integrity, Availability
DoS	Denial of Service
ECT	Electronic Communications and Transactions Act 25 of 2002
HIV/Aids	Human Immunodeficiency Virus/Acquired Immunodeficiency Syndrome
IAA	Identification Authentication and Authorisation
IT	Information Technology
ISMS	Information Security Management System
MIT	Multi-inter-transdisciplinary
OECD	Organisation for Economic Co-operation and Development
PAIA	South African Promotion of Access to Information Act 2 of 2000
PIN	Personal Identification Number
PoPI	Protection of Personal Information Act 4 of 2013
PSN	PlayStation Network
OCED	Organisation for Economic Co-operation and Development
SARS	South African Revenue Service
SMEs	Subject Matter Experts
SMS	Short Message Service
SSA	State Security Agency
Unisa	University of South Africa

Table of Contents

LIST OF ABBREVIATIONS	viii
CHAPTER 1	1
PROBLEM STATEMENT AND OVERVIEW OF THE STUDY	1
1.1 INTRODUCTION AND PROBLEM STATEMENT	1
1.2 SOCIAL ENGINEERING IN PERSPECTIVE	3
1.3 RATIONALE OF THE STUDY	5
1.3.1 Provision of in-depth and detailed clarification and contextualisation of social engineering in the academic fields of, criminology, security science, computer science, psychology and law	5
1.3.2 Disclosure of the probable vulnerabilities, risks and consequences involved in social engineering attacks	6
1.3.3 Provision of a scientific comparative to help inform, advise and enlighten similar studies in terms of the empirical data collected qualitatively and quantitatively	8
1.3.4 Provision for informed recommendations on security policies regarding social engineering attacks.....	8
1.3.5 Investigate the development of a social engineering model that facilitates comprehensive understanding, measurement, management and prevention	9
1.4 RESEARCH AIM AND OBJECTIVES	9
1.4.1 Aim of the study	9
1.4.2 Objectives of the study.....	9
1.5 RESEARCH QUESTIONS	10
1.5.1 Primary research question	10
1.5.2 Secondary research questions	10
1.6 KEY THEORETICAL CONCEPTS	11
1.7 OUTLINE OF THE DISSERTATION	17
1.8 CONCLUSION	20

CHAPTER 2	21
FUNDAMENTAL PERSPECTIVES ON SOCIAL ENGINEERING	21
2.1 INTRODUCTION	21
2.2 INFORMATION SECURITY CULTURE	22
2.2.1 Confidentiality	23
2.2.2 Integrity	24
2.2.3 Availability	25
2.3 CONCEPTUALISATION OF SOCIAL ENGINEERING	26
2.3.1 The occurrence of social engineering	27
2.3.2 International research on social engineering	28
2.3.3 South African research on social engineering	30
2.4 SOCIAL ENGINEERING THREATS	31
2.4.1 Hidden information assets	32
2.4.2 Third-party risks	32
2.4.3 Human resources	33
2.4.4 Home workers	33
2.4.5 Social networks	34
2.5 THE WEAKEST LINKS IN INFORMATION SECURITY	34
2.5.1 The importance of human safeguarding	36
2.5.2 The shortcomings of technology	36
2.5.3 The need for security awareness	38
2.6 THE PERPETRATORS	39
2.6.1 Modus operandi	40
2.7 SOCIAL ENGINEERING ATTACKS	44
2.7.1 Social engineering attacks defined	45

2.7.2 Social engineering attack framework	46
2.7.3 Application of framework	48
2.8 THE IMPACT OF SOCIAL ENGINEERING ATTACKS	51
2.9 CONCLUSION	53
CHAPTER 3	55
A PSYCHOLOGICAL AND LEGASLATIVE PERSPECTIVE ON SOCIAL ENGINEERING	55
3.1 INTRODUCTION.....	55
3.2 SOCIAL PSYCHOLOGY CONSIDERATIONS IN SOCIAL ENGINEERING	55
3.2.1 Background and origin of social psychology	56
3.2.2 Defining social psychology	56
3.2.3 The significance of trust in social engineering	57
3.2.4 The art of persuasion.....	60
3.2.4.1 Impersonation	61
3.2.4.2 Ingratiation	61
3.2.4.3 Conformity.....	62
3.2.4.4 Diffusion of responsibility.....	63
3.2.4.5 Appeal to Maslow's hierarchy of needs.....	63
3.2.4.6 Providing a reason	63
3.2.5 Compliance mechanisms.....	64
3.2.5.1 Reciprocation	64
3.2.5.2 Commitment to consistency	65
3.2.5.3 Social proof	65
3.2.5.4 Authority	66
3.2.5.5 Scarcity	66

3.2.6 A psychological examination of a phishing attack.....	67
3.3 SOUTH AFRICAN LEGISLATION.....	69
3.3.1 Overview and background of legislation addressing information security	69
3.3.1.1 The Electronic Communications and Transactions Act	72
3.3.1.2 The Protection of Personal Information Act.....	73
3.3.1.3 The Cybercrime and Cybersecurity Bill	77
3.4 CONCLUSION	78
CHAPTER 4	80
SOCIAL ENGINEERING AND CRIMINOLOGICAL THEORISING	80
4.1 INTRODUCTION.....	80
4.2 DEDUCTIVE AND INDUCTIVE REASONING	81
4.3 CLASSICAL CRIMINOLOGY	83
4.3.1 Lifestyle exposure theory	84
4.3.2 Routine activities theory.....	86
4.3.3 Deterrence theory	89
4.4 THE POSITIVIST SCHOOL	90
4.4.1 Social process theories.....	92
4.4.2 Differential association theory.....	92
4.4.3 Neutralisation theory	96
4.5 CONCLUSION	97
CHAPTER 5	99
RESEARCH METHODOLOGY AND DESIGN.....	99
5.1 INTRODUCTION.....	99
5.2 PHILOSOPHICAL PERSPECTIVES	99
5.2.1 Ontology and epistemology	100

5.2.1.1 Objectivism.....	101
5.2.1.2 Interpretivism.....	102
5.2.1.3 Social constructionism	105
5.2.1.4 Pragmatism	105
5.3 RESEARCH METHODOLOGY	106
5.3.1 Strategies of inquiry	107
5.3.1.1 Qualitative research	107
5.3.1.2 Quantitative research	108
5.3.1.3 Mixed methods research.....	109
5.4 RESEARCH PROCEDURES	112
5.4.1 Population and sampling techniques	112
5.4.1.1 Qualitative population and sampling techniques	113
5.4.1.2 Quantitative population and sampling techniques	113
5.4.2 Unit of analysis	116
5.5 DATA COLLECTION.....	116
5.5.1 Qualitative data collection.....	116
5.5.2 Quantitative data collection.....	118
5.5.2.1 Questionnaires	118
5.6 DATA ANALYSIS AND INTERPRETATION	119
5.7 PILOT STUDY.....	121
5.8 VALIDITY, RELIABILITY AND ACCURACY OF COLLECTED INFORMATION ...	122
5.8.1 Ensuring validity.....	122
5.8.2 Ensuring reliability.....	123
5.8.3 Deductive and inductive reasoning	124
5.8.4 Data triangulation.....	124

5.9 ETHICAL CONSIDERATIONS	126
5.9.1 Informed consent	127
5.9.2 Voluntary participation	128
5.9.3 Compensation.....	128
5.9.4 No deception of participants	128
5.9.5 Privacy, anonymity and confidentiality	128
5.9.6 Publication of the findings	129
5.10 CONCLUSION	129
CHAPTER 6	131
ANALYSIS AND INTERPRETATION OF DATA: A SUBJECT MATTER EXPERT AND BUSINESS PERSPECTIVE	131
6.1 INTRODUCTION.....	131
PART I: A SUBJECT MATTER EXPERT PERSPECTIVE	132
6.2 ANALYSIS AND INTERPRETATION OF SEMI-STRUCTURED ONE-ON-ONE INTERVIEWS.....	132
6.2.1 Defining social engineering.....	132
6.2.2 Occurrence of social engineering	133
6.2.3 Vulnerable groups.....	135
6.2.4 Profile of a social engineer	136
6.2.5 Types of social engineering attacks.....	136
6.2.6 The impact of social engineering on businesses	137
6.2.7 The impact of social engineering on individuals.....	138
6.2.8 Human element in information security.....	140
6.2.9 Legislation.....	141
PART II: A BUSINESS PERSPECTIVE	142

6.3 ANALYSIS AND INTERPRETATION OF GROUP-ADMINISTERED QUESTIONNAIRES	143
SECTION A.....	145
6.4 BIOGRAPHICAL DATA.....	145
6.4.1 Biographical characteristics of the respondents (Annexure F question 1, 2, 3, 4)	145
SECTION B.....	146
6.5 EMPLOYMENT DETAILS	146
6.5.1 Occupation and time period of employment (Annexure F questions 5 and 6)	146
SECTION C.....	148
6.6 GENERAL USE OF COMMUNICATION THROUGH TECHNOLOGY.....	148
6.6.1 Technological devices, frequency of internet usage and reasons for internet usage (Annexure F questions 7, 8 and 9).....	148
6.6.2 Accessibility of personal information (Annexure F question 10).....	149
6.6.3 Accessibility of telephone number and e-mail address (Annexure F questions 11 and 12)	150
SECTION D.....	152
6.7 ACCESS TO AND VERIFICATION OF PERSONAL INFORMATION.....	152
6.7.1 Access control procedures (Annexure F question 13)	152
6.7.2 Password management procedures (Annexure F questions 14, 14.1 and 15)	154
6.7.3 Electronic signature (Annexure F question 25)	154
SECTION E	155
6.8 ACCESS CONTROL	155
6.8.1 Similarity of passwords and frequency of password modification (Annexure F questions 29 and 30)	155
6.8.2 Social networks applications (Annexure F question 31)	156

6.8.3 Accessibility of passwords (Annexure F questions 33 and 33.1)	157
6.8.4 User access revoked (Annexure F question 34)	157
SECTION F	158
6.9 SOCIAL ENGINEERING	158
6.9.1 Social engineering awareness (Annexure F questions 35 and 35.1)	158
6.9.2 Awareness of social engineering threats (Annexure F question 36)	160
6.9.3 Social engineering hypothetical scenarios (Annexure F question 37)	161
6.9.4 Motives behind social engineering attacks (Annexure F question 38)	175
6.9.5 Vulnerable groups (Annexure F question 39)	177
6.9.6 Information security culture (Annexure F questions 40 and 40.1)	177
SECTION G	178
6.10 LEGISLATION RELATED TO INFORMATION SECURITY	178
6.10.1 Awareness of South African legislation relating to information security and social engineering (Annexure F question 41)	179
6.10.2 Familiarisation with the Protection of Personal Information Act 4 of 2013 (Annexure F question 41.1)	179
6.10.3 Familiarisation with the Electronic Communications and Transactions Act 25 of 2002 (Annexure F question 41.2)	180
6.10.4 Familiarisation with the Cybercrime and Cybersecurity Bill (Annexure F question 41.3)	181
SECTION H	182
6.11 IMPACT ON INFORMATION SECURITY AWARENESS (Annexure F question 41.3)	182
6.12 CONCLUSION	183
CHAPTER 7	185
ANALYSIS AND INTERPRETATION OF DATA: AN INDIVIDUAL PERSPECTIVE ..	185

7.1 INTRODUCTION.....	185
7.2 ANALYSIS AND INTERPRETATION OF SELF-ADMINISTERED QUESTIONNAIRES	186
SECTION A.....	187
7.3 BIOGRAPHICAL DATA (Annexure I questions 1, 2, 3, and 4)	187
SECTION B.....	189
7.4 EMPLOYMENT DETAILS	189
7.4.1 Occupation (N = 112) (Annexure I question 5)	189
7.4.2 Time period of employment (Annexure I question 7)	190
SECTION C.....	190
7.5 GENERAL USE OF COMMUNICATION THROUGH TECHNOLOGY.....	190
7.5.1 Technological devices (Annexure I question 8)	191
7.5.2 Frequency of internet usage (Annexure I question 9)	192
7.5.3 Reasons for internet use (Annexure I question 10).....	193
7.5.4 Accessibility of personal information (Annexure I questions 11 and 11.1)	194
7.5.5 Accessibility of telephone number and e-mail address (Annexure I questions 12 and 13)	198
SECTION D.....	199
7.6 IDENTIFICATION AND AUTHENTICATION.....	199
7.6.1 Contact with personal information (Annexure I question 14)	199
7.6.2 Perception that personal information can be used in an attack (Annexure I question 15).....	200
7.6.3 Identification and authentication via telephone, e-mail and physical contact (Annexure I questions 16, 17 and 18).....	201
7.6.4 Electronic signature (Annexure I question 19)	202
SECTION E	203

7.7 ACCESS CONTROL	203
7.7.1 Password protection of technological devices (Annexure I question 21)	203
7.7.2 Similarity of passwords (Annexure I question 22)	204
7.7.3 Frequency of password modification (Annexure I question 23)	205
7.7.4 Websites and password control (Annexure I question 24)	206
7.7.5 Social network applications and password control (Annexure I question 25) .	207
7.7.6 Accessibility of passwords (Annexure I question 27)	207
SECTION F	208
7.8 SOCIAL ENGINEERING	208
7.8.1 Social engineering awareness (Annexure I questions 28 and 28.1)	208
7.8.2 Awareness of social engineering threats (Annexure I question 29)	211
7.8.3 Exposure to social engineering threats (Annexure I question 30).....	211
7.8.4 Technology-based social engineering (Annexure I questions 31 and 31.2)....	212
7.8.4.1 Phishing (N = 66)	213
7.8.4.2 Hoaxing (N = 49)	214
7.8.4.3 Baiting (N = 56)	215
7.8.4.4 Online scams (N = 29)	215
7.8.4.5 Botnets (N = 32)	216
7.8.5 Human-based social engineering (Annexure I questions 32 and 32.2).....	217
7.8.5.1 Impersonation (N = 18)	217
7.8.5.2 Authoritative figure (N = 8)	218
7.8.5.3 Being a third party (N = 6)	218
7.8.5.4 Desktop support (N = 11)	219
7.8.5.5 Shoulder surfing (N = 4)	219
7.8.5.6 Dumpster diving (N = 4)	220

7.8.6 Motives behind social engineering attacks (Annexure I question 33)	220
7.8.7 Frequency of threats received (Annexure I question 34)	221
7.8.8 Reporting of social engineering attacks (Annexure I question 35)	221
7.8.9 Importance of information security (Annexure I question 36)	222
SECTION G	222
7.9 LEGISLATION RELATED TO INFORMATION SECURITY	222
7.9.1 Awareness of South African legislation relating to information security and social engineering (Annexure I question 37)	223
7.9.1.1 Familiarisation with the Protection of Personal Information Act 4 of 20 (Annexure I question 37.1)	224
7.9.1.2 Familiarisation with the Electronic Communications and Transactions Act 25 of 2002 (Annexure I question 37.2)	225
7.9.1.3 Familiarisation with the Cybercrime and Cybersecurity Bill (Annexure I question 37.3)	226
SECTION H	226
7.10 IMPACT ON INFORMATION SECURITY AWARENESS (N = 96) (Annexure I question 38)	227
7.11 CONCLUSION	230
CHAPTER 8	232
ACHIEVEMENT OF AIM AND OBJECTIVES, RECOMMENDATIONS AND CONCLUSION	232
8.1 INTRODUCTION	232
8.2 MULTI-INTER-TRANSDISCIPLINARY (MIT) SOCIAL ENGINEERING PROTECTION MODEL	232
8.2.1 Scientific context of the model	233
8.2.2 The MIT social engineering protection model	234
8.2.3 Explanation of model	237

8.2.3.1 Fundamental controls.....	237
8.2.3.2 Social controls.....	239
8.2.3.3 Legislative controls.....	240
8.3 ACHIEMENT OF AIMS AND OBJECTIVES OF THE STUDY	242
8.3.1 Achievement of aim	242
8.3.2 Achievement of objectives	242
8.3.2.1 The occurrence and nature of social engineering attacks	242
8.3.2.2 The awareness of social engineering attacks and information security....	244
8.3.2.3 The state of vulnerability to social engineering attacks	245
8.3.2.4 The contextual role of social engineering attacks within the various disciplines through MIT research	247
8.3.2.5 The MIT social engineering protection model.....	248
8.4 LIMITATIONS OF THE STUDY.....	249
8.4.1 Contemporary framework of the study.....	249
8.4.2 Sample size	250
8.4.3 Self-appraisal data.....	251
8.5 RECOMMENDATIONS FOR PREVENTION OF AND RESPONSE TO SOCIAL ENGINEERING ATTACKS.....	251
8.5.1 Recommendations for businesses.....	252
8.5.1.1 Measuring vulnerability	252
8.5.1.2 Data classification	252
8.5.1.3 Awareness and targeted training.....	253
8.5.1.4 Penetration testing	257
8.5.2 Recommendations for individuals.....	259
8.6 RECOMMENDATIONS FOR FURTHER RESEARCH.....	262
8.7 CONCLUSION	262

LIST OF REFERENCES	264
ANNEXURE A: Ethical clearance certificate	282
ANNEXURE B: Informed consent form (subject matter experts).....	284
ANNEXURE C: Semi-structured interview schedule (subject matter experts).....	287
ANNEXURE D: Letter of motivation	289
ANNEXURE E: Informed consent form (group-administered questionnaire).....	292
ANNEXURE F: Group administered questionnaire	294
ANNEXURE G: Business presentation	310
ANNEXURE H: Informed consent form (self-administered questionnaire)	316
ANNEXURE I : Self-administered questionnaire	318
ANNEXURE J: Certificate of editing.....	323

LIST OF FIGURES	Page
Figure 1.1: The social engineering attack cycle	4
Figure 2.1: The social engineering attack framework	47
Figure 3.1: A psychological examination of phishing attack	68
Figure 3.2: Timeline of legislation addressing information security	71
Figure 4.1: The relationship between theory and data	82
Figure 5.1: Exploratory mixed methods design	112
Figure 5.2: Data triangulation	125
Figure 8.1: The framework of social knowledge	233
Figure 8.2: The multi-inter-transdisciplinary (MIT) social engineering model	235

LIST OF TABLES	Page
Table 7.1: Biographic characteristics of the respondents	187
Table 7.2: Contact with personal information	198
Table 7.3: Perception that personal information can be used in an attack	199

LIST OF CHARTS	Page
Chart 7.1: Technological devices used by respondents	190
Chart 7.2: Reasons for internet use	192
Chart 7.3: Accessibility of personal information	193
Chart 7.4: Accessibility of telephone number and e-mail address	197
Chart 7.5: Identification and authentication via telephone e-mail and physical contact	200
Chart 7.6: Password protection of technological devices	202
Chart 7.7: Similarity of passwords	203
Chart 7.8: Frequency of password modification	204
Chart 7.9: Websites and password control	205
Chart 7.10: Social networks applications and password control	206
Chart 7.11: Social engineering awareness	210
Chart 7.12: Technology-based social engineering	211
Chart 7.13: Human-based social engineering	216
Chart 7.14: Motives for social engineering attacks	219
Chart 7.15: Frequency of threats received	220
Chart 7.16: Awareness of South African legislation	222
Chart 7.17: Familiarisation with the Protection of Personal Information Act	223
Chart 7.18: Familiarisation with the Electronic Communications and Transactions Act	224
Chart 7.19: Familiarisation with the Cybercrime and Cybersecurity Bill	225

CHAPTER 1

PROBLEM STATEMENT AND OVERVIEW OF THE STUDY

1.1 INTRODUCTION AND PROBLEM STATEMENT

During the course of history, human beings have sought to protect and secure themselves against all types of threats to their well-being and their property. In light of technological advances, the concept of property has evolved to include not only tangible assets such as land or possessions, but also intangible belongings such as ideas, artistic works or information (Thornburgh, 2004: 133). Cyberspace facilitates online communication through the electronic medium of computer networks. The concept of cyberspace includes a universal network of inter-reliant information technology infrastructures, telecommunications networks and processing systems. Socially, users can engage in a range of activities such as playing games, exchanging ideas, sharing of information, provision of social support and conducting business (Issac, 2011: 4).

The increasing expansion of technology provides opportunities for a vast range of exploitation by inventive minds. Although technology is used for many legitimate reasons, it is also used by those who have criminal intentions (Bryant, 2008: 2). Furthermore, cybercrime brings forth issues of spatial and temporal differences, anonymity, de-individualisation, legislative discrepancies and investigative challenges. Cybercrime crosses international and legislative boundaries and is not bound to time or territory. Cyberspace provides a sense of anonymity as it affords its users a notion of secrecy and false identity. In this way de-individualisation can take place through the loss of self-accountability and self-awareness. A growing concern regarding legislative problems in cyberspace is that despite the ever-changing nature of cybercrime, legislation takes years to be drafted and enacted. Moreover, by its inherent nature, cybercrime creates various investigative challenges as it continues to evolve (Bryant, 2008: 2-9).

Information security, the protection of information systems against unauthorised access or modification (vide section 1.3; Yeh & Chang 2007: 480), relies on a threefold process,

namely identification, authentication and authorisation (IAA) (Thornburgh, 2004: 133). According to Thornburgh (2004: 133) this threefold process asks the following questions respectively: “Do I know you?”, “Are you who you say you are?” and “Are you supposed to be here?” Individuals who attempt to exploit this process through misrepresentation of themselves, or who play on the emotions of others, exploit the innate nature of human beings and are engaging in the phenomenon of social engineering.

Within the scope of information security, social engineering entails a type of attack against the human element during which the perpetrator induces the victim to release information or perform unauthorised actions (Nohlberg, 2008). In other words, as clarified by Mann (2008: 11), social engineering involves the targeting of people through deception and manipulation with the purpose of two main outcomes – direct loss of critical information and the achievement of some action intended by the attacker. Moreover, Orgill, Romney, Bailey and Orgill (2004: 177) explain that a social engineer obtains access to seemingly secure systems by retrieving private information such as usernames and passwords through deception and manipulation. This technique can be implemented as opposed to breaking into systems through traditional hacking techniques. A social engineer identifies the weakest link in a security paradigm which is controlled by logic and subject to the impulses of human nature. Furthermore, Frangopoulos (2007: 1) argues that in conjunction with human vulnerabilities and the inherent complexity of present-day information technology (IT) systems, the inevitable consequence is that information security can be compromised by social engineering attacks. Such attacks can affect the individual, group, organisation or even governments of states and can take place in both online and offline settings.

Cybernetics is known as the science of self-regulatory devices or machines (Isaac 2011). Cybernetics operates under the basic principle that regulation will occur through communication, control and feedback (Issac, 2011). Within IT boundaries, individuals often take for granted the role of cybernetics as a protection mechanism against social engineering, as it can be assumed that stricter technical controls should be a viable solution to social engineering. However, stricter technical controls cannot effectively deal with the issues surrounding human beings, their inherent nature and security. Brostoff,

Sasse and Weirich (2002: 122) state that many users know their conduct is incompliant with the current security policies of the organisation. To relieve this pressure, they may find consolation in replicating similar behaviour of fellow employees, and the belief that the regulations put in place are unrealistic.

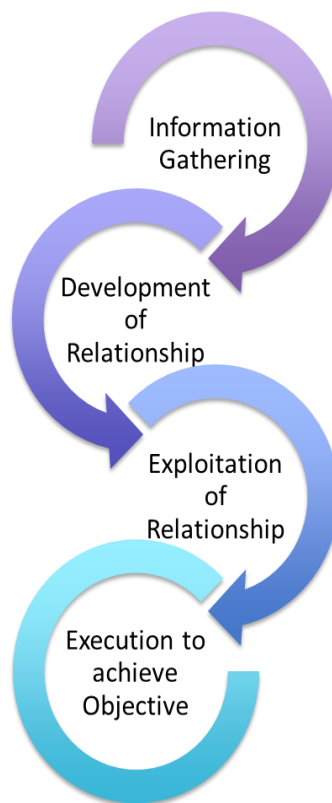
1.2 SOCIAL ENGINEERING IN PERSPECTIVE

The concept of "social engineering" originates from fields such as psychology, law, computer science, criminology and security science (Frangopoulos, 2007; Gragg, 2003; Nohlberg, 2008). In psychology, social engineering techniques are explained through "psychological triggers" (Gragg, 2003: 6). The field of law emphasises the extensive influence of social engineering on legality and social behaviour in society (Nohlberg, 2008: 3). The field of computer science also engages in social engineering as it uses and applies technical tactics and policies to sustain and consequently attempt to resolve it (Frangopoulos, 2007). Criminology and security sciences are particularly interested in social engineering and information security as these concepts cross the borders of criminality, legality and security. In essence, the notion of social engineering is multi-faceted and needs to be explored in its entirety through a multi-inter-transdisciplinary (MIT) approach.

According to Shaw (2013), these criminals use social engineering tactics, as they are comparatively easier than other attacks, and because victims innately want to trust other people and are naturally helpful. The victims of social engineering are tricked into releasing information which unknowingly can be used to attack a computer network. Alluding from the above, social engineers rely on the fact that people are not aware of the value of the information they possess and are careless about protecting it. Simplistically, social engineering preys on qualities of human nature: the desire to be helpful, the tendency to trust people, and the fear of getting into trouble (Guenther, 2001: 11). A social engineer with enough time, patience and tenacity will eventually exploit some weakness in the security of an institution. Social engineers are hacker-enablers, as the ultimate goal of the social engineer is to gain direct access to an organisation's information. The social

engineer enables a hacker to penetrate and infiltrate the system in order to extract, corrupt or delete information as well as interrupt services (Thornburgh, 2004: 134). The following illustration, as adapted from Mitnick and Simon (2002), depicts the foundational cycle of a social engineering attack.

Figure 1.1: The social engineering attack cycle



(Source: Author's own elaboration as adapted from Mitnick and Simon, 2002)

A successful social engineering attack often takes place from the inside of an organisation – this is known as “the insider threat” (Orgill et al, 2004: 178). Furthermore, in a survey conducted by the Computer Security Institute, it was found that two-thirds of social engineering attacks are assisted by an individual or individuals within the organisation (Orgill et al, 2004: 178).

Manske (2006) advocates that the risks and consequences associated with social engineering can be colossal for any organisation or individual. Although some social engineering attacks cannot always be classified as criminal, once these attacks cross the boundaries of South African legislation, such as the Protection of Personal Information Act 4 of 2013 and the Electronic Communications and Transactions Act 25 of 2002 (vide Chapter 3 section 3.3), they can be regarded as antisocial, harmful and criminal.

This study proposes to investigate, through MIT analysis, the nature and extent of social engineering attacks as well as to evaluate the current protection against such attacks. The rationale behind the study serves as a driving force of the research and thus needs to be outlined accordingly.

1.3 RATIONALE OF THE STUDY

The research study is deemed necessary because of the anticipated contributions it will make on the MIT level; that is research which is widely intertwining and which integrates and incorporates research of a multi-inter-transdisciplinary (MIT) nature (vide section 1.6). The research study will make contributions to knowledge production; it will add to empirical data collection; as well as inform policies on the enhancement of protective measures on a corporate and social level. Additionally, the study makes a contribution to South African academic literature in the fields of criminology, security science, computer science, psychology and law, as there is only evidence of similar studies internationally. The researcher developed a model of protection against social engineering attacks as an additional contribution to academic literature and organisations affected by it. Hence, the study is motivated by the following rationale:

1.3.1 Provision of in-depth and detailed clarification and contextualisation of social engineering in the academic fields of, criminology, security science, computer science, psychology and law

Social engineering is often discussed in the context of its root disciplines – namely information security and criminology. Certainly, it falls under these disciplines as it directly

interrelates with both information security and criminology; as a technology-based and human-based security breach respectively. However, the present study sought to purposively categorise social engineering under additional disciplines as it interconnects with fields of psychology, law and computer science. This was done by incorporating relevant principles from each of these disciplines into a framework in an effort to clarify and contextualise social engineering in these academic fields (vide Chapter 8, section 8.2).

The techniques and strategies involved in social engineering are largely psychological in nature (Gold 2010; Mann, 2008; Mitnick & Simon, 2002; Rogers, Seigfried & Tidke, 2006). Thus, social engineering should be explained and elaborated within this domain. Social engineering crosses paths with matters of legality when South African legislation is scrutinised. South African legislation concerning social engineering and its related matters are evaluated. The field of computer science embodies a technical perspective of social engineering, as the phenomenon is unpacked in terms of its specialised role and functionality. As a result, social engineering should not be viewed in isolation but rather within an integrated MIT perception in order to produce an in-depth and detailed clarification and contextualisation of the phenomenon. Social problems require solutions which are informed by multiple disciplines. For this reason, there is an increasing need for research which is MIT in nature (Stock & Burton, 2011: 1090).

1.3.2 Disclosure of the probable vulnerabilities, risks and consequences involved in social engineering attacks

Individuals and organisations are at risk to social engineering attacks as well as information security breaches. This study highlights these risks and vulnerabilities through the literature and empirical data collected. Individuals are at risk to the various techniques associated with social engineering attacks. Current news in South Africa confirms that social engineering is a growing risk affecting individuals (Towle, 2016). The most publically known scams are variations of phishing attacks which pretend to be well-known South African business brands in order to acquire sensitive information.

Similarly, businesses are at risk to social engineering attacks. In 2013, the Ponemon Institute, based in the United States of America (USA), conducted a global investigation into the cost of information breaches. Some of the key findings display that the root causes of the information breaches are represented as follows: malicious or criminal attacks (48%), human factors (27%) and system glitches (25%) (Ponemon Institute, 2016: 12). Overall, the following costs were recorded as being detrimental to the information breaches:

- *Direct cost:* The direct expenses needed to undertake a given activity.
- *Indirect cost:* The accumulated amount of time, effort and resources spent, which are not directly incurred.
- *Opportunity cost:* The costs that are consequential from lost business opportunities as a result of negative reputation effects after the breach has been reported and publicly revealed (Ponemon Institute, 2013).

Within a South African perspective, Burrows (2014) advises that security breaches could cost enterprises hundreds of millions of rand. The costs included in managing an incident could vary from alerting customers, legal consultation and the involvement of specialists to investigate the extent of the breach and restore or recover data and systems. In addition, business disruptions may occur and there may be a need to address reputational damage through public relations campaigns (Burrows, 2014). In a survey conducted by PricewaterhouseCoopers (South Africa) (2015), it was stated that reported security breaches have increased by 66 per cent annually since 2009 (18th Annual Global CEO Survey, 2015). Strydom (in the 18th Annual Global CEO Survey, PricewaterhouseCoopers, 2015) maintains that the actual extent of information security breaches is much higher when viewed in terms of the nature of detection and recording of the incidents. The possible vulnerabilities, risks and consequences involved in social engineering attacks need to be investigated within a South African context.

1.3.3 Provision of a scientific comparative to help inform, advise and enlighten similar studies in terms of the empirical data collected qualitatively and quantitatively

Internationally, a variety of academic empirical studies, specifically on social engineering, have been conducted (Evans, 2009; Nohlberg, 2008; Orgill et al, 2004; Slonka, 2014; Spinapolic, 2011). Fewer known studies have been conducted in South Africa, and those studies that could be found, tend to be isolated in certain disciplines (Frangopoulos, 2007) or largely theoretical (Mouton, Leenen, Malan & Venter, 2014a). Although such work on social engineering is highly informative and carries great contributory weight to any discipline, there is a need for empirical studies to help bridge this gap in research. This study was designed to address the research problem empirically through qualitative and quantitative means. Thus, this research will attempt to close the research gap by providing a scientific comparative study that may assist to inform, advise and enlighten future studies. However, it must be noted that by no means is the study's aim to generalise results or create stereotypical conclusions. On the contrary, the focus is on investigating a delimited research problem as represented by the participants and empirical examination.

1.3.4 Provision for informed recommendations on security policies regarding social engineering attacks

Policy denotes a plan or course of action within a particular institution with the purpose of influencing and determining decisions, actions and other related matters. As further explained by Whitman and Mattord (2008: 109), an information security programme of quality begins and ends with policy. Policies which are properly developed and implemented allow for operational matters to be carried out within an organisation almost flawlessly. Furthermore, Whitman and Mattord (2008: 109) observe that although information security policies are one of the least expensive means of control to effect, they are often the most difficult to implement.

Within a MIT framework, information security policies can be more practically informed

concerning social engineering as a means of prevention and intervention.

1.3.5 Investigate the development of a social engineering model that facilitates comprehensive understanding, measurement, management and prevention

Risks are analysed in terms of their probability, impact and frequency. In this way, plans can be identified and developed in order to reduce the risks (Clark, 2010: 260). Information is an asset that needs to be protected. Hence, the study endeavoured to develop a social engineering model that facilitates comprehensive understanding, measurement, management and prevention thereof, and that can serve as a standardised framework for individuals and businesses. This was achieved in Chapter 8 (vide section 8.2.3). The model integrates the disciplines of criminology, security science, computer science, psychology and law through its theoretical and empirical interpretation.

1.4 RESEARCH AIM AND OBJECTIVES

The focus of the study should clearly illustrate what forms part of the study and what is left out (Fouché & Delport, 2011: 108). The aims and objectives of the study act as a continuous guide to the researcher (Fouché & De Vos, 2011: 94).

1.4.1 Aim of the study

To explore, describe, explain and analyse social engineering attacks through a MIT approach in order to better understand, measure and explain such attacks as a means to formulate a protective strategy.

1.4.2 Objectives of the study

- To explore and describe the occurrence and nature of social engineering attacks.
- To explore and describe the awareness of social engineering attacks and information security.
- To determine the state of vulnerability to social engineering attacks among the

research respondents.

- To analyse and explain the contextual role of social engineering attacks within the various disciplines through MIT research.
- To integrate and evaluate the research results to design and apply a MIT social engineering model.

The above aim and objectives function as complementary tools when shaping and applying the research questions.

1.5 RESEARCH QUESTIONS

Ratele (2006: 540) explains that research questions are the questions that the study attempts to answer. Bless, Higson-Smith and Kagee (2006: 19) maintain that research questions should be comprehensive, precise and well-constructed. The research questions stem from a research problem and address the problem in such a way that it can be attended to in the study (Babbie & Mouton, 2001: 75). The research questions below were asked throughout the study.

1.5.1 Primary research question

- How can the description, explanation and analysis of social engineering attacks, through a MIT approach, facilitate better understanding, measurement, management and prevention of such attacks?

1.5.2 Secondary research questions

- What is the nature of social engineering?
- What is the current state of awareness of social engineering attacks?
- What is the current state of vulnerability to social engineering attacks among the research respondents?

- What is the contextual role of social engineering attacks within the various disciplines of MIT research?
- How can the design of a MIT social engineering model facilitate better understanding, measurement, management and prevention of such attacks?

For the purpose of this study, it is necessary to gain mutual understanding of the key theoretical concepts that will be used in the research study.

1.6 KEY THEORETICAL CONCEPTS

When investigating complex and inter-related phenomena such as social engineering and its related disciplines, it is necessary to clarify relevant concepts. The term concept can be defined as the words or phrases used to describe happenings about which science tries to make sense. Concept clarification facilitates mutual communication and comprehension (De Vos & Strydom, 2005: 29). The following key theoretical concepts will be defined:

▪ **Authentication**

The process of authentication involves validation that a proposed identity is indeed the person or entity requesting authorised access to a system or institution (Whitman & Mattord, 2008: 543). Maurushat (2011: 17) defines it as the process of ascertaining the identity of a computer or computer user.

▪ **Authorisation**

The process of authorisation involves the necessary permission granted to a validated person or entity by an authority to access (Whitman & Mattord, 2008: 543). Simply put, authorisation involves the discernment of whether or not the authenticated party has the right to access the information requested (Von Solms & Eloff, 2004).

- **Hacking**

Hacking refers to the exploitation of computer-mediated communications in an effort to disrupt targeted sites through various means such as e-mail bombs, web hacks, computer viruses and denial-of-service-attacks (Jewkes & Sharp, 2003: 12). Minnaar (2013: 5) explains that hacking involves the exploitation of weaknesses in a computer system or computer network which can result in a computer system's failure to perform efficiently. Additionally, hackers gain entry to a computer network without having the required authority to do so.

- **Identification**

Whitman and Mattord (2008: 543) indicate that the process of identification refers to the capacity and ability of an information system to recognise individual users.

- **Information security**

Information security entails the control of access to information assets and resources in an effort to ensure that this information is only available to authentic and authorised users. Confidentiality, integrity and availability are safeguarded when access to information assets are controlled (Casmir, 2005: 35). Furthermore, the Protection of Information Bill (Republic of South Africa B28-2008: 6), as it is not defined in the Protection of Personal Information Act, defines information security as a means of protecting information in its various forms. Moreover, in more technical terminology, information security is defined as the "preservation of confidentiality, integrity and availability of information" as well as the inclusion of "other properties such as authenticity, accountability, on-repudiation and reliability" (ISO/IEC, 17799: 2005).

- **Information security awareness**

Information security awareness entails the process of ensuring that all stakeholders recognise and comprehend their imperative role and responsibility towards securing and safeguarding the information they work with. They should be aware of possible information security threats and the countermeasures involved to prevent them (National Institute of Standards and Technology, 2000).

- **Information technology**

Information technology (IT) is the study, design, development, application and management of computer-based information systems, specifically regarding software applications and computer hardware. Essentially, IT involves the use of computers to manage and process information as well as the knowledge and skills to use computers and computer software (Van Jaarsveldt, 2010: 9). Furthermore, Bopape (2008: 3) defines IT as all of the technologies used to create, store, organise, distribute, retrieve, manipulate, interpret and transmit information to generate knowledge and improve communication.

- **Multi-inter-transdisciplinary (MIT)**

Multi-inter-transdisciplinary (MIT) encompasses research that integrates and incorporates research of various disciplines. As the term MIT is made up of certain concepts, each concept should be individually unpacked to better understand its meaning. Multidisciplinarity refers to the concurrent studying of a research topic across two or more disciplines (inclusive of sub-disciplines). Inter-disciplinarity involves the transfer of methods from one discipline to another, sometimes resulting in the development of a new discipline. Transdisciplinarity not only concerns research between and across different disciplines, but is also frequently used to describe research that sits above and beyond all disciplines (Minnaar, 2014).

Multidisciplinarity encourages researchers to share knowledge through the comparison of their research results and findings. There is no intention to create new centripetal knowledge, thus each role player is expected to contribute a specialised perspective on the topic under discussion. Interdisciplinary studies expand on

Multidisciplinarity, as these studies are interested in investigating real problems and thus need to incorporate a variety of unrelated disciplines to solve them. Transdisciplinarity is seen as the highest form of an integrated research study, as it infuses multiple disciplines with a multitude of non-academic participants (such as the general public and private entities) (Stock & Burton, 2011: 1095). Furthermore, Minnaar (2014) states that with regard to the concept of “trans”, the terms “boundary crossing” and “cross-fertilisation” are often used for the enhancement of the end result. Fundamentally, the concept of MIT has been originated to break down barriers between different disciplines. MIT research also seeks to contest “silo-isolation” and “compartmentalisation” in an effort to make research more pertinent and practical (Minnaar, 2014).

▪ **Personal information**

In order to yield an accurate, practical and current definition, personal information is defined according to the Protection of Personal Information Act (Republic of South Africa, Protection of Personal Information Act 4 of 2013: 14):

Information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to:

- (a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
- (b) information relating to the education or the medical, financial, criminal or employment history of the person;
- (c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
- (d) the biometric information of the person;
- (e) the personal opinions, views or preferences of the person;
- (f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- (g) the views or opinions of another individual about the person; and
- (h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

For the purpose of this study, personal information pertains to any of the above information.

- **Privacy**

Privacy in the context of information security denotes that all the information that is collected, used and stored belongs to the data owner and should only be used in ways known to the person providing it (Whitman & Mattord, 2008: 8).

- **Phishing**

Phishing is a means of fraudulently and deceitfully procuring personal information from a potential victim. Personal information includes matters such as passwords, identity numbers or financial details by sending e-mails that appear to be generated from trusted sources such as banks, law firms or other legitimate companies (Minnaar, 2013 99). Moreover, Kearney and Kruger (2014) argue that phishing is a type of embezzlement that makes use of social engineering techniques in order to attain personal information from its victims for the purpose of causing some kind of loss.

- **Risk**

The possibility that a threat agent will exploit some kind of weakness can be constituted as a risk (Ciampa, 2014: 228). Whitman and Mattord (2012: 596) define risk as the likelihood that something can happen.

- **Social engineer**

The term “social engineer” can be used as a noun or verb. When it is used as a noun it refers to an individual or group of individuals who execute an act of social engineering. As a verb it denotes the process of executing an act of social engineering (Mouton et al, 2014a).

- **Social engineering**

Social engineering entails a method of collecting information for an attack by exploiting weaknesses in the human element (Ciampa, 2014: 228). Whitman and Mattord (2012:

597) define social engineering as a practice of using social skills to persuade individuals to reveal valuable and personal information in order to use it against them. Furthermore, Mouton et al (2014a) denote social engineering to be the science of using social interface to coax an individual to comply with specific appeals from an attacker. For the purpose of the current study, social engineering refers to the use of manipulative and deceptive techniques against human nature. Techniques are executed as a means of accessing sensitive and confidential information for the purpose of illicit action or omission of action.

- **Social networks**

Sissing (2013: 9) explains social networks to be a web-based service which allows an individual to customise a public or semi-public online profile. The profile host and followers can participate in an assortment of online activities, including the viewing of profiles and posts, communication through chats and the playing of games. Interactions take place and relationships are often formed, which would not have been possible if not for the social network.

- **Threat**

Threat involves acts constituted as either accidental or intentional that can perpetrate various types of harm to information. In this way, a threat compromises the identification and authentication, authorisation, confidentiality and integrity of information and will eventually consequent in significant losses (National Institute of Standards and Technology, 2000). In essence, it is a type of action or omission of action that has the intention to cause harm (Ciampa, 2014: 14).

- **Vulnerability**

Vulnerability denotes a weakness in a system that can be exploited by a threat, subsequently resulting in negative effects for the system (Ciampa, 2014: 229; Frangopoulos, 2007: 226). Likewise, Garcia (2008: 303) denotes vulnerability to be that of an exploitable capability or an exploitable security weakness or deficiency in a security interest.

The key theoretical concepts discussed above form a vital part of the study. Similarly, a chapter outline should be mapped out to provide a better understanding of the content of the dissertation.

1.7 OUTLINE OF THE DISSERTATION

The researcher made use of a systematic structure to compile the chapters of the dissertation in an effort to guide the reader. The study is assembled as follows:

- **CHAPTER 1: DEFINITION OF CONCEPTS, PROBLEM STATEMENT AND OVERVIEW OF THE STUDY**

Chapter 1 provides an overview of the study by specifically focusing on the definition of concepts, problem statement and general outline of the study. This chapter serves as an introduction to the phenomenon of social engineering. The aim and objectives of the study, as well as the rationale of the study, are discussed at length. The chapter proposes to give the reader the opportunity of familiarisation and understanding regarding the nature of the research study.

- **CHAPTER 2: FUNDAMENTAL PERSPECTIVES ON SOCIAL ENGINEERING**

Chapter 2 discusses fundamental perspectives on social engineering derived from the criminology and computer science disciplines. This chapter introduces and contextualises social engineering and its related literature. It considers the significance of an information security culture, conceptualises social engineering, reviews social engineering threats as well as the weakest links in information security. The chapter also studies the perpetrators, social engineering attacks and potential impact thereof. Within this chapter, social engineering is extensively reviewed in order to provide the reader with a fundamental perspective.

- **CHAPTER 3: A PSYCHOLOGICAL AND LEGISLATIVE PERSPECTIVE ON SOCIAL ENGINEERING**

Chapter 3 provides an extensive and detailed investigation into literature pertaining to social engineering through a psychological and legislative perspective. Social engineering is contextualised into aspects of social psychology by investigating its historical nature, definition, the significance of trust and persuasion in social engineering and compliance mechanisms. In addition, a psychological example and analysis of a phishing attack are explained and analysed. With regard to legislation, South African legislation regarding social engineering and information security aspects is reviewed. This is done by providing a background of legislation addressing information security as well as unpacking specific legislation dealing with these matters, namely: the Electronic Communications and Transactions Act, the Protection of Personal Information Act and the Cybercrime and Cybersecurity Bill. In this way, the chapter seeks to broaden the reader's perception of the phenomenon of social engineering as well as its multidimensional nature.

- **CHAPTER 4: SOCIAL ENGINEERING AND CRIMINOLOGICAL THEORISING**

Chapter 4 roots the phenomenon of social engineering in criminological theories. This is done by showcasing the association between criminological theories and deductive and inductive reasoning, and embedding the phenomenon of social engineering in the Classical and Positivist school of thought. In this chapter, social engineering and its related aspects are practically applied to the following theories: lifestyle exposure theory; routine activities theory; deterrence theory; differential association theory; and neutralisation theory.

- **CHAPTER 5: RESEARCH METHODOLOGY AND DESIGN**

Chapter 5 serves as a representation of the research methodology that was implemented throughout the study. It presents the research methodology and

procedures that were used during the study. It provides an in-depth analysis of the philosophical perspectives adopted by this study, by reviewing the ontology and epistemology incorporated in the study. Furthermore, it sheds light on the research design and data collection methods incorporated in the study as well as discussing the research ethics, validity and reliability of the study. In addition, the pilot study is outlined and the ethical considerations are discussed. This chapter seeks to afford the reader the ability to successfully grasp the methods and techniques applied during the research study.

- **CHAPTER 6: ANALYSIS AND INTERPRETATION OF DATA: A SUBJECT MATTER EXPERT (SME) AND BUSINESS PERSPECTIVE**

Chapter 6 consists of two parts as it presents the analysis and interpretation of the data received from the SMEs as well as the businesses respectively. This chapter will allow for the analysis and interpretation of the data retrieved by means of the semi-structured interviews as well as the group-administered questionnaires. Part I unpacks the themes generated from the SMEs, while Part II analyses the findings obtained by contextualising them within a corporate framework.

- **CHAPTER 7: ANALYSIS AND INTERPRETATION OF DATA: AN INDIVIDUAL PERSPECTIVE**

Chapter 7 will allow for the analysis and interpretation of the data collected by means of self-administered questionnaires. This chapter systematically presents analyses and interprets the findings obtained. These findings are integrated with literature as a means of adding value and meaning to the data.

- **CHAPTER 8: ACHIEVEMENT OF AIM AND OBJECTIVES, RECOMMENDATIONS AND CONCLUSION**

Chapter 8 serves as the final chapter of the study which embodies the achievement of aims, recommendations and conclusion of the study. Here, an in-depth illustration, explanation and analysis of the integrative MIT social engineering model designed by the researcher, are promulgated. In addition, the chapter will examine the limitations of the study as well as present recommendations for future research as well as possible avenues for preventative solutions.

1.8 CONCLUSION

Social engineering is an ongoing threat to the security of computer systems due to the weaknesses inherently found in human beings. The social engineer attempts to exploit the natural desire of human beings to trust others. The impact of social engineering attacks vary widely according to the nature of the attack. Furthermore, many of these cyberattacks and data breaches are perpetrated for criminal purposes, as these acts contravene South African legislation. Through MIT analysis, this study proposes to investigate the nature and extent of social engineering attacks, as well as evaluate the current protection against such attacks by making use of qualitative and quantitative research approaches. Ultimately, the research seeks to facilitate better understanding, measurement, management and prevention of social engineering attacks.

CHAPTER 2

FUNDAMENTAL PERSPECTIVES ON SOCIAL ENGINEERING

“It doesn’t matter what technology you have - there is no technology that can protect you against human beings - forget it.” Björck (2005: 186)

2.1 INTRODUCTION

Research on information security is evolving from its technological foundations into an attempt to understand and provide explanations for the role of human behaviour in security infringements (Workman, 2011: 315). Social engineering is a term which is gradually being used regularly in current news and in various business institutions. However, this is a trend more evident in research abroad as compared to South Africa. Although social engineering is not as common among the ordinary individual, the behaviours manifested from it, such as phishing attacks or dumpster diving (vide section 2.6.1), are quite notoriously known. Regardless, very little academic research has been undertaken on the phenomenon and its related aspects. Therefore, in an effort to formulate a proactive strategy against social engineering, this research ventured to explore, describe, explain and analyse social engineering attacks through an integrated MIT approach. This chapter exhibits the fundamental perspectives on social engineering which are founded in the subject fields of criminology, security science and computer science.

The necessary discussion aims to conceptualise the construct of social engineering and social engineering attacks; to analyse and explain the context of social engineering as a systemic risk in lieu of specific threats and vulnerabilities; to analyse and explain the nature of social engineering attacks and processes; to analyse and explain the nature of perpetrators involved in social engineering and social engineering attacks as well as their modus operandi. In addition it discusses the impact of social engineering attacks and reviews international and national literature regarding social engineering.

In an effort to protect information, a culture of information security should be cultivated. With the intention of cultivating such a culture in organisations as well as for individuals, aspects of information security need to be considered.

2.2 INFORMATION SECURITY CULTURE

In the present day, information can be seen as a basic commodity, comparable to electricity, without which many organisations and individuals will fail to function effectively (Forouzan, 2014: 417; Van Niekerk & Von Solms, 2009: 476). However, information is a lot more vulnerable than other basic commodities, as it can be easily compromised. The protection of information is crucial to organisations and individuals; therefore the development of countermeasures against illicit and unauthorised access to information receives increasingly more attention (Mouton, Malan, Leenen & Venter, 2014b). As a result, the discipline of information security is growing and expanding rapidly. However, as current literature has observed, technology alone will not be enough to safeguard and protect information as the human element is often the weak link in any information security system (Frangopoulos, 2007; Furnell & Clarke, 2012; Kearney & Kruger, 2014; Mouton et al, 2014a; Mouton et al, 2014b). Within the scope of information security, social engineering entails an attack against the human element during which the perpetrator induces the victim to release information or perform unauthorised actions (Nohlberg, 2008).

Information contains key characteristics which make it desirable and valuable. The confidentiality, integrity, availability (CIA) triangle represents the three desirable traits of information (Whitman & Mattord, 2008: 6). This model has become a common security measure used to guard against information security threats encountered in the 21st century (Andress, 2014; Corey, 2015; Gibson, 2011).

2.2.1 Confidentiality

In order to ensure confidentiality, only those with appropriate privileges and a verified need may access certain information. Confidentiality is breached when unauthorised individuals or systems obtain access to confidential information (Whitman & Mattord, 2008: 6). Confidentiality is an element of privacy and thus protects data from those who are unauthorised to view it. Maintaining confidentiality obligates individuals who have access to sensitive information to know and understand the risks involved (Corey, 2015).

In any organisation, confidentiality of information pertains especially to the safeguarding of personal information about employees, customers, clients or patients. Despite the type of organisations, complications will arise when personal information is leaked or disclosed (Whitman & Mattord, 2008: 7). Information security breaches can occur either intentionally or unintentionally. For instance, confidential information could be casually discarded by an employee without taking the necessary actions to destroy it. Another example is when a hacker successfully breaks into an internal database and steals sensitive information about their client base, including identities, addresses or credit card information (Whitman & Mattord, 2008: 7). Moreover, for the individual, Andress (2014) explains that confidentiality can be breached through the loss of a laptop containing valuable information or by means of an attack penetrating a system for illicit intentions.

For the individual, confidentiality includes the maintenance of login, banking passwords, and personal information (Andress, 2014; Corey 2015). Corey (2015) advances that there are various measures used to secure confidentiality such as two-phased authentication, limiting the amount of locations used to store data and the rate in which data is transferred. Furthermore, Whitman and Mattord (2008: 6) maintain that measures such as classification of information, encryption, safe and secure document storage and operational application of security policies, as well as education and awareness of information by custodians and end users, are used to protect confidentiality.

Confidentiality is vulnerable to various attacks; some of which include snooping and traffic analysis. Snooping denotes the unauthorised access to or the interception of information. This can occur when a file, containing confidential information, is transmitted via e-mail.

An unauthorised entity may gain access to this transmission and use the content of the e-mail for own benefit. To prevent this from happening, data should be protected through encryption and encipherment (the conversion of data from plain text into code) techniques. Traffic analysis maintains that certain information can be obtained through the observing of online traffic, yielding encipherment techniques useless. By simply finding the electronic address of the sender or the receiver, the nature of the transaction can be deduced (Forouzan, 2014: 417).

2.2.2 Integrity

Information integrity is the authentic state of being whole, complete and uncontaminated. Information integrity is threatened when it is exposed to corruption, contamination, damage or destruction. Corruption can take place when information is being entered, stored or transmitted – as through many computer viruses and worms that are designed to corrupt data (Whitman & Mattord, 2008: 7). Hence, the method for detecting an integrity breach of a file system is to look for changes in the file's state as indicated by its size or by means of the file's hash value (the use of a specific algorithm that evaluates the bit in a file and then calculates a single representative number called a hash value). The file has been corrupted or compromised if the hashing algorithm varies from the original hash value (Whitman & Mattord, 2008: 7). Integrity is significant when information is perceived as the foundation for subsequent decision-making. For instance, if an attacker modified the results of a medical report, the wrong treatment plan may be prescribed, thus potentially causing a fatal outcome (Andress, 2014).

However, corruption of integrity does not only occur intentionally. Faulty programming or “noise” in the transmission channel, the path in which electrical signals pass, can cause information to be compromised (Whitman & Mattord, 2008: 7). Furthermore, Corey (2015) advocates that information should be backed up to allow for quick recovery when a data breach or loss has occurred. In addition, information backups preserve the integrity of data.

Integrity of information is vulnerable to the following types of attacks, as explained by Forouzan (2014: 418):

- *Modification:* Modification of information occurs after the attacker has gained access to the confidential data and then uses it in a way that is advantageous to the attacker. For instance, a client can send a communication to their credit card service provider to initiate a certain request. A social engineer who sees such a message can change the request to suit them. The social engineer could also delete or delay the message to harm the system.
- *Masquerading:* The impersonation of someone else and obtaining the information pertaining to that person, is known as masquerading. The social engineer may do this physically by stealing the target's bank card and password. The social engineer can also do this electronically by pretending to be the target's bank or service provider through a spoofed e-mail address or website.
- *Replaying:* Replaying involves the social engineer accessing a communication sent by the target and subsequently attempting to resend it. By means of an example, a social engineer can intercept an e-mail previously sent by this target. This e-mail can contain a request that the social engineer wants to be repeated.
- *Repudiation:* This type of attack can either occur through the sender or the receiver of a communication. Without a "read receipt" either party can deny that they have received the e-mail. Repudiation becomes particularly important when, for instance, a person buys goods from an online distributor, pays for it electronically but later the online distributor denies ever having received payment.

2.2.3 Availability

Availability of information enables authorised users access to information which is uninhibited, unobstructed and in functioning format (Whitman & Mattord, 2008: 8). Loss of availability includes, but is not limited to, various disruptions in the process of accessing data brought on by power loss or problems in an operating system (Andress, 2014). As

illustrated by a denial of service (DoS) attack, in which large amounts of traffic is sent to a site resulting in its disturbed functionality (Minnaar, 2014: 133), which then causes subsequent unavailability of information by the authorised user. Furthermore, DoS attacks are used to slow down or interrupt the service of a system. This can be done through a variety of ways: sending fake requests to a server, thus causing it to crash due to overload; deleting requests from senders, putting the sender under the impression that the receiver is not replying – or the other way around (Forouzan, 2014: 418).

The culture of information security as described above, serves as a backdrop when the concept of social engineering is unpacked.

2.3 CONCEPTUALISATION OF SOCIAL ENGINEERING

In a comprehensive study compiled by Mouton et al (2014a: 275), the most dated literature regarding social engineering was traced. Quann and Belford (1987) describe social engineering as an attempt to exploit the help desks and other support services associated with computer systems. Later on, according to Kluepfel (1989), social engineering was denoted as trickery and deceit. Furthermore, Mouton et al (2014a: 265) states that even in a current prominent hacker magazine entitled *The Hacker Quarterly*, the term “social engineering” is rarely used. A recent article in the mentioned publication explains in great detail how to perform a social engineering attack (Mouton et al, 2014a), although never referring to social engineering terminology. Davis (2007: 181) describes social engineering as an activity which involves someone who manipulates or uses deceit to gain the confidence and trust of an authorised network employee or individual by relying on the natural human inclination to trust and help others.

Mouton et al (2014a: 269) provide the following paraphrased definitions for social engineering and its related terminology. Social engineering is the science of using social interaction in order to persuade an individual or an organisation to comply with a request from an attack involving a computer-related entity. Thus, a social engineer refers to an individual or group who carries out an act of social engineering. A social engineering attack makes use of either direct or indirect communication and consists of a social

engineer, a target, a medium, a goal, one or more compliance principles and one or more techniques. Social engineering, therefore, refers to the process of retrieving valuable and often sensitive and private information through illegal means and/or the realisation of some other illegal objective by targeting individuals through deception and manipulation (cf. Mann, 2008).

A distinction can, however, be drawn between social engineering as the “art” involved in influencing people to disclose sensitive information, and the process of doing so as a social engineering attack (Mouton et al, 2014b). A social engineer ascertains the weakest link in a security paradigm, which is controlled by logic and subject to the inclinations of human nature. The hackers involved in social engineering will subsequently rely on the people within a targeted organisation to either willingly share private information, or are oblivious of the value of information they have access to, and are therefore careless about guarding it.

2.3.1 The occurrence of social engineering

As many social engineering attacks occur through electronic mediums, cybercrime statistics can be considered to document the occurrence thereof. Minnaar (2014: 128) explains that various challenges arise when attempting to verify the extent of cybercrime. Thus, determining the extent of social engineering relies on global reports compelled by cybersecurity institutions (Minnaar, 2014: 128). It is even more difficult to determine the extent of social engineering; consequently statistics in this regard depend on the findings made in cybersecurity reports. Throughout recent years, the number of detected information technology (IT) security breaches and the cost of fixing them have been increasing substantially (Trim & Upton, 2013: 22).

In a data breach investigations report conducted by an international study in 2010, the following was disclosed (cf. The Verizon Risk Team, 2010). It was revealed that 28 per cent of data breaches were successfully carried out by using social strategies such as deception, manipulation or intimidation in order to exploit the human element. These tactics were often used by combining other categories of threat such as malware

(software which is created to damage a computer system) or ransomware (software which is created to suspend access to a computer system until the requested amount of money is remunerated) perceived to be antivirus software (The Verizon Risk Team, 2010). Furthermore, the report concluded that 85 per cent of the attacks were deemed fairly easy to carry out and a staggering 96 per cent of breaches were considered to be avoidable through implemented security controls (The Verizon Risk Team, 2010). Moreover, in the 2013 data breach investigations report it was found that financial intentions were the motivating factor behind most data breaches (The Verizon Risk Team, 2013: 6-9). Verizon reports in 2015 revealed that almost 50 per cent of individuals click on phishing links, a popular social engineering technique, within an hour of receiving the e-mail (The Verizon Risk Team, 2015).

2.3.2 International research on social engineering

Social engineering has generated an increasing interest over the years as issues surrounding privacy and security are becoming more prominent. However, a comprehensive and holistic analysis portraying the illegal activities associated with the phenomenon proves difficult to find. Academic research on the topic at hand emanates from international studies (Mann, 2008; Mitnick & Simon, 2002; Nohlberg, 2008; Trim & Upton, 2013). Despite this wealth of knowledge produced by researchers, studies still seem to lack empirical insight or clear and comprehensible descriptions that focus on the impact social engineering can have on individuals or business institutions. The following discourse serves as a critical review of known literature and research studies gathered on social engineering, which are deemed influential to the study at hand.

In a detailed, comprehensive evaluation of social engineering, Mitnick and Simon (2011) provide a behind-the-scenes account of hackers, intruders and deceivers. The authors use real-life case studies to expose social engineering attacks ranging from hacking casinos out of millions of dollars to exposing the vulnerabilities of intellectual property. The book serves as an indication of the prevalence of social engineering in international narratives. The authors note social engineering as the most difficult attack, not only to

defend against but also to detect. One account provides a lengthy and detailed description of a social engineering attack (Mitnick & Simon, 2011: 222-232). The social engineer went against all security protocols by gaining physical access to restricted and “access-controlled” areas, casually retrieving confidential and sensitive information from employees regarding the company’s financial records and security breaches, deceiving unaware security personnel out of their money and managing to download classified information from the executive administrator’s computer. This detailed account signifies the astounding ease with which a social engineer can compromise the well-being of an institution.

In 2011, a study was conducted among university students in Malaysia, aimed at evaluating the awareness of social engineering, the factors causing participants to be susceptible to such attacks, as well as identification of the main types of attacks participants had been exposed to. Data were collected from 245 students through an online survey. The findings included that almost 46 per cent of students reported being exposed to social engineering attacks, while 38 per cent of those attacks were perpetrated via e-mail. Interesting to note is that only 34 per cent of students knew what the term “social engineering” actually meant (Adam, Yousif, al-Amodi & Ibrahim; 2011). The researcher took this into account when drawing up the questionnaires for the current study.

In an effort to evaluate user awareness of the social engineering threat through phishing attacks, Karakasiliotis, Furnell and Papadaki (2006) conducted an online study which yielded a total of 179 respondents from 22 different countries. The study was interesting in nature as it sought to measure how susceptible respondents were to social engineering attacks via e-mail. The respondents were tasked to differentiate between communication from legitimate institutions and illegitimate e-mails. From the responses the following was found: 37 per cent of the legitimate e-mails were identified incorrectly, and 28 per cent of the illegitimate e-mails were identified incorrectly, thus exposing the risk of social engineering among individuals. Limitations of the study included that the majority of participants were male and most were younger than 29 years of age. Also, the researchers acknowledged that 31 per cent of the respondents worked in IT-related fields,

making them less susceptible to such attacks. Moreover, this study is limited as it only reviewed one aspect of social engineering – the respondents' susceptibility to phishing attacks.

There are some social engineering surveys available online, which are aimed at social engineering awareness (<http://www.quibblo.com/quiz/10pm1kF/Social-Engineering>; <https://www.surveymonkey.com/survey-taken>). However, these online surveys lack academic insight, structure or a clear set of aims and objectives. The researcher used these surveys as a guideline to optimise the academic construct of the questionnaires used in this study.

Although international perspectives on social engineering provide direction and guidance, similar research is needed to specifically address the South African social engineering context.

2.3.3 South African research on social engineering

Little is known about social engineering from a South African standpoint, as studies on it rely on desktop research where little to no empirical research has been explored. Most reports on the phenomenon are reliant on current affairs published in news articles or citations within the IT and security professional disciplines. However, the researcher identified academic literature on the phenomenon which added value and insight to the current study.

Prominent academic literature concerning social engineering in South Africa was generated by Mouton and his associates. Though grounded in computer science perspectives, Mouton developed important research with reference to an ontological model defining the social engineering domain, the social engineering attack framework, social engineering attack detection model and ethical considerations in social engineering (Bezuidenhout, Mouton & Venter, 2010; Mouton et al, 2014a; Mouton et al, 2014b; Mouton, Malan & Venter, 2013; Mouton, Malan, Kimppa & Venter, 2015). The literature generated from the aforementioned research was not only incorporated in this current

study, but also used it as a reference point to guide the study. In addition, the known South African researchers who have done research on social engineering often include social engineering as a mere sub-theme within their body of work (*cf* Bechan, 2008; Botha, 2011; Dagada, 2014; Mashiloane, 2014; Padayachee, 2013).

In a news article published by the *Cape Times*, the sharing of personal information on social media is warned against (Anon, 2016). The article was endorsed by a representative of the South African Banking Risk Information Centre (SABRIC), who reported that banking clients should be cautious when exposing their personal details, as criminals are finding innovative ways to commit crime. The spokesperson explained that many South Africans only become aware that they were victims of crime, such as identity theft, when they apply for new credit services. Furthermore, social engineering tactics were identified as ways used to exploit victims by getting them to divulge personal information such as passwords over the telephone or through e-mail. Moreover, social engineers were noted to steal personal information through the conception of bogus competitions, directing consumers to spoofed websites as well as intercepting e-mails to gain access to personal information.

Through a critical review of both national and international literature on the topic at hand, the researcher noted general gaps in the body of work reviewed. In most cases, no fundamental theories were used as a foundational standpoint. The researcher used criminological theories as an instrument to help guide the research (*vide* chapter 5). The researcher was guided by structural and methodological processes in order to achieve the study's aim and objectives in a scientific and academic way (*vide* Chapter 1). Moreover, the research focused on the criminological foundations of social engineering by concerning itself with the associated behaviours to generate illicit activity. As this research study was guided by a specific aim and specific objectives, the researcher continuously kept these in mind in order to achieve the stated aim and objectives.

2.4 SOCIAL ENGINEERING THREATS

Social engineering threats should be identified in order to develop an operative and effective Information Security Management System (ISMS). These threats are discussed below.

2.4.1 Hidden information assets

Ritter (2015) explains that as the information age increases in momentum, information assets become more complex and diverse. In addition, the guidelines governing them escalate in number and volatility. When assessing information security risk identification, information assets play a vital role. Rather than putting emphasis on filing cabinets or electronic data, focus should be put on the knowledge and information that key people retain. Observably, this hidden information is difficult to secure as control is restricted. Consequently, key people in any institution are vulnerable to a social engineer's tactics; as such hidden information cannot be controlled by means of physical or electronic security (Mann, 2008: 16). A beneficial way to evaluate the value of hidden information assets is to determine if they contribute to new understanding, measurement or management (Mann, 2008: 16).

2.4.2 Third-party risks

Third-parties who have access to an institution's information are often underestimated. This is especially applicable to institutions that outsource aspects of their operational functions. Auditing of institutions has become a common practice in the workplace (Mann, 2008: 16). A social engineer can easily take on the identity and role of an auditor or any other third-party. In this way, the social engineer has access to any information sought after (Goodchild, 2010).

2.4.3 Human resources

The human resources department of any institution is particularly positioned to counter-manage social engineering attacks, as they are responsible for the vetting process. Organisations can be targeted through employee vulnerabilities. Although elaborate and extensive background checks can be expensive and time consuming for each new employee – the identification of certain key functions where information access is critical, could justify the need for pre-employment checks through sound human resource practices. These pre-employment checks should not be only reserved for senior members, but also for junior members such as secretaries, personal assistants or IT staff who often have access to critical and confidential information (Mann, 2008: 16). If such risks are not guarded against by means of thorough human resource policies, the organisation may fall prey to various attacks and crimes such as hacktivism, phishing or e-scams.

2.4.4 Home workers

People who work from home are suitable social engineering targets. They can be targeted directly or indirectly. Often, the security countermeasures such as antivirus systems are weaker than the countermeasures implemented at the main office. Therefore, social engineers can apply both technical and human attack techniques. This can be done through a virus attachment on an e-mail or through the exploitation of the employee's detachment from the organisation, as the employee is unfamiliar with his/her fellow colleagues. Additionally, people who work from home are indirect targets as fellow colleagues do not know them well, allowing for ease to misrepresent them in an effort to divulge information (Mann, 2008: 19). The recent case of the CryptoLocker virus, evident in South Africa and the United Kingdom (Anon, 2015), entails ransomware which holds sensitive information on computers ransom until the users have made the requested payment (Goodin, 2013). Security professionals indicate that such perpetrators are highly strategic in their choice of targets (Anon, 2015). As home workers often do not have strong computer security measures, they can be seen as seriously at risk to such attacks.

2.4.5 Social networks

Grouping individuals into clusters based on their interests, associations and likes, is known as social networking (Ciampa, 2014: 50). A social networking website is a virtual location where individuals can connect with each other and customise their profiles with pictures and details about themselves, inclusive of personal information such as contact details, values and opinions. Usually an e-mail address is the only prerequisite for creating a social network account (Hill, 2010). The number of subscribers to social networking sites has grown tremendously (Gross & Acquisti, 2005: 71). This is further supported with global statistics noting that in 2015, the number of social network users worldwide was estimated to be 1.96 billion. Considering the rate at which user subscription to social networking sites is increasing, it is envisioned that by 2018 there will be 2.44 billion social networking users (The Statistics Portal, 2016). Moreover, users' lives are evolving around social network sites, as networking is incorporated into their daily lives for both social and professional purposes (Boyd & Ellison, 2008: 210).

Individuals and businesses are at risk and are vulnerable to being socially engineered through social networks. Social networks are often the gateway which social engineers use to target their victims. Robinson (2015) reports that researchers have uncovered a network of more than two dozen social networking profiles that were intentionally created to compromise the security of organisations involved in telecommunications, defence and government. Furthermore, Robinson (2015) indicates that although social network users are aware of stereotypical phishing scams, they tend to be less likely to be apprehensive of prospective business contacts.

2.5 THE WEAKEST LINKS IN INFORMATION SECURITY

The social engineering risk is frequently ignored, as organisations often place all of their trust in IT security hardware and software vendors. The misconception that technical issues should be the sole responsibility of technical people, such as IT personnel, often extends security vulnerabilities as it does not address an organisation's greatest weakness – people (Mann, 2008: 21). Gonzalez (2002) argues that security is reliant on

technology and people. Even though technological advances contribute to making security products increasingly impressive, the human factors involved remain the downfall of information security.

Inherently, people long for a feeling of absolute safety, resulting in them settling for a false sense of security (Mitnick & Simon, 2002: 3). Consider the typical middle class home owner in South Africa. In an effort to achieve maximum security, he has attained access control at the security gate of his complex, a slam lock security gate guarding the front door of his house and burglar bars protecting each window. The owner now feels at ease knowing that he has increased his family's safety against possible intrusions. However, these means of physical security measures do not protect the home owner from an intruder who manages to crack the code to open the garage door. Hence, vulnerability to security breaches remains a concern. Just as the security-conscious home owner believes in this false sense of security, so too do many IT professionals, in that they too are deluded by a misconception that their companies are immune to attacks, as they have developed and implemented robust security systems. Consequently, as maintained by Mitnick and Simon (2002: 3), the human factor is security's weakest link.

Security is often an illusion; an illusion which can be fuelled by gullibility, naivety and/or ignorance. Social engineering practices are successful when people are unaware or uninformed of good security practices. In this way, it can be maintained that security is not a product but rather a process. In addition, security is not only a technology problem but it is a human and management problem (Mitnick & Simon, 2002: 4). Furthermore, anyone who presumes that security technology products alone offer invulnerable security is settling for the illusion of security. As IT professionals continue to produce improved security technologies, attackers will increasingly rely on exploiting the human factor, because technical vulnerabilities will become progressively more difficult to overcome. As Mann (2008: 21) maintains, human beings are complex, inadequately understood and thus they present a greater challenge in addressing security vulnerabilities.

2.5.1 The importance of human safeguarding

Most security practitioners will agree that an institution's security is only as strong as its weakest link (Arce & Levy, 2003: 72). Although people denote a significant function in obtaining security, they are often the point of failure. It is imperative to design systems and implement policies to assist people in ensuring their security systems, as matters of security ultimately impact all aspects of society regardless of age, creed, gender, individual or organisation (Furnell & Clarke, 2012: 983). Each employee has different roles and functions within an institution, which vary from those of their fellow colleagues (Arce & Levy, 2003: 74). Furthermore, Furnell and Clarke (2012: 984) argue that people-focused safeguards or human safeguarding, such as the creation and endorsement of policy, security awareness and education campaigns and the utilisation of security technology, should be emphasised.

Empirical research has shown that user actions, whether intentional or accidental, are often positioned closely alongside the more popular threats of malware or hacker attacks. The human element matters more now than it used to in the past, because there are various devices and services available and the extent of online connectivity has expanded, making it more of a need than a want. Consequently, individual users are faced with numerous security-related choices to make and more sensitive information to protect. Meanwhile, end-users' systems are being actively targeted with a greater magnitude of threats. Hence, today's users are by default more exposed to security breaches than their predecessors were. For these reasons a broader societal understanding of human safeguarding, security and related threats should be promoted by fostering an operative information security culture (Furnell & Clarke, 2012: 984).

2.5.2 The shortcomings of technology

Furnell and Clarke (2012: 985) propose that the evolution of security technology and the usage thereof directly overlaps with the human element. As technology advances and evolves, more pressure, responsibility and accountability are being put on the user. For instance, more and more web-based services are requiring two-phased authentication such as e-mail accounts or online banking. The traditional entry of the user's e-mail

address or user name as well as password does not suffice, but an additional password is sent via SMS, which needs to be entered to prove verification and gain access to the service. While this enhances security, it adds extra work to the user which involves time and effort, requiring them to have their mobile phone with them in order to log on (Furnell & Clarke, 2012: 985). Moreover, Kearney and Kruger (2014) emphasise the shortcomings of technology and maintain that technology cannot solely address information security risks, as attitudes and user perceptions play a crucial role.

In an effort to minimise risks and to ensure effective information security, many organisations depend on technology-based solutions (PricewaterhouseCoopers, 2015). Although it can be noted that these types of resolutions assist in refining information security, depending on them entirely is hardly enough to eradicate the risk (Bulgurucu, Cavusoglu & Benbasat, 2010; Dhillon & Backhouse 2001; Siponen 2005). Technology has progressed extensively in terms of antivirus protection and subsequently requires increased usability to enable users to utilise it effectively (Furnell & Clarke, 2012: 985). Furthermore, the complexity of technological protection systems are often concealed in simplicity, as “Internet Security Suites” are made up of personal firewalls, anti-spam, anti-phishing, anti-spyware as well as intrusion detection systems – leaving the user with the challenge of understanding and managing these protective measures. For instance, most antivirus programs are likely to present themselves as a challenge to the average user in terms of its security complexity. Consequently, the user may just ignore the prompts made by the antivirus in its entirety. This illustrates the shortcomings of technology, despite (or perhaps because of) technological advances.

The burden on the user has increased as threats and control of technological security systems have advanced. Few controls are entirely automated while the average user is likely to face increasingly varied interactions with security. For example, former security features may have warranted decisions such as deleting or isolating a virus. Today, modern security software can offer a range of complex scenarios in which the user is prompted to offer a suitable response. The proposed safeguard is undermined when unprepared users are expected to make these decisions (Furnell & Clarke, 2012: 986).

Furnell and Clarke (2012: 986) propose possible solutions to overcome end-user security accountability. The use of automation should be increased. Information should be presented to the user in terminology which they can understand and can relate to. Training should be provided to users so that they can be better equipped to deal with security related issues. In this manner some shortcomings of technology may be addressed.

2.5.3 The need for security awareness

Furnell and Clarke (2012: 984) maintain that the need for security awareness has had a significant and continuous shift in responsibility to the end user. The threats of information security breaches are too extensive for technology to resolve by itself. Additionally, these threats cohabit in too many contexts to be able to rely on one form of guardianship or protection mechanism. Peltier (2001: 4) maintains that the roles and responsibilities of end users are dependent on their current stance towards controls. As a result many users function in a society where they are inadequately equipped to operate effectively, because they lack security awareness as well as the understanding of technology and potential security breaches. In the meantime the same users find themselves still relying on the security technology that previous generations used such as firewalls, backup systems or Intrusion Detection Systems (IDS). Although these technologies originated in the field of IT, they have progressively surfaced to be the responsibility of the end user. Consequently, there is a need for security awareness to be raised (Furnell & Clarke, 2012: 984).

End users within an institution run the risk of encountering personal harm as a result of the threats they are exposed to such as through malware or phishing techniques. Additionally, without proper training and security awareness, they can amplify the threat for other people, for instance if a user gets infected by malware, then other users as well as organisations may be affected if the system initiates spam mails or DoS attacks (Furnell & Clarke, 2012: 985).

Regrettably, awareness and continuous training strategies have lagged behind technology-orientated safeguards and protection mechanisms. Interesting to note is that research extracted from the 2010/2011 CSI's Annual Computer Crime and Security Survey (Computer Security Institute 2011) indicates that two thirds of the respondents reported that they spend five per cent or less of their security budget on awareness programmes, while a large majority of the respondents reported spending 10 per cent of the same budget on security technologies (Richardson, 2010). Although technology-based protection investments are useful and beneficial, they can only secure protection to a certain extent (Furnell & Clarke, 2012: 984; Krombholz, Hobel, Huber & Weippl, 2014: 119); more so when the need for security awareness is also addressed.

2.6 THE PERPETRATORS

Trim and Upton (2013: 27) provide a taxonomy of hackers involved in social engineering attacks. According to the authors (Trim & Upton, 2013: 27), official hackers can function as penetration testers, security companies or network managers. Their skill set is wide and high and they can be regarded as experts in the field of information security. As their motivation is to test an organisation's vulnerability to information security breaches, the impact of such an attack will often lead to security enhancement. Criminal hackers operate with criminal intent and their skills range from medium to high. Their motivation is to carry out criminal activity such as theft or fraud. The impact of their endeavours is serious as it has financial implications. Hackers interested in commercial espionage are often represented as rivals, sales forces or recruiters. Their abilities range from low to high and they endeavour to obtain business information which could be beneficial to their own interests. Personal hackers are often script kiddies or disgruntled employees. Their skills vary as they seek personal satisfaction. The impact of such attacks serves as a mere annoyance and is quickly exposed. However, often such attacks yield unplanned social or financial implications. Political and social activists' activity varies but can be exceptionally sophisticated if highly motivated. Their motivation is often pre-empted by a single issue and is more likely to cause embarrassment to an organisation than financial

harm. The state hacker is concerned with issues of cyber-warfare, political and economic intelligence gathering. Such hackers intend causing harm through sabotage in times of strife or to give national organisations some type of commercial edge (cf. Trim & Upton, 2013: 27).

Mitnick and Simon (2002: 264) maintain that there are four types of information that social engineers frequently seek to attain. Confidential information is of utmost importance to the social engineer as it may contain trade secrets, financial data or strategic plans. Such information is rarely disclosed extensively within an organisation. Private information refers to personal information about specific individuals which could potentially cause financial or reputational harm to an organisation if leaked. Moreover, the social engineer often seeks internal information which relies on general operational knowledge regarding how an organisation functions. This is the most vulnerable category of information desired by a social engineer, as often people do not understand the sensitivity of some types of information. Lastly, social engineers seek public information which is freely disclosed and easily attainable. This assists them in the gathering of information to carry out a social engineering attack.

2.6.1 Modus operandi

Social engineering attacks can be divided into two categories, namely human-based and technology-based (Guenther, 2001: 20). As outlined by Shaw (2013), the following provides some examples of the most popular methods used by social engineers.

Human-based social engineering needs interaction with humans; it means person-to-person contact and then retrieving the desired information.

- *Impersonation:* Impersonation within social engineering entails constructing a fabricated character and then playing out the role of this fictitious character on a victim. For instance, the social engineer can pretend to be a chief financial officer of a particular organisation who requests the accountant to authorise a payment (vide section 3.2.4.1) (Ciampa, 2014: 45).

- *Authoritative figure:* The attacker pretends to be a very important person or high-level manager who has the authority to use computer systems or files. Most of the time, low-level employees do not ask any questions of someone who appears to be in this position. This attack would require detailed preparation and research by the social engineer to be successful.
- *Being a third party:* The social engineer pretends to have permission from an authorised person to use the computer system. It works when the authorised person is unavailable for some time.
- *Desktop support:* Requesting technical support for assistance is a classic social engineering technique. Help desk and technical support personnel are trained to help users, which makes them good prey.
- *Shoulder surfing:* This is the technique of gathering information by watching over a person's shoulder. Shoulder surfing can occur in various public locations where personal identification is requested from an individual. This could happen while entering a personal identification number (PIN) at an automated teller machine (ATM), inserting a PIN onto debit or credit card facilities or entering a password on a device such as a laptop, mobile phone or tablet. Tailgating is seen as an extension of shoulder surfing. Good security measures include installing specialised doors to monitor access control. However, often these systems cannot monitor the number of people who can enter. A tailgater can easily ask an authorised member to kindly hold the door for him or her. Often, good etiquette triumphs over good security practices (Ciampa, 2014: 49).
- *Dumpster diving:* This involves looking in the dustbin for information written on pieces of paper or computer printouts. Often items disposed of appear to be useless but a social engineer can use them to their benefit. Items of this nature include calendars, USB flash drives, memos, organisational layouts, phone directories, policy and system manuals. Although dumpster diving is prevalent in attacks against organisations – individuals are also vulnerable to such attacks when items containing personal

information (for instance bank statements, receipts or credit card information) are not properly discarded (Ciampa, 2014: 48).

Technology-based social engineering uses computer software that attempts to retrieve the desired information.

- *Phishing*: This involves false e-mails, chats, or websites designed to impersonate real systems with the goal of capturing sensitive data. This scam can also manifest into various forms such as vishing, spear phishing, whaling and pharming. Vishing entails a fake phone call where an attacker poses as a representative such as a bank consultant. The attacker grooms the victim to reveal financial information. Phishing involves sending out thousands of generic e-mails to unsuspecting victims, whereas spear phishing targets specific users. These communications are tailored for the intended recipients by including their names and personal information, making the communication appear authentic. The volume of spear phishing attacks is very low, thus making it difficult to detect. Whaling is a type of spear phishing attack that specifically targets “big fish” who are extremely wealthy. The attackers invest a lot of time and effort into finely tuning these messages to maximise the success rate. Pharming attacks automatically re-direct the user to a bogus website (Ciampa, 2014: 47).
- *Hoaxing*: A hoax disguises itself as a warning to the user. The hoax will report that there is a virus circulating through the internet and that specific files should be deleted or security settings should be changed. However, adhering to such requests could afford the social engineer an opportunity to compromise the systems (Ciampa, 2014: 47).
- *Baiting*: Baiting involves dangling something the person may want, to entice the individual to take an action the criminal desires. Amongst others, it can be in the form of a music or movie download on a peer-to-peer site or it can be a USB flash drive with a company logo labelled “Executive Salary Summary” left out in the open for the

person to find. Then, once the device is used or downloaded, the person or company's computer is infected with malicious software allowing the criminal to advance into your system.

- *Online scams:* E-mails sent by scammers may have attachments that include malicious code inside the attachment. Those attachments can include key loggers to capture users' passwords, viruses, trojans, or worms. Sometimes pop-up windows can also be used in social engineering attacks. Pop-up windows that advertise special offers may tempt users to unintentionally install malicious software. Online scams have the ability to become more customised with the incorporation of behavioural targeting techniques. Behavioural targeting uses online information such as clicks, searches and social networking websites, online shopping tendencies, to select ads that marketers think will appeal to you based on personalised online behaviour. Behavioural targeting observes online actions and subsequently makes predictions on future behaviour (Reczek, Summers & Smith, 2016). Online scams can now become more credible when social engineers are aware of their targets' interests and propensities.
- *Botnets:* A network of infected computers which are remotely controlled as a group without the knowledge of the owner, are known as botnets. Botnets are controlled by a bot master and many bots are classified as malware. Botnets are used to create spam or DoS attacks (Maurushat, 2011: 18).
- *Identity theft:* A social engineer can engage in fraudulent activity when they use stolen personal information for financial gain. Stolen information can be used to open up credit accounts, lease property or obtain loans. The victim is charged for these purchases and often endures reputational damage regarding their financial history (Ciampa, 2014: 49).

As adapted from Harley (1998), Mitnick and Simon (2002), Whitaker, Evans and Voth (2009) as well as Trim and Upton (2013: 25), the following serve as common social engineering practices.

- *Simple requests*: Naturally, people tend to provide information if it is requested nicely. Information obtained can be further extended if one individual is not bombarded with too many questions.
- *Obtaining trust*: Perpetrators try to develop rapport and a foundation of trust with the target.
- *Provide solutions*: Often, an issue or possible problem will be created or exploited in order for the social engineer to offer solutions. This approach requires some background information about the target.
- *Request assistance*: Social engineers play on the feelings of their targets by making up plausible stories in order to receive sympathy.
- *Use of guilt or intimidation*: The social engineer puts pressure on employees by imposing feelings of guilt or intimidation on them. For instance, the social engineer will pretend to be an important client.
- *Target entry-level employees*: New, temporary or junior staff members are more vulnerable to techniques of intimidation as they are not yet well trained or familiar with security protocol, as opposed to more experienced staff members. Furthermore, they are less likely to know fellow colleagues personally or recognise their voices and tendencies – allowing for easier impersonation.
- *Incident distraction*: By creating an incident, such as a bomb threat, people within an organisation will be pressurised, disrupted and distracted. This incident will allow the social engineer an opportunity to exploit the situation as an employee will most likely provide any information requested in order to normalise the situation at hand.

2.7 SOCIAL ENGINEERING ATTACKS

Mouton et al (2014b) distinguish between different social engineering attacks by dividing them into categories and sub-categories, direct and indirect communication. The former category (direct communication) is further divided into two sub-categories, namely bidirectional and unidirectional communication. Additionally, a social engineering attack

includes the following elements: a social engineer; a target; one or various compliance principles and techniques; as well as a medium and a goal. A social engineering attack framework adds to the foundational components of social engineering, as it considers temporal data such as flow and time (Mouton et al, 2014b).

2.7.1 Social engineering attacks defined

Kevin Mitnick, a convicted hacker and now well-known author and computer consultant, developed a foundational social engineering attack cycle (see figure 2.1), published in his book, *The art of deception: Controlling the human element of security* (Mitnick & Simon, 2002). The model contains four key phases, namely research; developing rapport and trust; exploiting trust; and utilising information. Research involves the gathering of as much information as possible about the target. Development of rapport and trust comprises the following: insider information; misrepresenting an identity; referring to those known by the target; expressing a need for assistance; or taking on an authoritative role. A target will more likely disclose requested information once trust has been established. Once trust is gained, the attacker will exploit the trust in order to achieve the desired information or action. The final phase is achieved when the outcome of the previous phase is utilised to reach the goal of the attack (Mitnick & Simon, 2002).

Although, Mouton et al (2014a: 275) argue that any taxonomy of social engineering will be limited in nature, the authors have developed an ontological model to explain a social engineering attack. Ontology allows for the separation of domain knowledge from operational knowledge as it involves the naming and defining of types, properties and interrelationships of entities (Mouton et al, 2014a: 276).

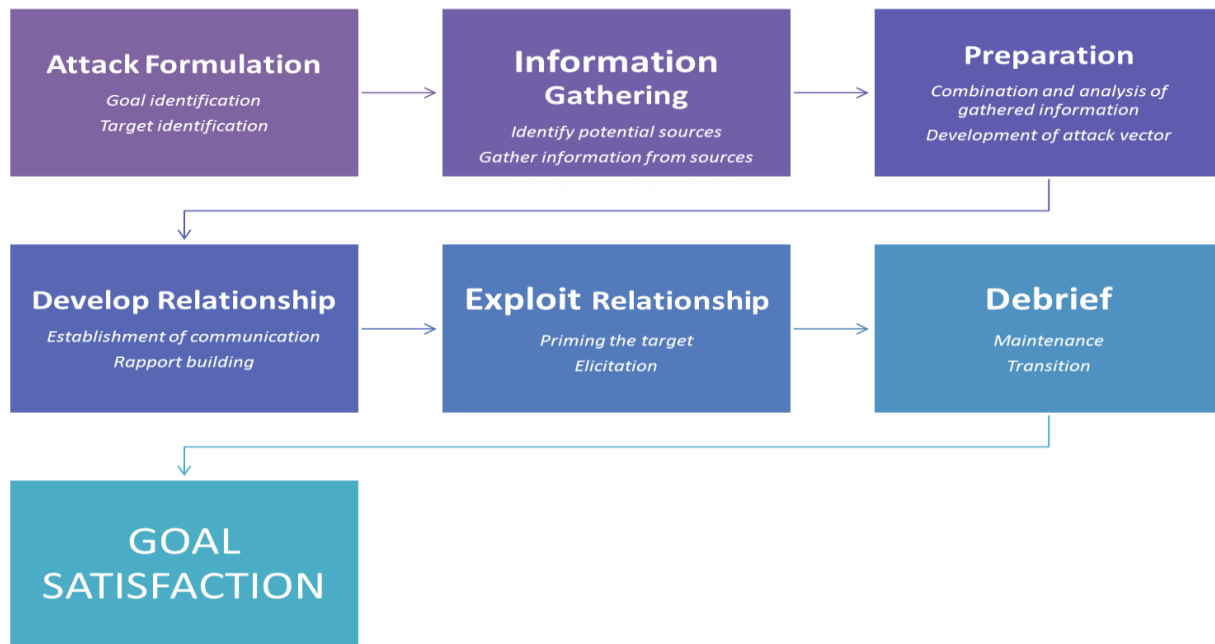
As mentioned earlier, social engineering attacks can be divided into two categories. A direct attack involves a direct conversation between two or more people – either one-sided or two-sided. Bidirectional (two-sided) communication is when two or more people take part in the conversation. For instance, an impersonation attack will involve communication between the social engineer and the target as the social engineer impersonates a fellow colleague in order to gain access to something which the target

has access to. Unidirectional communication is a one-sided conversation. The social engineer communicates with the target, but the target is unable to communicate back with the social engineer. This can be done through bulk e-mails or short message service (SMS). An example of this attack would be an e-mail phishing attack sent from the attacker to the target. An indirect attack is carried out when third party media are used as a way of communicating, be it through physical media such as flash drives, pamphlets or other forums such as web pages (Mouton et al, 2014a: 271).

2.7.2 Social engineering attack framework

Mouton et al (2014b) propose an extension of the original social engineering attack cycle developed by Mitnick and Simon (2002). The following figure depicts the social engineering attack framework as designed by Mouton et al (2014b).

Figure 2.1: The social engineering attack framework



(Source: Author's own elaboration as adapted from Mouton et al, 2014b)

The initial step involves preparation, because the goal of the attack as well as the identification of the best possible target to assist in reaching the goal should be established. Once these factors have been established, information gathering can take place in order to develop an attack formulation. Mouton et al (2014b) suggest that Mitnick and Simon's development of the rapport and trust phase first needs to meet the prerequisites of inaugurating communication and then the building of rapport will follow. The next phase (the exploitation phase), involves priming of the target to determine their emotional state, thus allowing information to be elicited. Furthermore, Mouton et al (2014b) add an additional phase to the cycle, as debriefing needs to take place. The target needs to be redirected to their original emotional state to avoid further repercussions. The target should feel at peace and pleased about giving unauthorised information instead of concerned or guilty about it. Mouton et al (2014b) argue that Mitnick and Simon's final phase of utilising information should not be included in the social engineering framework. Alternatively, within the debriefing phase either maintenance of the attack will take place if more information is needed, or transition will occur to achieve goal satisfaction.

2.7.3 Application of the social engineering framework

Ransomware is a growing threat to individuals and organisations (Correa, 2016). Ransomware is malicious software which is created to infect computer systems by encrypting the files and then holding the required decryption code for ransom until the victim makes a specified payment. It is estimated that in 2015, this method of extortion was used to successfully retrieve over \$400 million from targeted victims (CyberArk, 2016).

The following serves as a hypothetical example of typical locky ransomware attack in which the social engineering attack framework can be applied practically (Lee, Moon & Park, 2016: 1825). In a social engineering attack against targeted individuals, an attachment containing ransomware in a Microsoft Word document is sent via e-mail to the unsuspecting targets. The legitimately designed e-mails masquerade as an invoice issued to the recipients for services rendered. The targets immediately open the attachment while the virus starts running in the background without the target's knowledge. The files on the computer system are subsequently being encrypted, thus, rendering the victims unable to access any of the documents. The final stage involves changing the target's wallpaper into a message directing him or her to a website explaining what encryption is and how to obtain the decryption key. The message will refer the target to a link where an amount of money is requested in order to retrieve the target's documents (Lee et al, 2016: 1825). The social engineering attack framework can be applied to this hypothetical example, created by the researcher, as explained below:

The attack phase: The following constitute important features of the social engineering attack based on the work done by Mouton et al (2014b) :

- *Communication:* The social engineering attack is using indirect communication through third party mediums as the social engineer does not need to directly communicate with the target.

- *Social engineer:* The social engineer could be an individual or group of individuals.
- *Target:* The target is an individual; in this case it is the e-mail recipient.
- *Medium:* The medium is the e-mail appearing to be an invoice issued.
- *Goal:* The goal of the attack is to infect the computer system with ransomware in order to extort financial gain from the target.
- *Compliance principles:* Social compliance and curiosity is used to gain compliance.
- *Technique:* The technique that is used is ransomware.

Step 1: Attack formulation

- *Goal identification:* The goal of the attack is to infect as many computer systems as possible with ransomware in order to extort financial gain from unsuspecting targets.
- *Target identification:* The target of the attack is any person who receives an e-mail containing the ransomware.

Step 2: Information gathering

- *Identify potential sources:* Research was done on specific individuals who might fall prey to such attacks. These targets would need to regard the files on their computer systems as indispensable and also be able to afford to pay the specified ransomware.
- *Gather information from sources:* Information was gathered by observing and replicating valid e-mails containing invoices.
- *Assess gathered information:* This involves the establishment of reasonable and credible e-mails which are specific to what the target may require.

Step 3: Preparation

- *Combination and analysis of gathered information:* The e-mail, ransomware and subsequent link should be designed while a list of the intended targets should be orchestrated.
- *Development of an attack:* The e-mail, ransomware and link to the website containing the payment instructions should be developed. Subsequently, the money will be paid into the attacker's account.

Step 4: Develop relationship

- *Establishment of communication:* The action of sending the e-mail to the target establishes communication.
- *Rapport building:* The e-mail should be customised for the intended targets so that they will not doubt its legitimacy.

Step 5: Exploit relationship

- *Priming the target:* The e-mail should be convincing enough so that the e-mail recipient will take it seriously and open the attachment. The target should feel pressured enough due to social compliance to do the right thing and pay the invoice or curious enough to want to discover what the invoice was issued for.
- *Elicitation:* A website hyperlink must be installed on the computer system. Upon clicking on the link, the target will decide whether or not to succumb to the extortion.

Step 6: Debrief

- *Maintenance:* The e-mail should be designed in such a way that the target does not feel threatened or raise any alarm.

- *Transition:* The social engineer can use this opportunity to gain compliance from the target by receiving payment and can thus transition to the “goal satisfaction” step.
- *Goal satisfaction:* The social engineer has successfully achieved the initial goal of financial gain.

2.8 THE IMPACT OF SOCIAL ENGINEERING ATTACKS

Manske (2006) advocates that the risks and consequences associated with social engineering can be colossal for any organisation and individual. As social engineering targets, people are the most vulnerable component of information security, and the attacker is able to bypass protection measures (both physical and technological) put in place, thus nullifying any security investments made. Moreover, Manske (2006) goes on to explain that once a computer system has been compromised, IT costs drastically increase; computer systems must be inspected, repaired and re-secured, backups need to be reinstalled and the attack must be followed up through consultation with security and legal experts. Additionally, authorities may have to be involved to conduct forensic audits resulting in the disturbance of operational functions by end-users. These combined factors will result in low staff morale, overtime and poor turnovers.

In a study conducted by Check Point Software Technologies LTD (2011) the risk of social engineering on information security was investigated. The international survey consisted of information obtained from over 850 IT and security specialists from a variety of fields such as financial, industrial, defence, retail, healthcare and education. The main findings from the report are outlined below:

- *The social engineering threat is real:* The survey found that more than 80 per cent of the specialists surveyed were either aware or highly aware of the possible risks and dangers associated with social engineering. Moreover, almost 50 per cent of the

institutions surveyed reported that they had been victims of social engineering more than 25 times between the years 2009 and 2010.

- *Common types of social engineering techniques:* Phishing, social networking sites (where people share or reveal professional and personal information) and insecure mobile sites were listed as the most common types of social engineering techniques present.
- *Social engineering attacks cause catastrophic losses:* The study's research respondents indicated that each social engineering incident could cost the institution between \$25 000 to over \$100 000. These expenses include costs linked to business interruptions, client expenditures, profit loss and brand damage.
- *Primary motivation of social engineering attacks:* Monetary gain was listed as the most common reason for social engineering attacks. Other motives include access to trademarked information, or competitive advantage revenge.
- *People identified as most susceptible to social engineering attacks:* The survey participants cited new employees as those most at risk to social engineering attacks. This was followed by contract workers, executive support-staff, human resources, business leaders and IT employees.
- *Training and awareness:* The study revealed that more than 30 per cent of the institutions surveyed did not have training or security policies put into effect as a protective measure against social engineering attacks.

According to the Global Economic Crime Survey (2016: 18) the level of impact of cybercrime includes reputational damage, legal and enforcement expenses, service disruption, theft or loss of personal information, regulatory cost and actual financial loss. Furthermore, the survey indicates that all industries are at risk to some form of cybercrime breach.

Thornburgh (2004: 134) proposes that any single event, whereby a social engineer retrieves what he or she sets out to do, can be considered as a successful attack as any information gathered by the attacker increases the possibility of successful penetration.

The impact of social engineering attacks vary widely according to the nature of the attack. Large corporations, private industries, businesses, government agencies as well as individuals and children are at risk to information security breaches.

These security breaches also have great financial implications as money invested in technical protection is nullified (Conteh & Royer, 2016: 5; Thornburgh, 2004: 135). Further consequences of successful attacks can include: loss of public and clientele confidence; negative publicity; and fines and other regulatory consequences such as lawsuits (Conteh & Royer, 2016: 6; Guenther, 2001: 49; Manske, 2006). Lucks (2004: 13) maintains that as technology advances, society is becoming increasingly reliant on computers and the internet. The sphere of cyberspace facilitates information to be transferred, leaving millions of people vulnerable to information security breaches.

2.9 CONCLUSION

This chapter discussed fundamental perspectives on social engineering. During the course of this review, it has been emphasised that the risks associated with social engineering can be enormous for any organisation and targeted individual, with far-reaching direct and indirect consequences. The extent of the threat of social engineering attacks is equally far-reaching and non-selective. Large corporations, private industries, businesses, government agencies as well as individuals are at risk to information security breaches. Society is becoming increasingly reliant on computers and the internet as technology advances. Conversely, the sphere of cyberspace facilitates information to be transferred, leaving millions of people vulnerable to information security breaches. People often remain the weakest link in the security chain and social engineering is an effective method of getting around security obstacles. A skilled social engineer will often try to exploit this weakness in order to achieve a desired result. A culture of information security should be fostered in an effort to protect information in organisations as well as for individuals.

Having looked at the fundamental perspectives on and impact of social engineering, chapter 3 will present a psychological and legislative perspective on social engineering.

CHAPTER 3

A PSYCHOLOGICAL AND LEGASLATIVE PERSPECTIVE ON SOCIAL ENGINEERING

“The social engineer employs the same persuasive techniques the rest of us use every day. We take on roles. We try to build credibility. We call in reciprocal obligations. But the social engineer applies these techniques in a manipulative, deceptive, highly unethical manner, often to devastating effect.” Dr. Sagarin, Social psychologist (Mitnick & Simon, 2002: 221).

3.1 INTRODUCTION

Social engineering crosses the boundaries of various disciplines. Its roots stem from the criminological and computer science disciplines (vide chapter 2). It also derives from psychological perspectives as well as touches on issues of legislation. The aim of the current study is to explore, describe, explain and analyse social engineering attacks by means of MIT analysis. For this reason, these disciplines need to be explored through their relation to social engineering and its associated facets. In order to do this, the psychological and legislative perspective on social engineering will be discussed.

3.2 SOCIAL PSYCHOLOGY CONSIDERATIONS IN SOCIAL ENGINEERING

Social engineering is inherently psychological in nature, as it relies on manipulation and exploitation of the human element to be successful (Frangopoulos, 2007: 82). Thus, a need arises to explore the psychology behind social engineering attacks. Social engineering specifically incorporates aspects of social psychology, as humans and their social surroundings play a pivotal role in its methods of operation. Frangopoulos (2007: 82) further argues that effective social engineering results depend on human

vulnerabilities, because technical hacking methods alone would not be able to achieve the same results. The following section seeks to identify the methods and techniques used in social engineering attacks based on a social psychology perspective.

3.2.1 Background and origin of social psychology

Aspects of social psychology have most likely been considered, discussed and questioned as long as humans could think about each other and their social contexts. However, the scientific study of social psychology only commenced by the end of the nineteenth century (Kassin, Fein & Markus, 2014: 12). Early findings indicate that researchers such as Triplett and Ringelmann emerged as some of the first scholars interested in social psychology, for they explored how the presence of others influences an individual's performance. However, the discipline only started to develop structure once social psychology textbooks were written between 1908 and 1924. The field of social psychology started to develop rapidly when the world sought explanations to the violence of war and possible resolutions to it. Accompanied by this rapid growth, were the questions raised from the ethics involved in research practices, the validity of research findings as well as the generalisations made from research conclusions (Berscheid, 1992; Cartwright, 1979; Goethals, 2003; Kassin et al, 2014).

At present, social psychology assists in deciphering many societal problems such as racism, environmental pollution, Human Immunodeficiency Virus/Acquired Immunodeficiency Syndrome (HIV/Aids) and crime. In this way, social psychology can lead to the advancement of a theoretical model upon which intervention can be based (Buunk & Van Vugt, 2008: 4).

3.2.2 Defining social psychology

Kassin et al (2014: 6) define social psychology as the scientific study, inclusive of methodical observation, narrative and measurement, of how individuals think, feel and behave in a social context. Furthermore, these thoughts, feelings and behaviours are

studied in terms of their conceivable influence by the authentic, fictional or implied presence of other human beings (Stroebe, Hewstone & Jonas, 2008: 5). For instance, an individual needs only to imagine receiving positive or negative reactions from an authoritative figure for those reactions to influence that individual's self-esteem and confidence. Smith, Mackie and Claypool (2015: 3) state that social psychology is a science which focuses on the effects that social and cognitive processes have on the individual. Social psychology fixes its attention on the psychology of the individual and inhabits a social context as their thoughts, feelings and behaviours either concern other people or are influenced by other people (Kassin et al, 2014: 7).

Criminal activity should be perceived as a process, as opposed to an event or action. This process is often embedded in earlier experiences. Thus, the inherent nature of psychology focuses on individuals by investigating the latent process of cognitive, emotional and interpersonal facets of the criminal process (Canter, 2013: np). The psychology of crime can consequently provide insight into a wide range of criminal activity (Canter, 2013: np; Walters, 2012: 8; Webber, 2010: 6). Crime does not occur in a vacuum and thus needs to be investigated holistically.

In order to explore social engineering's correlation to social psychology and criminological principles, the following aspects need to be discussed: the significance of trust in social engineering; the art of persuasion; and compliance mechanisms used in social engineering attacks.

3.2.3 The significance of trust in social engineering

The social engineer's principal objective is to cultivate enough trust to successfully carry out an attack (Mann, 2008: 88). Human beings have a natural tendency to trust others. This element of trust is classically illustrated by the Milgram experiment conducted in 1961 (cf. Milgram, 1963: 371), in which Milgram set out to showcase the conflict between obedience to authority and personal conscience; it also highlights individuals' natural inclination to trust. There were two roles in the experiment – the teacher and the learner. Milgram ensured that one of his associates would always be the learner, unbeknown to

the participants. The teacher was told to ask the learner a series of questions and to administer an electric shock every time the learner answered incorrectly, increasing the degree of shock each time. The results of the experiment indicated that all of the participants continued to 300 volts while 65 per cent (two-thirds) of the participants continued to the highest level of 450 volts (Milgram, 1963: 371). Naturally, the teacher trusted the instructions from the researcher enough to carry out the electric shocks. Similarly, social engineers attempt to exploit the human tendency to trust and follow what people say.

A common aim of the social engineer is to establish rapport with the target. Rapport refers to mutual feelings of trust and openness between the researcher and the research respondents. In this way, greater levels of insight and understanding between both parties can be obtained (Davies & Francis, 2011: 352). Rapport can be established through a multifaceted mix of aspects which ultimately seek to build confidence and trust. Research shows that people who function in a high level of rapport will mirror one another's body language. In scientific terms the art of mirroring someone's body language is known as limbic synchrony. Mirroring involves observing a person's body posture and then subtly manoeuvring the body in such a way that it reflects that person's position (Goman, 2011). In society, this can be demonstrated through couples who are attracted to each other. Upon observation, it would appear as if they are mirroring or copying each other's posture, movements and gestures. This is often done unintentionally and with little to no concentration as it is a subconscious activity (Goman, 2011; Handel, 2013; Mann, 2008). Correspondingly, Hadnagy (2011: np) notes the importance of mirroring for social engineers in terms of observing a target's demeanour. A timid target will likely not be persuaded if approached in a loud or bold way, subsequently endangering the social engineer's attack.

Mann (2008: 92) argues that a combination of rapport building techniques is required for a successful social engineering attack. Of particular interest is a technique called "mirroring breathing". A person's state of mind is revealed through their breathing rate. This can easily be mirrored by observing the movements of the shoulders and thus matching their breathing frequency. This technique is advantageous as it compels the

social engineer to talk less and listen more. True listening is an additional method used to gain rapport. This type of listening is seldom done as it involves intense focus on what the other person is trying to say (Hadrnag, 2011: np). During conversations, most people only listen enough to be able to formulate what they want to say next. On the contrary, true listening can yield powerful effects when put into practice. Mann (2008: 94) suggests that an effective way of engaging in true listening is by reinstating the idea presented through agreement, and by then paraphrasing what was said using different words. Moreover, Mann (2008: 94-95) mentions the “magic pause” as another practice to gain further rapport. The magic pause consists of a social engineer making a conscious effort to wait before speaking. If the target stops talking, it is essentially the social engineer’s turn to speak. This is particularly imperative for when the social engineer is about to introduce his/her own ideas into the target’s mind.

Similarly, attire has an important role to play in developing rapport. The way one dresses projects a certain image and is often reflective of one’s personality. Hence, when someone is dressed similarly to the target of a social engineering attack, that person becomes more likeable and a sense of comfort and trust can be instantly achieved. The appearance of people and the way they look also influence rapport building. People tend to gravitate more to people who look like them. People often exhibit a natural prejudice and tend to trust people with similar demographic characteristics as them (Mann, 2008: 91). Additionally, the social engineer’s voice, tone of voice and speed of speech stimulates the process of rapport building (Mann, 2008: 91-92). For instance, a social engineer can easily gain unauthorised access into an institution. This can be done through research of the target – finding out what time employees start work, what type of dress code they follow and what type of physical controls are used to control access. If this information is obtained, a social engineer can access the institution and further exploit the target by accessing sensitive information through shoulder surfing or dumpster diving (vide section 2.6.1). Moreover, Frangopoulos (2007: 91) maintains that friendliness and pleasantness aid in a successful social engineer attack. In this way, trust and relationships are built as this technique is useful for the preparation of future attacks.

3.2.4 The art of persuasion

The art of persuasion is a vital tactic needed for a successful social engineering attack. It is a process by which attitudes and perspectives are modified (Kassin et al, 2014) to suit the social engineer. Within the realms of social psychology, there are two routes to persuasion, namely the “central” and “peripheral” route. Petty and Cacioppo (1986) outline this dual-process model by advocating that communication is not always processed in the same way. The former route (central) leans itself towards a systematic order and makes use of logical arguments in order to evoke a favourable response (Frangopoulos, 2007: 87). This route allows the individual to think critically about the information received and to be swayed by the strength of its arguments (Petty & Cacioppo, 1986). This technique cannot be employed by the social engineer, as there is no logical reason to give sensitive information to an unauthorised individual. Divergently, the latter technique (peripheral) makes use of mental shortcuts, distraction techniques and peripheral cues as a means of stimulating favourable responses (Frangopoulos, 2007: 87). Petty and Cacioppo (1986) argue that the peripheral route to persuasion is determined by superficial cues. Thus, this method is preferred by social engineers as it allows for the misrepresentation of objectives (Rusch, 1999). In this way, the social engineer attempts to manipulate the human mind by shifting its opinion.

The brain is divided into two hemispheres which function distinctively. By examining the roles of the left and right side of the brain, the mechanisms of persuasion are highlighted. The left side of the brain is responsible for analysis, reasoning and logic, while the right side is responsible for creativity and imagination (Kosslyn & Miller, 2014). A skilful social engineer attempts to exploit the functioning of the brain by keeping the left side occupied in pursuance of the right half. For instance, a social engineer could pretend to be a credit card company consultant and phone the target during the middle of the night reporting suspicious activity happening in relation to the card, such as online purchases. The social engineer could offer immediate assistance by reversing the transactions made and blocking the card if only the target provides the details of the card. In this manner, the social engineer successfully puts the target in a perilous and risky situation that requires

analysis by the left side of the brain while the real request (disclosure of the credit card details) is processed by the right side of the brain.

Amidst the artistry of persuasion are certain persuasion tactics (Cialdini: 2001; Granger, 2001; Makosky, 1985) which should be discussed in terms of social engineering attacks.

3.2.4.1 Impersonation

This technique of persuasion can be executed electronically, via the phone or through a physical attack. Reliant on the type of scenario the social engineer is operating in, impersonation can take on a variety of forms (Frangopoulos, 2007: 89). Inclusive of these forms is pretending to be an executive via e-mail or phoning as a technician from the IT department. In terms of a physical attack, the social engineer can pretend to be a repairman who has been called in to attend to a problem (vide section 2.6.1). McCann (2014) reports cases where criminals tamper with communication systems between corporate executives and their financial institutions. This is done by hacking into the companies' e-mails or financial systems. In furtherance of the criminal antics, the hackers will send fraudulent e-mails within the targeted company. The hacker will pose as a senior executive instructing a junior staff member to urgently execute a financial transaction such as a payment to a service provider. Subsequently, money is then transferred to a fraudulent account. Often these e-mail addresses are spoofed by adding, removing or subtly changing characters in the e-mail. This makes it difficult to distinguish between a bogus and legitimate e-mail address.

3.2.4.2 Ingratiation

Provided with an advantageous prospect to gain favour with people of authority and power, a target might be willing to go out of their way by doing something that he or she is not particularly supposed to do. The target may fear that the fictitious person of authority will foster imminent ill feelings towards him or her if the appeal is not adhered to (Frangopoulos, 2007: 89). Ingratiation can also be illustrated through the example posed

in section 3.2.4.1. McCann (2014) goes on to convey that not many people have the confidence to challenge senior personnel. These attacks are often successful because junior staff members are trying to impress senior management by completing tasks assigned to them swiftly and efficiently.

3.2.4.3 Conformity

Kassin et al (2014: 257) define conformity as the propensity to change perceptions, views or behaviour in ways that are consistent with group norms and standards. In 1978, Milgram and Sabini (1978) conducted a study where research respondents were asked to request subway passengers to give up their seats – an unusual violation of the custom of acceptable conduct. Many of the research respondents failed to perform their assignment at all and some of those who could go through with it became so nervous and apprehensive that they pretended to be sick in an effort to make their request seem warranted. As a deduction, not many people want to go against social norms because it makes them feel out-of-place, uncomfortable and isolated. The social engineer benefits from this human trait by offering the target mental shortcuts to rationalise actions that would initially appear to be unreasonable (Frangopoulos, 2007: 90). The social engineer would convey to the target that what is being sought by him or her has already been given to the social engineer by the target's associates and superiors. Thus, the social engineer reinforces the mental shortcut that if everybody else is doing it – it must be fine. However, such a request should not be direct but rather very subtly put. For example, the social engineer should explain to the target that upon discussing certain information with a mutual known person, certain information was shared. This will make the target assume that he or she is only providing the social engineer with information that someone else has already given. Inclusive in conformity practices, the social engineer might make use of "name-dropping" mechanisms by mentioning respected individuals who are well known to the target. The social engineer seeks to create the impression that the respected individual has already complied and agreed with the social engineer's request (Frangopoulos, 2007: 92).

3.2.4.4 Diffusion of responsibility

Diffusion of responsibility involves the belief that someone else should take responsibility and in effect be blamed for something under question (Kassin et al, 2014: 409). The social engineer is tasked to diffuse responsibility from the target to someone else in furtherance of making the target feel comfortable enough to proceed with the request. In such a way, the social engineer alleviates the burden the target feels of protecting sensitive information and upholding certain rules and regulations (Frangopoulos, 2007: 90).

3.2.4.5 Appeal to Maslow's hierarchy of needs

Although Maslow's hierarchy of needs theory is embedded in personality psychology (McLeod, 2014), it is a useful persuasion technique for social engineers. The social engineer aspires to fulfil as many of the target's needs as possible, namely: biological and physiological, safety, love and belonging, esteem and self-actualisation (Maslow, 1987). A social engineer masking as a disgruntled client or employer could deceive the target into thinking they can lose their job if they do not go through with the request, thus directly impacting their biological, physiological and safety needs (food, drink, shelter and perhaps even sleep and security). Characteristics such as flattery, acceptance, respect and expressions of prestige will impress on the target's need for love, belonging and esteem. A skilful social engineer could even imprint on the target's need for self-actualisation by making him or her realise their own potential through a specific request (Maslow, 1987; McLeod, 2014).

3.2.4.6 Providing a reason

Human behaviour often denotes that complying with a successful request is dependent on providing a reason. In a study done by social psychologist, Ellen Langer, this hypothesis was tested (Langer, Blank, & Chanowitz, 1978). Langer et al (1978) conducted an experiment by trying to bypass the cue at a photocopy machine by attempting to

phrase the request in different ways. The initial request was: "Excuse me, I have five pages. May I use the Xerox machine because I'm in a rush?" The researcher provided an authentic and reasonable reason for the request and thus the request was granted 94 per cent of the time. Subsequently, no reason was provided: "Excuse me, I have five pages. May I use the Xerox machine?" This request proved to be granted only 60 per cent of the time. Based upon comparison, it would appear that the success rate was dependent on providing a legitimate reason for a request. Be that as it may, the final request proved that as long as a "reason" was provided, success could be achieved. The third request received a 93 per cent success rate, which was: "Excuse me, I have five pages. May I use the Xerox machine because I have to make some copies?" This request blatantly stipulated the obvious and failed to provide any proper reasoning for requesting to cut in the line (Langer et al, 1978). Cialdini (2001: 4) observes that the mere presence of the word "because" triggered a human response automaticity providing for instant persuasion.

3.2.5 Compliance mechanisms

Kassin et al (2014: 271) describe compliance as the modifications and changes in behaviour which are prompted by direct requests. Cialdini (2001) denotes people who attempt to make others comply with or adhere to their requests as "compliance practitioners". Appropriately, social engineers fit into this category of compliance practitioners. The following compliance mechanisms will be discussed as they directly relate to social engineering: reciprocation, commitment to consistency, social proof, authority, and scarcity.

3.2.5.1 Reciprocation

Reciprocation is a social norm as it dictates that people treat other people the way they are treated. This can result in both positive and negative manifestations. Positively, acts of kindness are reciprocated, while negatively, such acts can cause retaliation against

those who have caused an individual harm. Thus, the norm of reciprocity reinforces predictability and fairness in social interaction and interdependence. However, the principle of reciprocation can be used for manipulation and exploitation purposes (Kassin et al, 2014: 272). Frangopoulos (2007: 94) argues that this principle can be exploited by social engineers in many ways. The social engineer may direct a “free” online offer to a list of particular targets and instead of providing just a piece of innocent software, lure the target to install software that could perform a spying function in addition to its advertised function. Similarly, the social engineer can also exploit the principle of reciprocity by solving a problem for the target and thus causing the target to feel indebted to the social engineer.

3.2.5.2 Commitment to consistency

This compliance mechanism is based on the principle that once a choice is made, personal and interpersonal pressures will enable the individual, who made the choice, to consistently commit to that choice (Cialdini, 2001: 53). In essence, human nature tends to stand by earlier decisions made (Frangopoulos, 2007: 95). In this way, the social engineer entraps the target based solely on previous interaction. In order for the target to be consistent towards the requests made by the social engineer, these requests will need to be continually granted. This requires careful planning by the social engineer. A commitment in the form of a promise by the target – be it direct, alluded to or even suggested – will be exploited by the social engineer (Frangopoulos, 2007: 96).

3.2.5.3 Social proof

This principle maintains that humans determine what is correct and acceptable by ascertaining what other people think is correct and acceptable (Cialdini, 2001: 100). Social proof can be exploited by the social engineer on the basis of uncertainty and similarity. The former involves a target which is so unsure of what to do, that when provided with information on what others are doing, by the social engineer, the target will

most likely conform. The latter assumes that people are prone to follow the lead of others similar to them, such as their peers. If these peers adhere to strict security protocol, the target is likely to do the same. However, if the target's peers view security haphazardly or if proper security measures are not implemented, the target will most likely view security measures in the same way. Consequently, this will either facilitate or impede a successful social engineering attack (Frangopoulos, 2007: 98).

3.2.5.4 Authority

It is considered a societal norm that individuals tend to have respect for authoritative figures. Furthermore, modern society promotes a culture whereby members are expected to obey legitimate authorities (Frangopoulos, 2007: 99). People who hold positions of authority are often perceived as being exceptionally knowledgeable, wise and powerful. Thus, when an opportunity arises, it is easier to relinquish the responsibility of a complicated decision to such a person. Interesting to note is that even the symbol of authority (titles, clothing, and luxurious cars) may yield positive results for the social engineer. When accompanied by the right assertiveness and composure, these symbols of authority can conjure an automated response from the target. This attack is difficult to identify and guard against as the influence of authority pressure on the target is often underestimated.

3.2.5.5 Scarcity

Scarcity perpetuates that a higher value is demarcated to goods and services which are not easily available. Subsequently, the value and appreciation of these goods and services are increased when they are viewed as a scarce commodity. For instance, during a phishing attack via e-mail, offers are presented as rare opportunities because they are only valid for a limited time (Frangopoulos, 2007: 100). In a typical online scam, a social engineer would pose as an attorney who came across a case in which a rich person unexpectedly died leaving a large sum of money in the bank. Since no family members

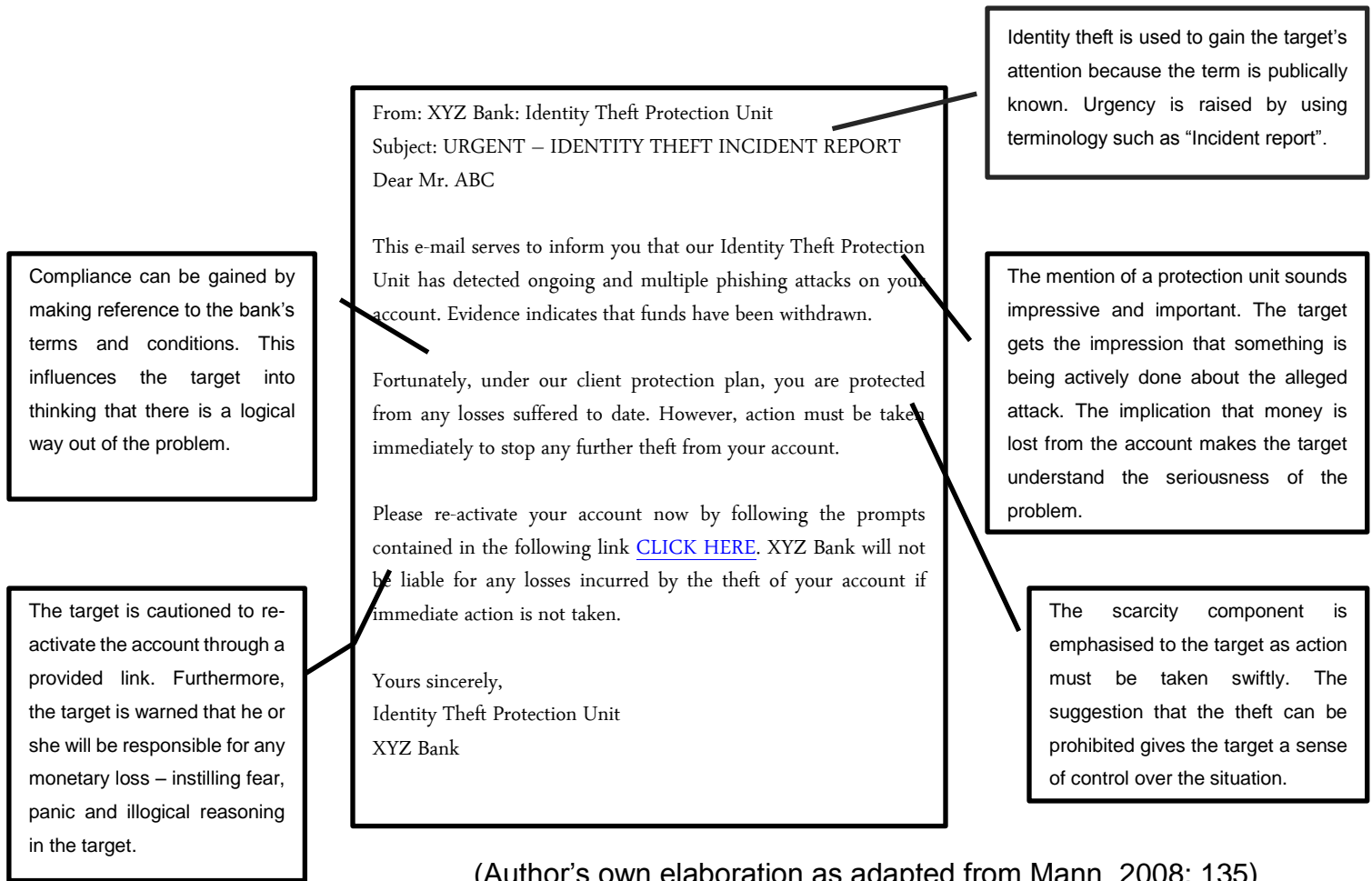
could be traced, the money would soon be dissolved into the state's fund. The target is asked to pose as the relative of the deceased as they supposedly share the same last name. This is usually done as a matter of urgency as if they do not act quickly, the money will soon be reclaimed. People who fall victim to this scam often lose money because they are tasked to share any transfer costs, legal fees and bribes to officials associated with the "attorney" (Anon, 2010).

In pursuit of further explanation of the psychological relevance of social engineering, an example will be elaborated on by applying psychological principles to a typical phishing attack.

3.2.6 A psychological examination of a phishing attack

The illustration below, based on research by Mann (2008: 135), depicts a common example of a typical social engineering attack by making use of a phishing e-mail and website. The target is made aware that money is being stolen from the target's bank account. The e-mail appears to be authentic and the alarm created in the target prevents the target from contacting their bank to confirm the e-mail's legitimacy. The target is then directed to a phishing website where their banking log-in details can be obtained. The social engineer is now at liberty to use these details to make transfers or to shop online.

Figure 3.1: A psychological examination of a phishing attack



The website hyperlink included on the notice will lead the target to the phishing website. Once the target clicks on the link and “reactivates” the account, the social engineer will gain access to the target’s personal banking log-in details. These details can subsequently give rise to various fraudulent activities.

The principles of social engineering are largely based on psychological attributes. Social engineering attacks cross the boundaries of legislation, as often the goal of the attack is to bring about illicit activity. The next section will discuss the current status of South African legislative measures put into place to guard against social engineering attacks.

3.3 SOUTH AFRICAN LEGISLATION

The following section represents a South African historical overview of the legislation pertaining to information security.

3.3.1 Overview and background of legislation addressing information security

Throughout South African history, the importance of protecting information and its related aspects has been advocated for. South African legislation often finds its roots in international policies, guidelines and legislation. This is traced back to 1980, when the Organisation for Economic Co-operation and Development (OECD) drafted and circulated guidelines on the “Protection of privacy and trans-border flows of personal data” (PoPi Compliance, 2016). Already at that time, the OECD was a global organisation which consisted of 30 prominent states; South Africa being one of them. The OECD’s guidelines recognise that even though national laws and policies vary, affiliates share a communal interest in safeguarding privacy and individual liberties. It acknowledges that automatic processing and trans-border movement of personal information produce new forms of relationships among countries and thus necessitate the expansion of compatible guidelines and practices. The guidelines also document that trans-border movement of personal data is vital, as it contributes to economic and social development (PoPi Compliance, 2016).

In 1981, the Council of Europe Convention on Data Protection, which consisted of 47 heads of states within European nations, drafted principles on data protection. These principles discuss the quality of data in the context of collection, purpose, precision and destruction of personal data. It also classifies data into special categories and recommends information security measures (PoPi Compliance, 2016). Thereafter, in 1995, the European Union adopted a data protection directive designed to protect individuals with regard to the handling of personal information and the free flow of such information. These directives paved the way for South Africa to include the right to privacy within Section 14 of the Constitution of the Republic of South Africa. In light of South

Africa's history of apartheid, this right to privacy (Constitution of the Republic of South Africa, Act 108 of 1996) entails the following:

Everyone has the right to privacy, which includes the right not to have :

- a) their person or home searched;*
- b) their property searched;*
- c) their possessions seized; or*
- d) the privacy of their communications infringed.*

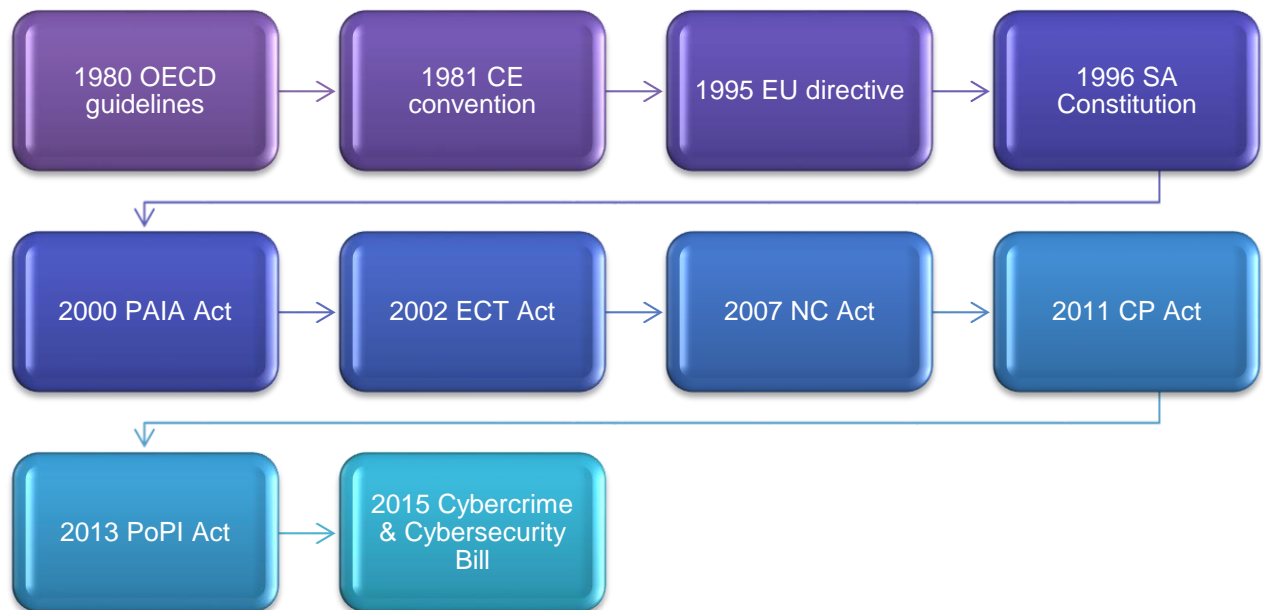
The Constitution of the Republic of South Africa was the starting point for all of the other later manifestations of legislation regarding information security in South Africa.

The South African Promotion of Access to Information (PAIA) Act 2 of 2000 was drafted in legislation to afford individuals access to manual and electronic records comprising personal information. In addition, Act 2 safeguards the privacy of third parties by prohibiting access to information that would result in unreasonable infringements. Shortly after the PAIA, in 2002, the Electronic Communications and Transactions (ECT) Act 25 of 2002 was promulgated. In sum, this Act makes provision for protection in terms of unwanted e-mail or spam, the unauthorised access to, interception of or interference with data as well as provides guidelines for privacy and security policies for e-commerce (vide section 3.3.1.1). Soon after this, the National Credit Act 34 of 2005 became fully operational. The purpose of Act 34 is to regulate consumer credit, but it also makes provision for persons dealing with personal information and stipulates that the confidentiality of financial information should be protected. In an effort to address unwanted communication, South Africa's Consumer Protection Act 68 of 2008 requires that consumers must be given the option to opt out of electronic commercial communications – non-compliance can result in a fine or up to one year imprisonment.

Nonetheless, the South African government still sought to establish a comprehensive piece of legislation that would be able to govern information security, thus the Protection of Personal Information Bill 2009 (PoPI) was passed by Cabinet and later in 2013 signed into law as Act 4 of 2013 (Republic of South Africa, 2013). Thereafter, in 2015 the

Cybercrime and Cybersecurity Bill was initiated as a means to develop a comprehensive framework dealing with issues of cybercrime and cybersecurity. The below figure is representative of this legislative timeline.

Figure 3.2: Timeline of legislation addressing information security



(Author's own elaboration as adapted from PoPi Compliance, 2016)

The account that follows offers a comprehensive discussion of legislation pertaining to information security in South Africa and how it impacts on social engineering and its related aspects.

3.3.1.1 The Electronic Communications and Transactions Act

The Electronic Communications and Transactions (ECT) Act 25 of 2002 (Republic of South Africa, 2002) originated as a formal structure aimed at defining and regulating e-commerce in South Africa. As noted by Sissing (2013), the Act has legal consequences for actions related to electronic communications, data messages and transactions. Furthermore, it includes various forms of communication mechanisms. The Act also functions as one of the first of its kind as an informative and enabling resource in which concepts relating to e-commerce, are legally identified and defined. The Act sought out to present statutory criminal offences relating to information systems. This includes unauthorised access to data; interception of or interference with data; computer-related extortion; fraud; and forgery – all of which are particularly of great importance to the social engineer. Additionally, the Act monitors unauthorised access to, interception of or interference with information as follows:

Unauthorised access to, interception of or interference with data

(1) Subject to the Interception and Monitoring Prohibition Act, 1992 (Act No. 127 of 1992), a person who intentionally accesses or intercepts any data without authority or permission to do so, is guilty of an offence.

(2) A person who intentionally and without authority to do so, interferes with data in a way which causes such data to be modified, destroyed or otherwise rendered ineffective, is guilty of an offence.

(3) A person who unlawfully produces, sells, offers to sell, procures for use, designs, adapts for use, distributes or possesses any device, including a computer program or a component, which is designed primarily to overcome security measures for the protection of data, or performs any of those acts with regard to a password, access code or any other similar kind of data with the intent to unlawfully utilise such item to contravene this section, is guilty of an offence.

(4) A person who utilises any device or computer program mentioned in subsection (3) in order to unlawfully overcome security measures designed to protect such data or access thereto, is guilty of an offence.

(5) A person who commits any act described in this section with the intent to interfere with access to an information system so as to constitute a denial, including a partial denial, of service to legitimate users, is guilty of an offence.

Alfreds (2015) maintains that it is relatively easy to gain personal and financial information from unsuspecting victims. This is often done through social engineering techniques such as phoning to request copies of identity documents or designing false e-mails to retrieve credit card identifications for malicious reasons. These stolen credentials can then be used to fund internet hosting services. The ECT Act makes it illegal for service providers to host malicious content, thus in effect contributing to the fight against cybercrime. The penalties involved in such misdemeanours range from a fine to imprisonment for a maximum of six months (Republic of South Africa, 2002). However, the practical implications of the Act are yet to be realised in South Africa. Perhaps this is a contributing factor to the need for additional legislation in an effort to safeguard information, such as the introduction of the Protection of Personal Information, Act 4 of 2013 (Republic of South Africa, 2013).

3.3.1.2 The Protection of Personal Information Act

Cybercrime is gaining increasing attention among South African individuals and businesses (Pillay, 2016; Thulin, 2015). In 2014, it was reported that cybercrime cost the South African economy R5.8 billion rand (Pillay, 2016). Consequently, this has greatly affected businesses in South Africa, which in turn affects the individual. Correspondingly, Pillay (2016) reports that it is estimated that between 70-80 per cent of South Africans have been victims of some form of cybercrime in their lifetime. As a countermeasure, the state introduced its first piece of legislation intended to protect personal information. Suitably, the Protection of Personal Information, Act 4 of 2013 (PoPI) was born (Republic of South Africa, 2013).

The Act, which took many years to develop, integrates international best practices. The PoPI Act endeavours to protect and safeguard personal information through the regulation of how information is treated, kept, secured and destroyed, by invoking minimum information protection requirements. In essence, the Act makes the safeguarding of information, inclusive of its collation and application relating to identifiable natural or social entities, compulsory. Thus, the PoPI Act affords individuals the right to

challenge those applications, within practical grounds, and to request that their information be deleted (Opland & Moodley, 2013).

The Act denotes personal information as information that is inclusive but not restricted to information such as “contact details, demographic information, history, biometric information, opinions of and about a person or private correspondence [like e-mail or text messages]” (Anderson, 2015). Prior to this, any information minimum standards were not made obligatory but rather used as a general guideline (Pillay, 2016). Plausibly, cybercriminals and social engineers need to access personal information in order to carry out criminal activity; and thus legislation such as the PoPI Act will aid in curtailing cybercrime.

Although, the South African Constitution (Republic of south Africa, 1996) protects its citizens’ right to privacy, the PoPI Act gives effect to section 14 of the Constitution. Within this right to privacy, is the right to “protection against the unlawful collection, retention, dissemination and use of personal information” (Republic of South Africa, 2013). In Section 2 of Act 4 of 2013, the purpose of the PoPI Act is outlined to:

(a) give effect to the constitutional right to privacy, by safeguarding personal information when processed by a responsible party, subject to justifiable limitations that are aimed at:

(i) balancing the right to privacy against other rights, particularly the right of access to information; and

(ii) protecting important interests, including the free flow of information within the Republic and across international borders;

(b) regulate the manner in which personal information may be processed, by establishing conditions, in harmony with international standards, that prescribe the minimum threshold requirements for the lawful processing of personal information;

(c) provide persons with rights and remedies to protect their personal information from processing that is not in accordance with this Act; and

(d) establish voluntary and compulsory measures, including the establishment of an Information Regulator, to ensure respect for and to promote, enforce and fulfil the rights protected by this Act.

Preceding the PoPI Act, disclosure of data breaches was not made compulsory, thus giving all individuals and businesses a false sense of security as the true extent of the cybercrime problem could not be established. Thulin (2015) lists simple social engineering techniques as one of the biggest breaches occurring in information security. This is done by illegally assessing employer or employee usernames and passwords, inadequate data encryption or infection of malware or ransomware. Thulin (2015) goes on to say that in South Africa these security breaches are centred on social engineering attacks, identity theft and fraud.

In 2011, South Africa faced one of its largest known data breaches, when Sony's PlayStation Network (PSN) was hacked into. The incident caused 77 million accounts, internationally, to be compromised, including more than that of 10 000 South African users. The security breach permitted the perpetrators access to users' personal information such as their credit card details. Although credit and debit cards are not necessary to become PSN members, the network offers its users the liberty to buy games, music and demos online. Since the discovery of the breach, Sony has encouraged its users to change their online log-in details and to be on the alert for any dubious activity on their cards (Germaner, 2011). Additionally, the perpetrators gained access to the PSN users' e-mail addresses, usernames, passwords, purchase history and home addresses. Stuart and Arthur (2011) argue that access to this type of personal information could subsequently give rise for malicious users (for instance social engineers) to steal other information, as people often use the same passwords for multiple sites. Furthermore, Germaner (2011) states that even when prompted for answers, Sony has decided against disclosing if the stolen personal information had been stored in encrypted files. Currently, when put into proper effect, legislation such as the POPI Act makes it mandatory for organisations to disclose such information.

Pillay (2016) reports that businesses will have one year to conform to legislation, upon the Act being fully implemented. This might be possible for smaller businesses, but may prove to be much more challenging for larger institutions as the necessary changes are more complex. The PoPI Act details the service of an "information regulator" (Republic of South Africa, 2013). Non-compliance with the Act can come about when complaints are

made to the information regulator. Opland and Moodley (2013) encourage organisations to address these complaints as quickly and effectively as possible. The PoPI Act makes it mandatory for organisations to inform the information regulator and its data subjects of any compromises relating to their personal information (Republic of South Africa, 2013). Additionally, organisations must release information pertaining to the loss of or stolen laptops containing personal data. Any incidents of misallocated faxes or e-mails, paper records thrown in the rubbish bin without being shredded, or employees inappropriately accessing information for personal reasons, must be declared (Opland & Moodley, 2013). Such information is immensely valuable for the social engineer as detailed in Chapter 2 of this study. Furthermore, Opland and Moodley (2013) explain that once the organisation informs the data subjects and information regulator of any data breaches, an investigation will be undertaken. However, to ensure compliance, regular spot checks of organisations can be held by the information regulator.

There are various consequences involved if the information regulator determines that an organisation lacks compliance or has violated the PoPI Act in any way. The information regulator can impose fines on organisations of amounts up to R10 million. This amount will vary, based on factors such as the degree in which the organisation endeavoured to comply with legislation, their cooperation with the investigation, the number of data subjects the data breach affected, and the potential magnitude of harm to those individuals. Criminal prosecution may be enforced in cases where fines are issued at their maximum and persons liable may face a prison sentence of up to 12 months. On the other hand, if an individual or organisation deliberately hinders an investigation, prison terms can be enforced of up to 10 years. If needs be, the information regulator can issue an “enforcement notice”, instructing the organisation to discontinue any processing of personal information. This can have vast operational and financial impacts on the organisation. Finally, depending on the specific incident, the information regulator can commence a civil law suit on behalf of the data subjects against the organisation. This best practice was imitated from the United States legislation which has been implemented due to data breaches. However, no case has yet to be successful as financial harm was not proven. On the contrary, in South Africa, the PoPI Act makes provision to guard

against harm such as emotional distress, loss of time and changing of information due to data breaches (Opland & Moodley, 2013; Republic of South Africa, 2013).

In an effort to create a more holistic piece of legislation to combat cybercrime and its relating facets, as well as to bring current legislation in line with international standards, the Cybercrime and Cybersecurity Bill was drafted in 2015 for public comment and scrutiny.

3.3.1.3 The Cybercrime and Cybersecurity Bill

The Department of Justice and Constitutional Development (2015) estimates that in South Africa, cyber-related crimes are increasing and cost the country more than R1 billion per annum. The need for the Cybercrime and Cybersecurity Bill stems from government's commitment to effect measures which can competently deal with cybercrime and cybersecurity. These crimes have adverse impacts on individuals, businesses and the government alike. The Bill seeks to create a comprehensive and cohesive cybersecurity legislative framework. In this way, the inadequacies which are present in dealing with cybercrime and cybersecurity can be addressed. The Bill aims do this through:

- creating offences and prescribing penalties related to cybercrime;
- regulating jurisdiction, as well as the powers to investigate search and gain access to or seize items in relation to cybercrimes;
- regulating aspects of evidence, relative to cybercrimes;
- regulating aspects of international cooperation in respect to investigations of cybercrimes;
- the establishment of various structures to deal with cybersecurity;
- the identification and declaration of National Critical Information Infrastructures and measures to protect these infrastructures;

- creating obligations for electronic communications service providers regarding issues that impact on cybersecurity. (The Department of Justice and Constitutional Development, 2015).

Inherent flaws in the Cybercrime and Cybersecurity Bill are noted. The Bill should be divided into two separate legislative Bills. The first should focus on cybercrime, while the other should purely deal with cybersecurity and the digital vulnerabilities and inadequacies of cyberspace. This split would allow for each piece of legislation to have distinct responsibilities. For instance, cybercrime will serve directly under the South African Police Service, while cybersecurity and its related aspect, such as information security, would fall under the jurisdiction of the State Security Agency (SSA). In addition, the Bill does not examine in any detail the technical aspects of cybercrime, cyberattacks, and hacking exploits in general. Aspects such as these should be comprehensively defined and conveyed in order to make clear distinctions.

3.4 CONCLUSION

This chapter established the psychological and legislative aspects of social engineering. The chapter attempted to expose the psychological ambiguities exploited by social engineers, in order to explore the mind of the attacker. In this way potential victims of social engineering attacks can be vigilant in resisting the psychological techniques used against them. Criminality cannot be studied in the absence of psychological elements such as behaviour, beliefs, perceptions and cognitive processes which are shaped through experiences. Similarly, principles embedded in social engineering have roots in social psychology and thus need to be reviewed holistically. Legislative issues surrounding social engineering were discussed. Although South African legislation addresses aspects of social engineering and information security, its practicality in enforcing such legislation is yet to be seen. By examining the psychological and legislative perspectives of social engineering, required steps can be taken towards the development of an integrative social engineering protection model.

The phenomenon of social engineering encompasses a vast array of disciplines in effectively defining, explaining and analysing it. The former chapter 2 and the current chapter 3 clearly indicate that the problem of social engineering cannot be merely situated in a single scientific discipline. On the contrary, it must be approached through a multitude of integrated disciplines, such as a multi-inter-transdisciplinary (MIT) approach. The following chapter will discuss the criminological theories underpinning the study.

CHAPTER 4

SOCIAL ENGINEERING AND CRIMINOLOGICAL THEORISING

4.1 INTRODUCTION

Crime is relative – it evokes diverse thoughts and denotations to different people (Brown, Esbensen & Geis, 2013: 8). The field of criminology, the fundamental discipline upon which this study is based, acknowledges that crime is the result of multiple causes (Henry & Einstadter, 1998: 5). Criminological theories influence social policy devised to address the crime problem. This involves identifying the nature of the particular crime as harmful, examining the bases of harm construction and distinguishing the assortment of interconnected effects on criminological processes. However, theories are not generated in a vacuum but are fostered within a historical and political milieu (Henry & Einstadter, 1998: 8-9). They respond to current events and are modified accordingly. For this reason, contemporary crimes can still be explained by traditional criminological theories when applied appropriately.

Criminological theories are constructed in an effort to find conceivable explanations for a particular anomaly. Such theories should be scientifically assessed in order to induce truth and cognisance. Theories rooted in criminology endeavour to provide answers to the following questions: why some people commit crime, why certain people are more prone to victimisation than others, and what constitutes certain crime patterns (Brown et al, 2013: 9; Van der Westhuizen, 2011: 123). Theories denote a set of logically interconnected propositions based on empirical findings (Bachman & Schutt, 2014: 31). Criminological theories offer immense value and insight as they provide explanations of crime and assist in making predictions about criminality. In addition, criminological theories aid in the organisation of empirical findings, direct future research and guide state policy (Bachman & Schutt, 2014: 31).

As previously indicated (vide section 2.3.2 & 2.3.3), research done on social engineering lacks sound theoretical support. The present study seeks to establish itself in foundational

criminological theories. Thus, the theoretical underpinning of this study will encompass theories evolving from the Classical school of thought, as well as the Positivist school of thought. Criminological theories are multidimensional and multidisciplinary in their very nature. Theories have been influenced by other disciplines such as sociology, psychology (vide section 2.3), education and geography amongst others. These theories, listed below, which are used to explain both victimisation and offending behaviour, are discussed in this chapter:

- Lifestyle exposure theory.
- Routine activities theory.
- Deterrence theory.
- Differential association theory.
- Neutralisation theory.

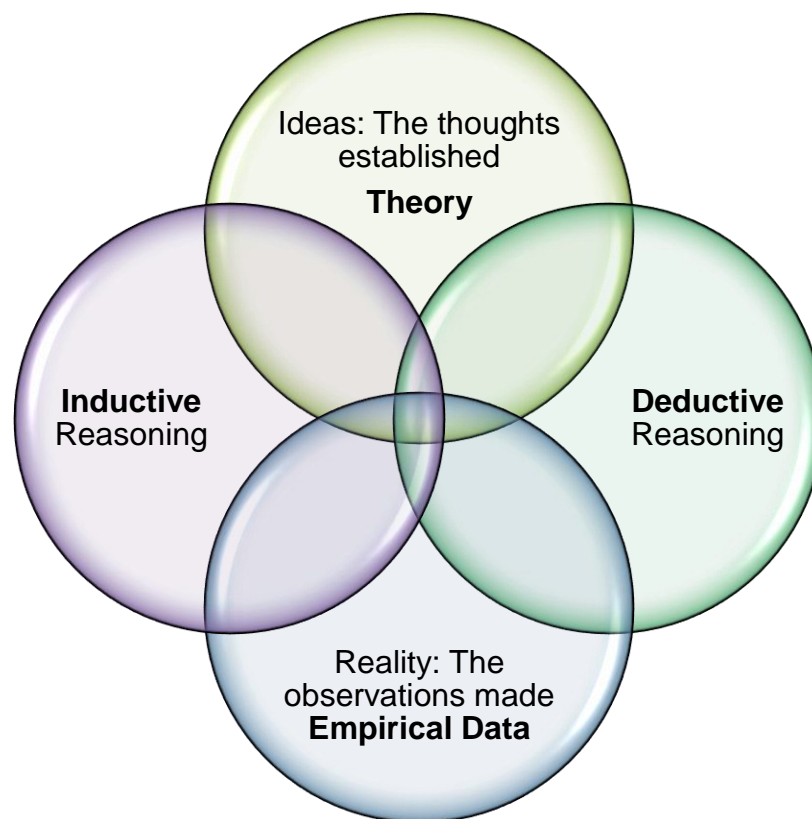
All types of social research strive to connect theory to empirical data. The following narrative discusses deductive and inductive reasoning in relation to criminological theorising.

4.2 DEDUCTIVE AND INDUCTIVE REASONING

Deductive reasoning progresses from general ideas, inclusive of theories, to specific reality, inclusive of empirical data. On the contrary, inductive reasoning begins with specific reality and then moves to general reality. Both types of reasoning systems are vital in the discipline of criminology. Theories are only tested fairly when deductive reasoning is employed. This involves establishing expectations and then choosing methods to test the gravity thereof. Unless a theory has undergone testing, it can only be viewed as tentative (Bachman & Schutt, 2014: 33). Nonetheless, it is acknowledged that theories cannot always make expedient predictions about every research problem, as

serendipitous findings can be established. These findings represent unanticipated patterns in data which can inspire new ideas or theoretical approaches (Bachman & Schutt, 2014: 34). Regardless of the outcome, inductive reasoning should be utilised in order to make sense of unanticipated findings. Subsequently, if validity is determined in new findings, deductive reasoning can be used to construct a new study as a means of testing these new ideas. The relationship between theory and empirical data is portrayed in Figure 4.1 within the context of deductive and inductive reasoning.

Figure 4.1: The relationship between theory and data



(Author's own elaboration as illustrated from Bachman & Schutt, 2014: 34)

4.3 CLASSICAL CRIMINOLOGY

Historically, the punishments put into place to address crime, deviance or non-conformity had an inclination to be severe and inhumane. This marked a pivotal time to introduce a new school of thought (Brown et al, 2013: 158). The Classical school of criminology, founded by researchers such as Beccaria and Bentham, advocated for a revolutionised, impartial and proficient justice system. Subsequently, Classical criminology campaigns for an unbiased and better controlled social order. This school of thought is influenced by the utilitarian philosophy where punishment should be proportional to the crime and simultaneously dissuade potential offenders from recommitting that particular crime. It argues that individuals are innately hedonistic by nature as they subscribe to the pleasure-pain principle. This principle maintains that individuals evaluate available choices in terms of how much pleasure can be gained as opposed to how much pain can be circumvented. This process of change should be systematic, as it can only take shape through an analytical, organised and legal mandate. The Classical school puts focus on the criminal act rather than the criminal - ultimately assuming that offenders are rational, pleasure-seeking, self-interested beings and able to make their own decisions (Siegel, 2004: 108; Tibbetts & Hemmens, 2010: 5; Tierney, 2006: 50).

Further developments in the Classical school of thought reasoned that not only do potential offenders consider the penal consequences of crime, but they also consider the situational opportunities available to commit crime. Therefore, in an attempt to remedy such situational opportunities, various factors in the environment should be manipulated to consequently strengthen potential targets and thus reduce victimisation. Criticism of this school of thought notes that if potential offenders are self-motivated, manipulating environmental factors and target hardening will only displace crime (Henry & Einstadter, 1998: 17). With regard to social engineering, if potential targets undergo victim resilience through education and awareness they will be less prone to social engineering attacks. If a general and widespread culture of information security is adopted and strictly adhered to, potential criminal activity can only be displaced to individuals ignorant of such a culture.

The subsequent section will discuss the lifestyle exposure, routine activities and deterrent theories in terms of their applicability to social engineering.

4.3.1 Lifestyle exposure theory

The lifestyle exposure theory originated from the Classical school of thought. It was developed by Hindelang, Gottfredson and Garofalo (1978). The theory maintains that the probability of victimisation is reliant on an individual's way of living (Reyns, 2010: 37). It is rooted in the notion that individuals subscribe to a personal daily routine which makes up their specific lifestyle. The theory proposes that victimisation rates correlate with an individual's demographic make-up such as age, gender and race. Furthermore, younger and unmarried individuals are more susceptible to victimisation as they are often away from home. The theory puts forward that change in the customary activities of a group or an individual directly influences their vulnerability to risk as well as the opportunities for offending or victimisation (Davis, 2005: 36; Saponaro, 2013: 15). The theory is applicable to social engineering as its basis lies in lifestyle. With regard to social engineering, victim vulnerability increases when one is in contact with personal information and not consciously protective of it. This is applicable to individuals and to business institutions.

Individuals who have any information which they regard as personal, private or sensitive such as passwords, pin numbers, purchasing patterns - or even health status - as informed by the relevant legislation (vide section 3.3), are vulnerable to social engineering attacks. Modern lifestyles are governed by information and individuals are often unaware of the extent of this governance. Individual lifestyles involve the standardisation of information sharing, without being aware of the potential consequences. This is evident in current news, as Mokati (2015) reports. The article warns South African citizens against publicising too much personal information. For instance, posting pictures of oneself on social media sites revealing residential location or regular hang-out spots opens doors to potential victimisation. Similarly, "check-in" functions on social network sites and "tagging" of locations also increase possible victimisation, as potential offenders can access this information with ease. Furthermore, on these sites personal information is freely shared such as mobile numbers, work and residential addresses as well as e-mail addresses.

Thus, individuals' lifestyles directly impact their risk to social engineering attacks (vide section 2.4). Of equal importance is the impression that the lack of information safeguarding, as well as inadequate awareness of and adherence to information security practices, is becoming a trend among South Africans. This is evident in South African subcultures as became apparent in recent banking attacks and social engineering attacks on the South African Revenue Service (SARS). In an article by Vermeulen (2013), where the head of digital channels and payments at Absa Retail was interviewed, it was reported that many South Africans are falling prey to e-mail scams from "SARS" claiming that large sums of money are owed to them after an evaluation on their tax return had been done. Further instructions indicate that the target should go to a spoofed SARS website and enter their online banking details. As most banking systems make use of SMS authentication processes, social engineering tactics are used to retrieve the cell phone number, for instance by phoning the target's workplace and asking for the cell phone number. Once the social engineer has the target's cell phone number they can intercept the random verification number sent out by the bank.

Further social engineering techniques are used when the social engineer attempts to guard against being caught by transferring the money into an account that cannot be traced back to the perpetrator. The social engineer can easily convince a stranger to let money be transferred to their account, by means of an emotional appeal combined with a promise of monetary gain. Upon further investigation, Vermeulen (2013) maintains that these attacks can be successful for up to six months, and often this is the social engineer's main source of income. Moreover, the article explains that even if banks or cellular operators tighten security features in one place, the social engineers will merely target something else, or change banks.

The unawareness of information protection among individuals opens doors to victimisation. As long as individuals are not aware of information security protocols, it is reflected in their lifestyles and in turn influences their victimisation probability as well as increases offending opportunities. SARS actively guards against such attacks through their website, where such attacks are exposed. The website provides examples of a variety of different social engineering attacks which target unsuspecting tax payers. In

addition, social engineers will use the credibility of SARS to target victims into paying administration fees for fictitious internship programmes (SARS, 2016). Although this information is enlightening and useful, if individuals are not made aware of the potential dangers as well as their vulnerability to victimisation, social engineering attacks will continue to prevail.

Business institutions are also at risk to social engineering attacks due to the nature of their occupational lifestyles. Young (2015) affirms that in the business world, information is vulnerable to a variety of attacks. For instance, social engineering is used to gather information about the target to be used in a phishing e-mail. The e-mail impersonates a communication from a known associate but a corrupted website link or document containing malware or ransomware can be attached. This could enable analogous processing such as access to system files, e-mail and keystrokes. Thus, an unsuspecting employee, engaging in a stereotypical occupational lifestyle, will let criminals into their business, increasing vulnerability to a wide range of attacks and consequences.

In a recent incident reported in France, Keyworth and Wall (2016) documented how a medium-sized business was deceived out of thousands of euros in a social engineering scam. The company's accountant was contacted via telephone and told that the president of the company was going to send an e-mail authorising a confidential transaction. The phone call and e-mail seemed very standard as they followed customary business protocol. Soon the accountant issued the approval of four large transactions to be carried out – three of them were held up by the bank but one was successfully made, resulting in a huge financial loss. This example indicates that as long as business personnel have access to personal and private information in their everyday functionality, they are susceptible to social engineering attacks.

4.3.2 Routine activities theory

The routine activity theory, founded by Cohen and Felson (1979) rationalises crime as a derivative of the recurring, routine activities and structuring of everyday life (Kirwan & Power, 2013: 25). Similarly to the lifestyle exposure theory, the theory maintains that

victimisation can be linked to the habitual activities that individuals take part in every day. Important to note is that this theory was developed to explain how the spatial-temporal structuring of social activities reinforces the conversion of criminal capacity into actual crime (Cohen & Felson, 1979). Innately, the theory was used to explain the capacity and extent of contact crimes such as violent crime or burglary, in which the victim and offender are physically and mutually present at the crime scene (Davis, 2005: 39; Reyns, 2011: 217; Saponaro, 2013: 19; Siegel, 2004: 92; Tibbetts & Hemmens, 2010: 103). On the contrary, research indicates that this theory can also be used to explain crimes that occur regardless of the offender and victim being in the same place (cf Eck & Clarke 2003; Holtfreter, Reisig & Pratt 2008; Pratt, Holtfreter & Reisig 2010; Reyns, 2011). With regard to crimes that manifest from social engineering attacks, victims do not necessarily need a mutual physical location for the crime to take place. Phishing attacks can be carried out through the telephone or e-mail. On the contrary, social engineers can also use human-based attacks to incur victimisation whereby the victims or targets are in a mutually present location (vide section 2.3.1).

The framework of the theory proposes that the likelihood of victimisation depends on the presence of three variables occurring at the same time: a motivated offender, suitable target and the absence of capable guardians (Kirwan & Power, 2013: 25). These factors will be discussed in terms of their correlation to social engineering and its related aspects.

- **Motivated offender**

A motivated offender constitutes an individual who has reason to commit a crime. Regardless of logic or sound judgment, to the motivated offender their reasoning is personal and prudent and thus should be executed (Davis, 2005: 40). Social engineers need to be motivated in order to carry out their attacks. Motivations vary for illicit activity ranging from financial gain, access to trademarked information, competitive advantage, revenge, embarrassment and humiliation or even reputable damage (vide section 2.3.4).

- **Suitable target**

The theory suggests that the presence of four components, namely: value, physical visibility, accessibility and inertia, dictate the appositeness of a target (Felson & Cohen, 1980). The value of a target is found in its financial and symbolic disposition, thus magnifying the desirability of it. Physical visibility denotes the prospect of being perceived by potential offenders. Accessibility necessitates the ease with which an offender can approach a target without enticing suspicion. Inertia refers to the ease with which a target can be attained (Saponaro, 2013: 19). With regard to social engineering, the value of the target is the determining factor why the social engineer chooses that individual as the target. This could be because that specific individual has access to information needed to carry out a social engineering attack; thus the social engineer needs the target to carry out the attack (vide section 2.3.2). Physical visibility is not always a necessary requirement for a social engineering attack. However, as long as the target is perceived, for instance through electronic mediums, an attack can take place. Accessibility and inertia are of vital importance to the social engineer to carry out attacks, as evident in the modus operandi (vide section 2.6.1) of the social engineer as well as evident in the social engineering attack framework (vide section 2.7.2).

- **Absence of capable guardianship**

Felson and Cohen (1980: 392) explain that protection entails any form of spatial-temporal surveillance of people or property which may aid in decreasing the likelihood of criminal offences from transpiring. Guardianship can take on many forms, such as through an individual (e.g. parent or police officer) or through technological aids such as a firewall. Furthermore, the theory proposes that the quantity of offences directly interrelates with the nature of daily routines and interactions. The theory identifies certain crime hot spots as areas where teenage males and unemployed adults assemble. Not many people frequent such places in the company of capable guardians, often resulting in an increased risk of social engineering. Moreover, such areas tend to have high victimisation rates (Saponaro, 2013: 20). Although these hot

spots were initially identified as physical in nature, it is also applicable to the study at hand. The absence of capable guardianship with regard to social engineering attacks could include a lack of appropriate and effective technological safeguards, as well as the absence of information security awareness. As Young (2015) indicates, the only way to counter increasingly swift, globally allied and synchronised attacks is to embrace a multifaceted, swift, globally allied and synchronised approach to information security. In this way, effective guardianship against social engineering attacks requires an integrated MIT approach.

The use of the lifestyle exposure theory, as well as the routines activity theory, does not afford blame to the victim but rather seeks to expose the risks and vulnerabilities associated with lifestyle.

4.3.3 Deterrence theory

The deterrence theory postulates that motivated individuals will infringe the law if they do not fear the penalties of their actions. Thus, it can be deduced that criminality can be monitored and controlled by escalating the actual or perceived threat of punishment (Siegel, 2011: 95). Deterrence is distinguished as two types, namely general and specific. The former (general) makes use of punishment, perceived or actual, to serve as an example to potential offenders who might intend committing similar crimes. In this way additional illegal activity may be reduced as potential offenders are encouraged to reconsider illegal behaviour by making use of the rational-calculative process.

In order for general deterrence to be effective, publicity plays an important role. The more aware the public is about possible sanctions associated with specific crimes, the less likely they will want to engage in illicit behaviour. Publicity is achieved through media and word-of-mouth campaigns whereby accurate or distorted information about possible sanctions can be disseminated to the public. General deterrence aims to convey to the public that crime does not pay. Specific deterrence is focused on the individual offender and aims to deter him or her from future misconduct through punishment. This principle makes use of punishment to convince the offender to reconsider additional crime

involvement (Brown et al, 2013: 175). Publicity is an imperative factor in the continuation or hindrance of social engineering attacks. Applicable and comprehensive legislation has been drafted in South African law (vide section 3.3). However, if the details and consequences of this legislation are not unpacked clearly to the general community, deterrence will not be achieved.

Moreover, theory suggests that the frequency of crime patterns will be lowered if certainty, severity and speed of legal sanctions are increased and carried out effectively (Siegel, 2011: 95). The certainty of punishment assumes that if the process of arrest, conviction and sanction is an inevitable definite, crime rates will decline. The certainty of punishment will thus outweigh any benefit associated with committing the crime. The severity of punishment assumes that if punishment is harsh and relentless, potential offenders are likely to resist criminality. The swiftness or speed of punishment ascertains that the quicker punishment is effected, the better it would serve as a deterrent for future offending. Important to note is that these elements of punishment are reliant on each other for effective deterrence (Siegel, 2011: 95-96). All of the elements proposed for deterrence to occur will coincide with effectively prosecuting behaviour associated with social engineering attacks. There should be certainty of punishment as outlined in the legislation, severity to suit the crime and its impact and prosecution should not be a long and drawn out process.

4.4 THE POSITIVIST SCHOOL

Whereas the founders of the Classical school consisted of writers and philosophers, the Positivist school is made up of scientists, mathematicians and doctors. Those who advocated for Classical regimes intended to modernise and civilise research within the social sciences. The Positivists sought out to categorise and explain the world around them. Thus, Positivists find value in scientific exploration and the discovery of new facets within the social world (Williams & McShane, 2013: 32). The main assumptions of Positivist criminology incorporate a deterministic perception of reality, emphasis on criminal behaviour, as well as the prevention of crime by means of treatment and

rehabilitation of offenders. Hence, Positivists use scientific research techniques when investigating a research problem. In essence, Positivism is a philosophical system which promotes the “positive” application of science to knowledge production (Williams & McShane, 2013: 33). As elaborated by Williams and McShane (2013: 41) the following denote the major assumptions of this school of thought:

- Reality is dictated by a cause and effect process. Characteristics of reality portray order and can be explained and understood through systematic observations.
- As crime is a social problem, it can be alleviated by means of a systematic investigation into human behaviour. By applying science to human behaviour, human existence can be improved.
- Criminality is a product of abnormalities. These abnormalities may be internal or operate as external influences.
- Abnormalities are discovered through a comparative analysis of characteristics which are considered to be normal. Once abnormalities are identified, the discipline of criminology is required to correct it. In this way, abnormalities can be treated and the criminal rehabilitated.
- Rehabilitation is beneficial for the criminal, so that normality can be induced, as well as for society, so that members of society can be protected from crime.
- The employment of sanctions against criminals is not merely for punishment purposes but rather for treatment.

The Positivist school of thought is based on biological, psychological and sociological perspectives. In summary, it argues that criminal behaviour can be determined by forces outside of the offenders’ control, which can shape their behaviour. In this way, criminal behaviour is not based only upon free choice. Furthermore, it puts forth that knowledge is acquired scientifically through observation and experience and relies on empirical data. Social process theories form part of the Positivist school of thought, as it maintains that criminal behaviour can be learnt (Brown et al, 2013: 218).

4.4.1 Social process theories

Social process theories attribute crime as a consequence of learning the norms, standards, beliefs and behaviours concomitant with criminal activity. They conclude that criminal behaviour is acquired through social context and social interactions, thus crime is perceived as “normal” in lieu of “pathological”. These theories attempt to provide explanations for how individuals become criminals. Social process theories explore both the psychology and modus operandi of criminality (Brown et al, 2013: 309; Siegel, 2011: 173). Social process theories cut across social classes and economic status of criminals, as delinquency is not exclusively viewed as a lower-class problem. Furthermore, these theories are supported by self-report findings (Brown et al, 2013: 310). Self-report studies are often used in determining the extent of social engineering attacks and similarly used in the empirical inquiry of this study.

The following discussion will outline differential association theory and neutralisation theory, subcategories of social process theories, in terms of their applicability to social engineering and its associated facets.

4.4.2 Differential association theory

Edwin Sutherland was the founder and developer of the differential association theory (Sutherland, 1949), which has evolved to be one of the most well-known theories explaining criminal behaviour (Brown et al, 2013: 311). Through Sutherland’s research on white collar crime, professional theft and intelligence, he concluded that crime is not merely the result of intrinsic inadequacies of the lower class, but as behaviour which is learned (Siegel, 2011: 174). Bearing in mind that the theory was in 1947 (Siegel, 2011: 173), it promulgated that individuals who are brought up in disorderly and dysfunctional neighbourhoods are likely to be exposed to deviant or criminal cultures and associations, thus indicating that crime is a learned behaviour through these associations.

In a joint endeavour, Sutherland and Cressey (1974: 75) developed the nine principles of differential association theory, in which the manner by which an individual comes to participate in illicit and deviant behaviour is explained. The following dialogue depicts these principles as applied to a self-proclaimed and previously cited (vide section 2.7.1) social engineer, Kevin Mitnick. As part of a plea settlement, Mitnick was convicted of four counts of wire fraud, two counts of computer fraud and one count of illegally intercepting a wire communication. He served five years in prison and upon release, was forbidden to use any electronic communication systems besides a landline telephone. However, he appealed this ruling and it was overturned (Mitnick & Simon, 2002; Mitnick & Simon, 2011).

1. *Criminal behaviour is learned.* Criminality is learned similarly to other learned behaviours such as walking, writing or cooking. Mitnick mentions how he continuously worked at the craft of social engineering, always looking for new ways to perfect his technique. This crafting of technique started from a young age as he engaged in dumpster diving near his local bus depot to get free bus rides. He did this by scavenging the bus depot to find partly-used bus tickets which were thrown away by bus drivers after their shifts had been completed. He deviously found out where the punches (used to clip the bus tickets) were sold, by pretending to need something similar for a school project, and bought one. Now, armed with a pad of blank bus tickets and the punch he could mark his own tickets and travel for free.
2. *Criminal behaviour is learned through communication by interacting with other persons.* Criminality necessitates human interaction to occur. Through socialisation with criminal teachers and mentors, criminal behaviour is studied, imitated and practised. Although Mitnick describes himself as a loner as a child, he alludes to many mentors throughout his lifetime who helped teach him social engineering techniques. A particular incident was when a friend taught him how to use the telephone to participate in phone phreaking. Through this technique, Mitnick learned how to exploit the phone systems and phone company employees such as obtaining private

information on customers linked to the phone company and making calls for “free”. Mitnick also notes that he joined a hacker group where much of his learning occurred.

3. *The dominant way in which learning of criminal behaviour occurs, is within intimate personal groups.* The most influential people in an individual’s life are those closest to him or her, such as their family, friends and peers. In the same way, these people have the greatest influence in terms of deviant and antisocial behaviour. Mitnick acknowledges that a lot of his learning of criminal behaviour came from his friends and peers. He also refers to his father and uncles, who were salesmen, as being influential teachers as they possessed characteristics necessary to social engineers such as manipulation and persuasion skills and having the gift of the gab.
4. *When criminal behaviour is learned, the process includes techniques of committing the crime as well as the specific direction of motives, drives, rationalisations, and attitudes.* The techniques and procedures needed to commit crime need to be learned from associates. Within this learning process, the proper terminology and jargon need to be learned as well as the appropriate reactions to law violations, which are inclusive of defence mechanisms, suitable justifications and when to express feelings of remorse and guilt. In Mitnick’s criminal career he needed to learn the proper terminology, techniques, justifications for his actions and responses to law violations. Mitnick rationalised, in a court testimony, that often he did not know what he was doing was against the law, but rather did what he did to ease his own curiosity. He also attributes his disregard for authoritative figures to the molestation he experienced as a child by his stepfather who worked in law enforcement.
5. *The specific direction of motives and drives is learned from definitions of the legal codes as favourable or unfavourable.* Different people possess various beliefs and opinions that might view criminality in a positive or negative light. In this way, individuals are exposed to culture conflict as they encounter various people who are either in favour of criminality or against it. Mitnick validates this proposition by detailing

that his parents and peers approved of his deceitful and criminal behaviour and often commended him for it – thus motivating him to continue.

6. *A person evolves into a delinquent because they encounter more definitions favourable to violation of law than definitions unfavourable to violation of the law.* Delinquency is cultivated when individuals come into contact with persons, groups or dealings that produce a surplus of definitions in favour of criminality, thus insulating opposing perceptions. In Mitnick's case, he encountered more people who approved of his illegal activity than those who did not, thus fuelling his criminality.
7. *Differential associations may differ in frequency, duration, priority and intensity.* The persons in one's life who are most influential share quality social interactions. The longer-lasting these relationships are, the more influential they will be. Correspondingly, the more recurrent and regular these interactions are, the more significant they will be. Priority denotes the time period in which the particular associations were originated. Associations made in early childhood are viewed as having a greater impression than those made later on in life. Intensity emulates the value placed on a particular association, as well as the extent of identification an individual attributes to a specific association. Mitnick's parents and peers were all associates who were consistent in terms of frequency, duration, priority and intensity.
8. *The process of learning criminal behaviour by association with criminal and anti-criminal patterns involves all of the mechanisms that are involved in any other learning.* It is emphasised that learning criminal behaviour requires all the mechanisms and procedures needed to learn any other behaviour. Mitnick's criminal career brings truth to this proposition as all the mechanisms needed to learn any behaviour such as mentorship, practise, diligence and determination were evident in his transformation into a social engineer.
9. *While criminal behaviour is an expression of general needs and values, it is not clarified by those needs and values, since non-criminal behaviour is an expression of*

the same needs and values. This principle suggests that the motives which fuel criminal behaviour cannot be the same as those which fuel conventional behaviour. For instance, merely possessing an attribute such as financial ambition will not necessarily be motive enough for criminal behaviour, as one could also channel this attribute into working hard in obtaining a lucrative career. Thus, learning deviant norms and patterns through interaction with an excess of definitions in favour of criminality, will produce law violations. Although a great deal of Mitnick's explanation for engaging in criminal behaviour can be found in learned behaviour, other factors should also be considered such as opportunity, rational choice and neutralisation techniques.

4.4.3 Neutralisation theory

The neutralisation theory emanated from research done by Sykes and Matza (1957) where they too advocate that criminality evolves through a learning process. The foundation of the theory suggests that criminals must learn and master certain techniques that enable them to neutralise conventional and accepted values and attitudes, which in turn allows them to drift between illicit and conventional activity. The neutralisation theory argues that even the most committed criminal does not allocate all of his or her time to illicit activity. On the contrary, they can lead relatively normal lives such as work a job, attend to family responsibilities and participate in religious events. In order to drift from the conventional to non-conventional behaviour, criminals develop neutralisation techniques (Sykes & Matza, 1957: 664). These techniques, as outlined by Sykes and Matza (1957), are reviewed in light of their practical implications to social engineering.

- *Denial of responsibility:* The offenders might deny responsibility for their actions, claiming that the violation was not their fault but rather an accident or a result of circumstances out of their control. Denial of responsibility is often apparent in social engineering behaviours. Blame can be attributed to ignorance of legislation or lack of implemented or effective technological and human protective mechanisms (vide section 2.3.1).

- *Denial of injury*: The offender neutralises his or her illicit behaviour by reasoning that no real harm was done. Behaviours associated with social engineering can reason that no real injury was caused, especially when motivated by financial gain, as victims are already perceived to be well off. Thus, no real loss occurred.
- *Denial of the victim*: The offender may afford blame to the victim of the offence by refusing to view the victim as a victim at all. Instead, the offender believes that the victim deserved what happened to him or her. Crimes involving information security breaches are often viewed as victimless crimes because the social engineer does not usually come into direct contact with victims or targets.
- *Condemnation of the condemners*: The offender may subdue the acknowledgement of their own illicit actions by shifting the blame to others. Authoritative figures are blamed for the offender's actions. This is evident in Mitnick's case, as he admittedly blamed authoritative figures for his actions (vide section 4.4.2).
- *Appeal to higher loyalties*: Offenders may struggle with the loyalty they have to their deviant peers and the loyalty to adhere to societal norms. However, the needs of their peers take primacy because these demands are urgent and localised. Social engineers find solace in hacking communities where techniques are learned and perfected. These techniques can be used to motivate and influence their peers and at the same time be used to gain acceptance and value. Such communities can thrive in places such as the Dark Web - a collection of websites which are publically visible but the Internet Protocol addresses of the servers that run them are concealed (Egan, 2015).

4.5 CONCLUSION

Crime theories play an integral role in the explanation of criminality. A single explanation of offending and victimisation will be insufficient to explain criminality, as crime is inherently complex and interdependent on many different variables. For this reason, the present study was guided by criminological theories which provide possible explanations for victimisation and offending patterns. The lifestyle exposure theory investigated the

correlation between lifestyle and potential victimisation, while the routines activity theory attributed opportunities for crime to take place according to the routines that individuals occupy. The deterrence theory is essential with regard to the current study, as it attributes the involvement with criminality to unclear and operationally ineffective legislation. Subsequently, the differential association theory was extensively unpacked by making use of a practical example. Furthermore, the neutralisation theory was used to highlight how criminals engage in neutralisation techniques to rationalise their illicit activity. These criminological theories were paramount to guide the current study, as well as to root social engineering in a theoretical foundation.

The theoretical underpinning of the study was established in Chapters 1 to 4. These chapters set the tone for the rest of the chapters, as well as qualified the necessity for empirical evidence on the topic under investigation. Scientific studies are informed by research methodology and design, hence the next chapter will provide a substantial account of the research methodologies employed to conduct the empirical research.

CHAPTER 5

RESEARCH METHODOLOGY AND DESIGN

5.1 INTRODUCTION

The aim of this study is to explore, describe, explain and analyse social engineering attacks through a MIT approach in order to better understand, measure and explain such attacks as a means to formulate a protective strategy. In order to achieve this aim, clear guidelines for conducting the research had to be considered, applied and documented. The research methodology is the crux of any study, as it involves the techniques and procedures applied to investigate the topic at hand. In this chapter the researcher discusses the relevant research methods and data collection at length to demonstrate the realisation of the formulated aim and objectives (vide section 1.4).

5.2 PHILOSOPHICAL PERSPECTIVES

At the most foundational level, social knowledge is made up of concepts that provide the linkage to the social world. Thus, concepts incubate meaning as they facilitate the process of identifying and referring to social phenomena by describing and defining the main features of these phenomena. The use of concepts needs to be incorporated in sentences that either have semantic meanings (definitions) or epistemic knowledge (empirical findings). Nonetheless, the use of these concepts on their own would not suffice to understand and explain social phenomena. Conversely, these statements (concepts, definitions and empirical findings) need to be infused to create a comprehensive framework consisting of typologies, models and theories. Ultimately, this comprehensive framework can be developed into extensive theoretical or research paradigms (Mouton, 1998: 180). This process is demonstrated in the study at hand as the researcher incorporated both semantic statements/concepts and empirical findings to generate an integrative MIT social engineering model (vide Chapter 8 section 8.2). Certain factors

influence the decision to use specific research strategies. Philosophical perceptions on reality and the role taken on by the researcher will contour the methodological preferences employed by the researcher (Bachman & Schutt, 2014: 65).

5.2.1 Ontology and epistemology

The social sciences study facets of human society which include their behaviour, intercommunication and institutions (De Vos, Strydom, Schulze & Patel, 2011: 5). The researcher wanted the research problem to be clarified in the most truthful and representative way. In this way the transition of a research topic into a research design is developed (Fouché & Schurink, 2011: 308). Ontology is interested in unpacking the nature of reality and what there is to discern about aspects of the world (Ormston, Spencer, Barnard & Snape, 2014: 4). Epistemology entails the ways of knowing and learning about the world and draws the attention to how reality is learnt and what shapes the foundations of our knowledge (Ormston et al, 2014: 6).

Thus it is imperative that the researcher establishes the relevant ontology and epistemology regarding the research study, in order to understand the foundations of her thinking. Two questions emerge when establishing ontology and epistemology: “How should social reality be viewed?” and “What are the standards and rules by which reality should be known?” (Fouché & Schurink, 2011: 309). As aptly put by Tuli (2010: 99): “The selection of research methodology depends on the paradigm that guides the research activity, more specifically, beliefs about the nature of reality and humanity (ontology), the theory of knowledge that informs the research (epistemology), and how that knowledge may be gained (methodology).” The following epistemological approaches are discussed in order to explain the various epistemological positions that influenced the nature of this research study in an eclectic fashion.

5.2.1.1 Objectivism

Objectivism is a preeminent approach used in quantitative research; the basis of which lies in its belief that external reality can be studied objectively, similarly to the way natural sciences are studied. Objectivity is the aptitude to know things as they really are. If structured methods are applied to a research study, subjectivity and personal judgement will be minimised and even eradicated. Such methods and techniques executed in a research study permit the researcher to truly and objectively understand the meaning and significance people attach to their everyday experiences (Fouché & Schurink, 2011: 309). Tuli (2010: 100) elucidates that researchers interested in this perspective provide descriptions in quantitative language how variables interrelate, characterise events, elicit conclusions and influence the quantitative empirical research undertaken. The inherent nature of objectivism lies in Positivism and thus needs to be discussed accordingly.

Positivistic researchers acknowledge that reality is objective, separate to the perceptions and belief systems of those who observe it. Thus, science is needed to understand this reality. Positivism argues that there are existing universal laws of human behaviour and only once an objective and unbiased standpoint is adopted, can reality be clearly understood. This school of thought does concede that the knowledge of this reality is likely to never be complete (Bachman & Schutt, 2014: 65). Criminologists explain that positivistic research studies human phenomena through the use of traditional scientific methods. It emphasises objectivism, methodical observation, empirical evidence and deductive reasoning. Additionally, positivists investigate behaviour from a biological, psychological and sociological viewpoint (Williams & McShane, 2013: 34).

To gain a better understanding of the positivistic philosophy, with regard to conducting research, the following common assumptions are outlined as described by an integrated analysis according to Bachman and Schutt, (2014: 65); Siegel (2011: 10); as well as White and Haines (2004: 36):

- *Ideas are tested against empirical research without personal investment in a particular outcome.* Positivistic research needs to be tested as opposed to merely

reacting to phenomena. Also, this type of research should guard against consciously seeking for particular results.

- *Research is planned and executed systematically.* Careful planning and consideration need to be undertaken when testing ideas to ensure the most accurate results.
- *Procedures are documented and released for public viewing.* Researchers should disclose the methodology upon which their findings are based. This advocates against the construction of self-interested findings.
- *The clarification of assumptions.* Any research study relies on contextual assumptions. These assumptions need to be clearly clarified in order to promote validity of the study's conclusions.
- *The specification of terminology.* Words and concepts vary in meaning. Key concepts incorporated in a research study should be specified to promote mutual understanding.
- *The maintenance of a sceptical stance towards current knowledge.* The results of any research study should be critically examined. However, even if the study's results are duplicated and receive similar findings, researchers should consistently maintain a sense of scepticism about current knowledge, as the understanding of reality cannot be complete.

Furthermore, Bachman and Schutt (2014: 67) maintain that the goal of positivistic research is to advance knowledge. This can be achieved by publishing articles in academic journals as well as the presentation of findings at academic conferences.

5.2.1.2 Interpretivism

Interpretivism derived from research done by Weber (1864-1920) and Schütz (1899-1959) (Lewis-Beck, Bryman & Liao, 2004: 1). They wanted to study subjective phenomena objectively by constructing scientific and verifiable knowledge of the meanings that make up the social world. Consequently, they focused on the nature of meaningful social activity, its function in discerning paradigms of social life and the ways in which meanings can be determined. Approaches to social science which harness mutual ontological and epistemological assumptions are categorised under interpretivism (Lewis-Beck et al, 2004: 1).

Interpretivism assumes that the subject matter studied in social sciences is essentially and inherently different from that of the natural sciences. Accordingly, different methodology is required to acknowledge the subjective nuances of social action (Fouché & Schurink, 2011: 309). Davies and Francis (2011: 349) postulate that interpretivism inspects occurrences in their innate setting, unobstructed by the researcher. Any social phenomenon under investigation directly correlates with the social worlds which individuals occupy. These worlds and experiences have already been interpreted through the meanings individuals give them. These interpretations are regularly modified accordingly as the need arises. While the natural scientist assigns interpretations to the subject matter, the social scientist reviews phenomena that have already been interpreted (Lewis-Beck et al, 2004). Thus, interpretivists are not concerned with generalising a population, but rather with understanding the particular phenomenon under investigation (Tuli, 2010: 100). Furthermore, Tuli (2010) adds that interpretivism views daily reality as paramount, as described by the subject under investigation. To encapsulate the foundations of interpretivism, Ormston et al (2014: 12) describe the following key characteristics of it:

- Considerable attention is given to the meanings and interpretations the subject(s) allocate to their social world and reality.
- The research practice is principally inductive as interpretation is grounded in data, while observations are based on theories because they are facilitated by ideas and presumptions.

- Reality is affected by the research process; truths and standards are not divergent and objective research is impossible.
- Methodology used to study the natural sciences proves to be incompetent when applied to the social sciences, as society is not governed by legality but it is rather enabled through meaning and human agency.

Thus, social reality cannot be captured accurately and precisely because people hold different perceptions and understandings to what they see as truth.

▪ **Phenomenology and researcher reflexivity**

One of the main intellectual positions that influenced the interpretivist view has been phenomenology; a philosophy that is concerned with how humans make sense of the world in which they live, and researcher reflexivity (Bryman, 2012: 30).

The underpinning of phenomenology was founded by philosopher, Edmund Husserl (Bernard, 2013: 20). Husserl proposed that the scientific method appropriate for the study of physical science was unsuitable for the study of human reasoning and action. Alfred Schutz (Fouché & Schurink, 2011: 316) expanded on the work of Husserl by researching how the “real world” of subjects is established and experienced by them. In addition, Bernard (2013: 21) indicates that a phenomenological study aims to view reality through someone else’s eyes and to document the descriptions of those experiences rather than find explanations and causes. The essence of phenomenology revolves around its intention to understand the phenomenon being studied. Data retrieved are often presented in a relatively raw form to enhance their truthfulness.

In line with Hennik, Hutter and Bailey (2011: 19) reflexivity involves the cognisant decision of the researcher to introspect her own potential influence on the research process. This influence is rooted in a variety of ways including social background, personal assumptions, positioning and conduct. In this fashion, researchers should

continually engage in a process of close examination of their own role and actions in the research process. Additionally, the inclusion of reflexivity during the research process indicates that the researcher understands that she is part of the research respondents' social worlds. Hennik et al (2011: 20) go on to explain that reflexivity can be classified as personal or interpersonal. Personal reflexivity is the way in which researchers meditate on their own assumption, upbringing and traditions and how these can affect the research process, specifically the data collected. In this study, the researcher acknowledged that if she disclosed any of her own beliefs about the subject matter, personal reflexivity may be compromised as it could influence the research respondents' responses. Interpersonal reflexivity acknowledges that even the data collection setting and the social dynamics between the researcher and the research respondents can influence knowledge production. The researcher worked hard to gain good rapport with all the research respondents, as to avoid any discomfort and insensitivity. Additionally, researcher reflexivity is closely linked to bracketing, whereby the researcher's own biases are acknowledged and put aside in an effort to not infiltrate other people's encounters through her own cultural lens (Bernard, 2013: 21).

5.2.1.3 Social constructionism

While social constructionism bears a lot of resemblance to interpretivism, it differs distinctly in that it advocates that knowledge is actively and consciously constructed and created by human beings, rather than inertly being received by them. Both approaches discard the notion of neutral observations and general laws, but rather seek to comprehend lived experiences from the frame of reference of those who hold it (Ormston et al, 2014: 13). In essence, social constructionism maintains that there is no real world but only a narrative truth, as reality can only be known by those who experience it (Fouché & Schurink, 2011: 310).

5.2.1.4 Pragmatism

Pragmatism denotes a viewpoint that emerges from actions, circumstances and consequences as opposed to prior situations. It argues that research problems should focus on understanding the problem identified by adopting pluralistic research approaches instead of focusing on specific methods (Creswell, 2013: 10). In other words, research inquiries should focus on the research problem by finding methodological solutions to solve it, rather than trying to fit a research problem to one particular methodological instrument. Correspondingly, Munyua and Stilwell (2012: 25) collected evidence postulating that no research paradigm can solve a research problem on its own. Alternatively, pluralistic paradigms and methodologies are thus advocated for. Furthermore, it is proposed that research inquiries can employ facets of more than one paradigm to address the intricacies of social science research. In turn, the mixing of paradigms permits the use of various data collection methods as applicable to the study at hand.

It would be logical (but misleading) to assume that research should be directed by one particular methodological philosophy. However, complex research problems call for complex methodological solutions. Contemporary research is increasingly relying on mixed methods approaches to research, which are rooted in facets of positivism, interpretivism and constructivism (Bachman & Schutt, 2014: 67).

5.3 RESEARCH METHODOLOGY

Research methodology refers to the methods and tools the researcher employs to conduct and complete a research study (Babbie & Mouton, 2001: 74). In this way it can be characterised as being a map or blueprint of the study. In this section a narrative of the research approach and design will be explored. In addition, research procedures such as population and sampling techniques, unit of analysis, data collection and data analysis will be discussed.

5.3.1 Strategies of inquiry

Strategies of inquiry pertain to the types of qualitative, quantitative and mixed methods designs that are responsible for detailed direction of procedures in a research design (Creswell, 2013: 11). In real-life human sciences, qualitative and quantitative approaches are not mutually exclusive. The combination of elements from both of these approaches is referred to as a mixed methods research approach (Fouché & Delport, 2011: 433). Furthermore, Fouché and Delport (2011: 433) explain the differences in qualitative and quantitative approaches respectively. The former focuses on describing and understanding rather than the explanation and prediction of human behaviour; thus natural observation as opposed to a controlled measurement and the subjective exploration of reality rather than an outsider perspective, often associated with a quantitative model. Due to the necessity of encompassing all the important elements mentioned above in the research study at hand, the mixed methods approach proves itself to be the most appropriate for this study.

5.3.1.1 Qualitative research

The research study employed a qualitative approach to retrieve the knowledge and experience of research respondents on the subject matter. Qualitative researchers function as philosophers directed by abstract principles which are based on perceptions about ontology, epistemology and methodology (Denzin & Lincoln, 2003: 31). Qualitative research intends to examine people's habitual lives within their natural setting (Myers, 2009: 8).

As explained by Myers (2009: 30), qualitative research provides many beneficial outcomes. It allows the research respondents to share the meaning and understanding they have assigned to events, situations and experiences. It also assists in detecting unforeseen occurrences and influences, while cultivating fundamental explanations. Davies and Francis (2011: 23) explain qualitative research as an inquiry to describe, explore and investigate people's attitudes, motives and behaviours. Therefore, a qualitative approach to research was reasoned to be suitable for the study at hand, as

the researcher sought to enter the research respondents' perceptions of reality, truth and everyday experiences.

However, qualitative research by itself was not enough, as the researcher endeavoured to create an in-depth, comprehensive and holistic analysis of social engineering and its related aspects. Thus, the researcher also employed a quantitative research approach, which together with the qualitative approach culminated in a mixed methods approach. For this reason, the research approaches utilised in the study at hand need to be unpacked.

5.3.1.2 Quantitative research

Kumar (2005: 12) classifies quantitative research as a structured approach because all the elements of the research process are predetermined. Consequently, this approach is useful in determining the extent of a phenomenon. Quantitative research is used to examine trends and to explain relationships between variables. The questions posed to the research respondents are very specific and narrow (Creswell & Plano Clark, 2007: 255). Leedy and Ormrod (2005: 94) put forth the following characteristics of quantitative research:

- It provides explanations about the relationship between variables to enable the clarification, prediction and control of a phenomenon. In this way it establishes or authenticates relationships and generates generalisations.
- Due to its structured nature, concepts, variables, hypotheses and tools for measurement are usually demarcated before the commencement of the study and remain the same throughout.
- Objective research is promoted through the detachment from the research respondents in an effort to make unbiased conclusions and findings.

- Variables used in quantitative research are isolated and controlled by using standardised techniques to collect numerical data in order to produce statistical conclusions.
- It tends to be dependent on deductive reasoning by moving from generalisations towards specifications. This is achieved by beginning from a certain premise and thereafter construing logical conclusions from them.

In the present study, the quantitative and structured approach was represented in the gathering of data for statistical purposes in order to establish patterns and trends regarding social engineering.

As qualitative research is specifically focused on investigating meaning, it would appear that quantitative research is not concerned with extracting meaning from the data collected. On the contrary, within the scope of interpretivism, quantitative research derives meaning and insight from the variety of questions posed within the questionnaire administered. Thus, the gap between qualitative and quantitative research is not as big as it is often portrayed to be (Bryman, 2012: 617). However, both qualitative research and quantitative research are interested in what people do and what they think, but they undertake the investigation thereof differently (Bryman, 2012: 620). For these reasons, the present study decided to incorporate a mixed methods research approach, including qualitative and quantitative research.

5.3.1.3 Mixed methods research

The mixed methods approach involves the use of different research methods to study the same phenomenon. The rationale for merging the two research methodologies is that both can be used to better explore, describe, explain and analyse social engineering. Quantitative research makes provision for the researcher to undoubtedly aggregate,

compare, summarise and statistically analyse data. Qualitative research is useful for obtaining the descriptions of participants' behaviour as well as the content of their answers to interview questions (Fouché & Delport, 2011: 434). The following integration of literature is reflective of the value of mixed methods research (Bergman, 2008; Creswell & Plano Clark, 2007; Hanson, Creswell, Plano Clark, Petska & Creswell, 2005; Johnson & Onwuegbuzie, 2007; Teddlie & Tashakkori, 2009). These authors contend that mixed methods research:

- Makes provision for the verification and development of theory as it concurrently addresses a research problem.
- Often bridges the gaps that are found in both qualitative and quantitative approaches, thus producing enriched and comprehensive findings.
- Increases the possibilities of receiving divergent perspectives and uncovers the multifaceted nature of the research problem.
- Advocates the implementation and integration of multiple worldviews and archetypes, as it crosses the boundaries of those existing only in qualitative or quantitative research.
- Is practical, as all possible methods can be used to solve the research problem at hand.
- Eradicates various types of preconceptions, as it describes the true nature of a phenomenon and advances the study's validity and reliability.

Although mixed methods research is not a task which can be taken lightly, as it is time consuming, dependent on resources and requires a sophisticated skills-set, the researcher resolved that it was best suited to the current research study and implemented it accordingly.

A good research design proposes a comprehensive explanation of the planned procedures with such clarity that another researcher can easily follow and execute the

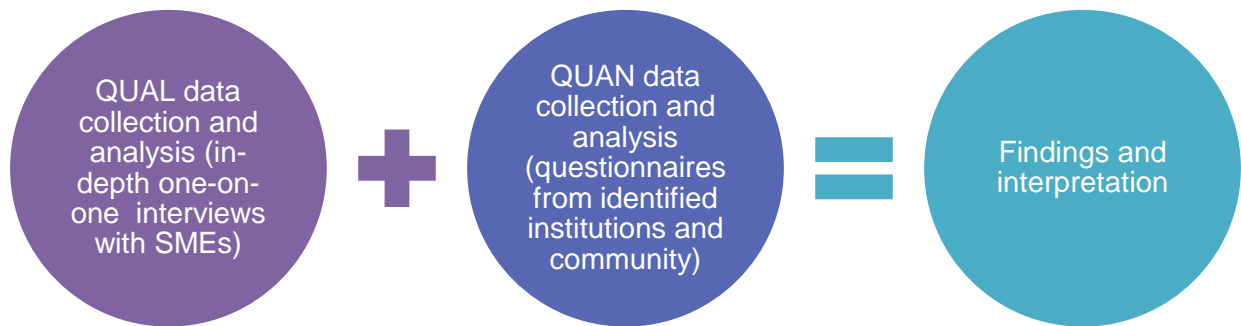
same steps (Kumar, 2005: 195). The present study will specifically make use of the exploratory mixed methods design. This design is used when the researcher first needs to explore a phenomenon using qualitative procedures, before endeavouring to measure and test it quantitatively. This two-phase design allows the results of the first phase to inform and provide direction to the second phase (Fouché & Delport, 2011: 441).

Theoretical data were first collected through an in-depth investigation of social engineering within its various disciplines. Empirical data were initially gathered through interviews with five Subject Matter Experts (SMEs) in the fields of criminology, security science, computer science, psychology and law. Furthermore, permission was obtained to conduct information security workshops at three business institutions. In addition, individuals within the greater Tshwane area were identified and an information questionnaire was distributed among 150 community members. In terms of the mixed methods approach, data were collected through a thorough literature review, complemented by questionnaires and one-on-one in-depth interviews.

By incorporating both qualitative and quantitative approaches in this study, the following benefits were achieved: triangulation (increases validity of the study); completeness (provides a comprehensive account of the topic under investigation); and credibility (combining the approaches enhances the integrity of the study) (Bryman, 2012: 633).

The illustration below depicts the process of exploratory mixed methods design as adapted from Fouché and Delport (2011: 441).

Figure 5.1: Exploratory mixed methods design



5.4 RESEARCH PROCEDURES

Research procedures refer to the sequence of actions taken during a research study. It embraces the selection of stages which need to be completed in order to produce academic research (Barkhuizen, 2004: 104). The following section presents the procedures undertaken when conducting the research study at hand.

5.4.1 Population and sampling techniques

A population consists of a set of entities which represent all the measurements of interest to the researcher (Delpont and Roestenburg, 2011: 193). A sample represents elements (or a subset of a population) which are identified to be included in the study (Strydom, 2011: 223). The next section is divided into qualitative and quantitative population and sampling techniques.

5.4.1.1 Qualitative population and sampling techniques

Since the researcher did not know the actual population size or the odds of selecting a particular individual (Strydom & Delport, 2011: 391), non-probability sampling was incorporated throughout the qualitative process. Within the constraints of non-probability sampling there are various types of sampling methods such as purposive, theoretical, deviant case, sequential, key informant and snowball sampling (Strydom & Delport, 2011: 392). The researcher focused on the two latter types of sampling techniques and used jointly in order to limit sample bias. Key informant sampling relies on community members as identified experts in the specific field of interest (Strydom & Delport, 2011: 394). The community in this case refers to the identified community of SMEs. The researcher also used key informant sampling to contact the SMEs by means of the academic research and literature they have produced, such as academic journals and dissertations. Once these initial community members were identified and located, the researcher used snowball sampling as a tool to request the SMEs to recommend other relevant participants who might add valuable input and knowledge to the study (Strydom & Delport, 2011: 393).

As the researcher is concerned with an integrated MIT perspective on the phenomenon of social engineering attacks, the researcher sought out SMEs who have a background and/or experience in the fields of criminology, security science, computer science, psychology and law. The researcher located five SMEs who were deemed competent to share valued expertise on a under researched topic in South Africa.

5.4.1.2 Quantitative population and sampling techniques

Quantitative sampling techniques pay attention to randomisation, representativeness and generalisability. Although quantitative sampling techniques focus on probability sampling, non-probability sampling is also employed in quantitative research (Strydom, 2011: 222) and thus the researcher made use of it. Strydom (2011: 223) explains that within the constraints of quantitative sampling, a population is referred to as the entirety of persons,

events, case records or organisation units. The present research study is interested in organisation units as well as individuals from Tshwane, Gauteng, as its population.

The researcher targeted small to medium institutions in which to conduct the relevant research. Purposive sampling was implemented, as the researcher relied on the willingness of business institutions to take part in the research study. This method is in line with purposive sampling, as the sample is composed of elements that contain the most representative qualities of the population that serve the objectives of the study best (Strydom, 2011: 232). The researcher sent out a request to conduct research in various business institutions which she thought may be willing to take part. This request was clearly formulated and sent out to 20 identified small to medium businesses. Once permission was received from the business institutions, the researcher distributed the group questionnaires (see Annexure F) to the personnel who attended the workshop. Thereafter, the researcher facilitated a presentation on information security and social engineering (Annexure G). Three business institutions responded to this request and subsequently allowed the researcher to conduct her research in their organisations.

For the purpose of gaining an individual perspective on and current awareness of social engineering and information security, the researcher conducted a questionnaire within the community of Tshwane located in Gauteng, South Africa. Convenience sampling was put into effect as it targets research respondents who are nearest and most easily available (Alston & Bowles, 2003: 87). Convenience sampling is beneficial when a researcher would like to extract prevailing attitudes from a certain population (Bachman & Schutt, 2014: 117). Research indicates that convenience sampling is often biased due to the over-representativeness of certain groups of people located in certain areas (Grinnel & Unrau, 2008: 355). However, in this research study this was not the case as respondents varied in age, race and in gender and were all part of the Tshwane community. In a comprehensive article written by Prinsloo (2008) the use of the self-appraisal questionnaire is examined. Prinsloo (2008: 4) finds value in this type of data collection technique as it accommodates individual reflection and introspection in comparison to a normative population. The research respondents who formed part of this identified community were asked to complete a questionnaire relating to information

security and social engineering (see Annexure F). A total of 114 research respondents completed the questionnaire satisfactorily.

There are two classifications of human behaviour and characteristics which can be observed: secondary verbal behaviour; and primary observable behaviour, (inclusive of individual behaviour, social interface and discernible characteristics) (Mouton, 1998: 142). Nonetheless, the validity of research results retrieved from either classification is vulnerable to human responsivity (Mouton 1998:143). In this way, researchers are attempting to control the research environment. However, it is difficult to research social phenomena, such as crime, in a controlled environment as the outcome of all the variables cannot always be equated (Prinsloo, 2008: 4). Furthermore, this is particularly evident when criminogenic factors are forced to adhere to social stratification processes which hinder any efforts to deal with elected variables randomly. Thus, even though some research respondents are selected randomly, the original variables cannot be allocated randomly as they have distinctive personal traits and qualities that are unrelated to the research question and are consequently allocated to specific groups by means of “self-selection” (Fitzgerald & Cox, 2002: 85; Newburn, 2007: 919).

In various social science disciplines, such as criminology, research designs accept the notion that representative samples are not a requirement for generalisation, as long as inductive generalisation and/or retroductive (logical reasoning that provides a comprehensive extension of the data collected) techniques are observed (Mouton 1998:81). In criterion-groups design, groups are randomly chosen from populations that are representative of the independent variable in order to compare the extent to which these groups differ (in terms of behaviour and characteristics) in relation to the dependent variable. The theory of probability suggests that objective degrees of implication are present among definite propositions grounded on probabilities that are considerate to the organisation of results as well as the evidence of frequencies of incidence (Prinsloo, 2008: 5). Subsequently, probability of generalisation increases through the process of induction (vide section 5.9.3).

5.4.2 Unit of analysis

The unit of analysis identifies the object of the study by specifying who or what the researcher seeks to draw conclusions about (Terre Blanche, Durheim & Painter, 2006: 41). Davies and Francis (2011: 48) contend that the unit of analysis entails data which are assembled on variables such as individuals, social communities, perspectives or events. In this study, the unit of analysis comprised each person who participated in the study, specifically referring to the SMEs and all the personnel of the identified business institutions, as well as each individual who took part in the information security questionnaire.

5.5 DATA COLLECTION

Data collection involves the means and methods of collecting data, as data represent the important material used by researchers. Valid conclusions can only be made from a research study if sound data have been appraised and interpreted. In this way, the true meaning of the research observations and explanations will be conveyed (Durrheim, 2006: 51). The subsequent section will provide a discussion on the applied means and methods of collecting data through the qualitative and quantitative processes.

5.5.1 Qualitative data collection

The research study pursued information from various experts and academics interested in the field of social engineering. These experts were located in different geographical areas, therefore innovative ways of interviewing were explored. The study made use of semi-structured one-on-one, telephonic and e-mail interviewing systems. The researcher conducted four one-on-one interviews and one telephonic interview, which was followed up by an e-mail interview. This was based on the time, convenience, location and preference of the research respondents.

- **The semi-structured one-on-one interview** (Annexure C – SMEs)

The qualitative approach to research allows the researcher to collect data through semi-structured one-on-one interviews (Greeff, 2011: 347). Furthermore, Greeff (2011: 351) explains that semi-structured interviews allow the researcher and participants flexibility during the interviews. The participants are at liberty to give a detailed description of the subject at hand, while the researcher will have a set of predetermined questions to guide the interviewer. In this way the research respondents in this study were allowed the liberty to raise interrelated themes that the researcher did not consider when designing the interview schedule. The researcher made use of semi-structured one-on-one interviews when interviewing the SMEs (Annexure C) when time, convenience and distance allowed, while gaining insight and knowledge from their specific fields.

- **The telephonic interview** (Annexure C – SMEs)

Historically, telephonic interviews were negatively perceived by professional researchers as producing a social class bias, since few people owned telephones (Babbie, 2010: 279). However, the growth of technology concerning both landlines and cell phones has ruled out this concern as accessibility and availability have increased. So much so that in 2013, the United Nations reported that globally, more people have access to mobile phones than working toilets (Wang, 2013). The telephonic interview was deemed as an appropriate method of collecting data from SMEs as it is affordable, convenient and non-intrusive (Greeff, 2011: 356). Moreover, it eliminated travelling costs as well as geographical constraints and all questions were answered and clarified satisfactorily. However, limitations of this type of interviewing were noted by the researcher. These included difficulty in establishing rapport and the duration of the interviews seemed to be shorter than for the one-on-one interviews.

- **The e-mail interview** (Annexure C – SMEs)

The use of e-mail communication has been extensively used for more than a decade, although its use as a data collection tool is limited (Hunt and McHale, 2008: 1420). In contemporary research studies such as Deyzel (2014), Liebenberg (2008), Mphidi (2015), and Sissing (2013), e-mail interviews were effectively administered. An e-mail

interview involves online communication exchange in which a virtual and transcribed conversation occurs (Sissing, 2013: 25). The interactions between the researcher and e-mail respondents are asynchronous, as they often do not take place during real time (Bampton & Cowton, 2002). The researcher in this study provided particular guidelines for the interview, which included the duration of the interviews, anonymity and confidentiality, and suggested response time. Respondents were asked to make their responses as comprehensive as possible to aid the data collection process.

5.5.2 Quantitative data collection

Information security, and more specifically social engineering, affects business institutions and the individual. For this reason the researcher decided to expand her research focus to include individuals and business institutions, as both units are vulnerable to data breaches. The researcher used structured questionnaires to collect data from these populations.

5.5.2.1 Questionnaires

Quantitative data collection relies on measuring instruments such as checklists, indexes, scales and questionnaires (Delport & Roestenburg, 2011: 171). Although the research study employed questionnaires (group-administered and self-administered) as a measuring instrument, the questionnaire was constructed qualitatively. This was to overcome logistical challenges while still sourcing comprehensive and descriptive data from the research respondents.

- **Group-administered questionnaires** (Annexure F – businesses)

The researcher received permission from three small to medium business institutions to conduct research in their institutions. The session started with the distribution of group-administered questionnaires to the research respondents (see Annexure F). The research respondents completed the questionnaire concurrently. The participants were asked not to discuss or share their answers but rather to complete the

questionnaire individually. Clear verbal and written instructions were given to the research respondents on how to complete the questionnaire. As supported by Delport and Roestenburg (2011: 189) this method works well in a workplace setting, as arranging respondents in a group setting is made easier. Thereafter, a presentation (see Annexure G) was made by the researcher to all the personnel present. This presentation focused on issues of information security and social engineering in an effort to create awareness in a work environment. In this way, the research study was beneficial to both the researcher and the research respondents.

- **Self-administered questionnaires** (Annexure I – individuals)

As clarified by Delport and Roestenburg (2011: 188) and put into practice by the researcher, the research respondents completed the self-administered questionnaires by themselves, although the researcher was available to answer any questions that arose. Nonetheless, the researcher kept her contribution to the completion of the questionnaire to the bare minimum. Instead, the researcher functioned as a means of encouragement towards completion by continually emphasising the importance of the research respondents' contributions. The researcher approached each research respondent personally, explaining the research study's purpose as well as the research respondent's role in the study. This was also formally explained on the questionnaire (see Annexure I). Subsequently, permission was granted and 114 research respondents completed the questionnaire satisfactorily.

5.6 DATA ANALYSIS AND INTERPRETATION

The process of organising and manipulating data in order to develop findings, interpretations and recommendations, is known as data analysis. Furthermore, it involves the creation of order, formation and meaning to the mass of information gathered (Schurink, Fouché & De Vos, 2011: 397). In addition, Henning, Van Rensburg and Smit (2004:128) maintain that explanations, interpretations and predictions are crucial. It is during this stage of research where the researcher attempts to answer the how, why and

what questions of the study. Mouton (1998: 161) describes analysis as the process of fragmenting a complex whole into smaller parts.

Content analysis was used to analyse and interpret the data collected from the qualitative interviews with the SMEs (Schurink et al, 2011: 401). To a large extent, crime and criminality are portrayed through media coverage such as newspapers, television and social network sites. However, to what extent is this coverage valid and reliable? Content analysis provides assistance in this regard, as it is a research method used for the systematic analysis and interpretations from text. This research method is useful as it provides insight into popular culture by evaluating the content of the communication shared through the mass media. However, this representation of crime can be over-exaggerated, inaccurate and misleading (Bachman & Schutt, 2014: 293). The current study referenced various media sources, because the phenomenon – identification and understanding of social engineering – is relatively new. Recent attention has been given to the phenomenon as information security breaches continue to escalate (vide Chapter 2). The study was impelled to investigate the topic at hand by infusing literature and empirical findings.

The researcher used the following coding processes when analysing the data retrieved, as outlined by Schurink et al (2011: 412):

- *Open coding*: The data retrieved were categorised and disseminated through a process of comparison, conceptualisation and examination.
- *Axial coding*: The data were then synthesised in a new way through the identification of relationships, themes and patterns.
- *Selective coding*: A central theme was found which could explain the relationships, themes and patterns found in the prior stages. Thereafter, the data could form the basis of the model (vide section 8.2).

The researcher systematically read through the data collected and grouped the data according to various themes. Data were analysed, interpreted, compared and integrated as it had been collected through different perceptions and fields of study. With regard to the quantitative approach to research, descriptive analysis was used to analyse the data. Thus, the data were analysed statistically, making use of tables and graphs to interpret the data collected (Fouché & Bartley, 2011, 248). This was done through a spreadsheet program - Microsoft Excel. Inclusive of the mixed methods methodology, the questionnaires consisted of qualitative components. In addition, the use of data triangulation, as adapted from the mixed methods methodology, was employed to make comparisons and to integrate the findings from both qualitative and quantitative data (Fouché & Delport, 2011: 442).

5.7 PILOT STUDY

A pilot study is a means for testing and validating the research instrument by administering it in a small group of participants in the proposed test population (Strydom, 2011: 237). Persuad (2010: 1033) explains that a pilot study is useful in that it can alert the researcher of any possible problems associated with the proposed methodology. A pilot study can also inform the researcher on any possible failures and potential modifications that need to be made to achieve the intended outcomes, as well as also to expose other problems that might affect the research study. Consequently, a pilot study increases the probability of success in the actual study.

The researcher conducted a pilot study for both the qualitative and quantitative research. With regard to the qualitative research approach, executing a pilot study was deemed important as this means of data collection formed the basis of the study. The researcher piloted the study by interviewing a few local SMEs to test the validity and reliability of the interview, as well as a means to evaluate the relevance of the content with regard to the aim and objectives of the study. These interviews were included in the final study. The researcher also piloted the quantitative research by distributing questionnaires to a few

respondents. These questionnaires also formed part of the final study. Issues that arose during both pilot studies were rectified before the real study was conducted.

In light of the detailed research methodology discussed above, the researcher needs to ensure validity, reliability and accuracy of the empirical data collected.

5.8 VALIDITY, RELIABILITY AND ACCURACY OF COLLECTED INFORMATION

In order to promote the validity, reliability and accuracy of the collected information, the researcher took the following into consideration: ensuring validity and reliability, deductive and inductive reasoning and data triangulation.

5.8.1 Ensuring validity

Validity accentuates whether the conclusions the researcher makes are credible for the specific context and time period under investigation. Furthermore, it is believed among social science researchers that findings and interpretations are neither right nor wrong – only more or less credible (Davies & Francis, 2011: 12). Within the qualitative research process, the researcher compiled an interview schedule made up of semi-structured questions which were answered by the identified SMEs. By using open-ended questions, the researcher gathered as much information as possible. Moreover, the researcher was cautious to ask questions which were not leading. By following the in-depth means of quantitative data collection discussed in section 5.5.1, as well as only using open-ended questions and the same list of questions for each participant, validity of the study was ensured. Validity was further strengthened by submitting the interview schedule and questionnaires to the researcher's supervisor, experienced colleagues and UNISA College of Law Ethics Committee for comments and input.

To ensure validity when conducting the quantitative research, the following was taken into consideration:

- **Face validity** determines the extent to which the data instrument measures what it intended to measure (Bachman & Schutt, 2014: 86; Delport & Roestenburg, 2011: 173). The questions contained in the questionnaires (see Annexure E and Annexure H) set out to determine the current criminogenic risk faced by the research respondents.
- **Content validity** sufficiently covers a variety of elements of the phenomenon under study (Bachman & Schutt, 2014: 86; Delport & Roestenburg, 2011: 173). The questionnaires were designed to cover a wide range of elements pertaining to social engineering.
- **Construct validity** is established when the measuring instrument is linked to an underlying theory (Bachman & Schutt, 2014: 87; Delport & Roestenburg, 2011: 173). The study was influenced and underpinned by criminological theories as discussed in detail in Chapter 4 (vide Chapter 4).

5.8.2 Ensuring reliability

Davies and Francis (2011: 353) explain that the reliability of data depends on the extent to which concepts and measures are well explained, consistent and repeatable. The results of this research study are considered to be reliable because the sample comprised people who have extensive knowledge of the topic at hand. Accordingly, the SMEs were able to provide the researcher with the necessary knowledge to achieve reliable findings for the research. The researcher engaged in a process of reflexivity in order to dismiss her own bias. Bracketing (setting aside of personal assumptions and beliefs) was done by making notes during the data collection and analysis phase. This was done in order to reflect upon the interaction with data.

Through the information security workshops as well as the use of questionnaires, reliable research data were collected as the same techniques and procedures were used to yield similar results. Additionally, in an effort to ensure reliability, the findings of both the

qualitative and quantitative research methodology were compared, interpreted and integrated through the process of triangulation (Fouché & Delport, 2011: 442).

5.8.3 Deductive and inductive reasoning

Deductive reasoning is a thinking pattern whereby the conclusions which are made are generated from the original premise. Thus, the conclusion is already contained in the original premise. Inductive reasoning allows for the possibility of various conclusions to be made, not necessarily as generated from the original premise. Accordingly, within a deductive argument, true premises create true conclusions, while within an inductive argument genuine auxiliary evidence merely leads to highly plausible conclusions (Mouton, 1998: 77).

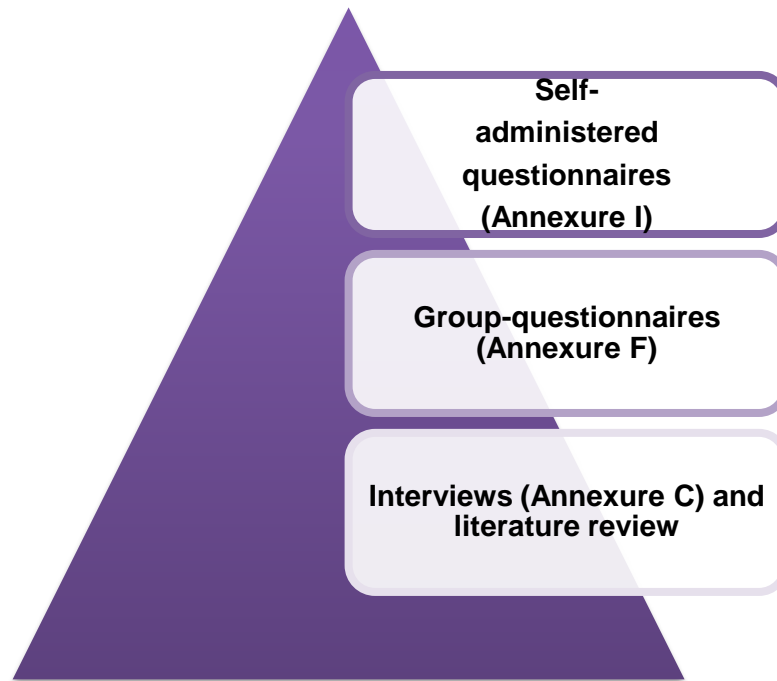
Induction makes broad generalisations from specific observations; from concrete observations to a universal theoretical explanation. In this way, inductive reasoning begins with observation (Delport & De Vos, 2011: 49). In accordance with Leedy and Ormrod (2005: 32) specific examples and occurrences are used to draw assumptions about entire objects or events. Customarily, a sample is drawn and conclusions are made about the population from which the sample originates. The researcher thus begins the research with a general topic and then works towards refining it by categorising it into theoretical concepts. Induction encourages creative reasoning where knowledge can be modified and refined, causing conclusions to be merely tentative and possible (Neuman, 2006: 60). The study at hand followed inductive reasoning when making conclusions about the data received.

5.8.4 Data triangulation

By making use of a mixed methods approach, data triangulation has been achieved as data were collected in three ways to achieve mutual collaboration; firstly from SMEs (Annexure C) who formed the foundation of the study by offering their expertise on social engineering and its related aspects. This was combined with current literature on the topic

at hand. Secondly, data were collected from small to medium businesses (Annexure F) to shed light on social engineering in the workplace. Finally, to gain insight into the nature and impact social engineering has on individuals, data were collected accordingly (Annexure I). The process of data triangulation is depicted below.

Figure 5.2: Data triangulation



In addition to ensuring validity and reliability, the researcher needed to explore all the possible ethical considerations involved in the study.

5.9 ETHICAL CONSIDERATIONS

The most commonly accepted definition for “ethics” describes the norms and standards put into place to guide the process of distinguishing between acceptable and unacceptable behaviour (Resnik, 2011: 1). Furthermore, Resnik (2011:1) denotes ethics as the methods, procedures or perspectives involved in deciding what to do when investigating complex problems. Davies and Francis (2011: 283) convey that ethics are the guidelines of mandatory conduct carried out during research. It involves the moral beliefs and behavioural anticipations observed by researchers when engaging with other people, as the objective is to avoid harm (Bezuidenhout, 2011: 53).

Research should be founded on mutual trust, acceptance, participation and known expectations between all the parties involved in a research study (Strydom, 2011: 113). Since human beings are the focus of social science research, and specifically of the study at hand, ethical considerations are raised here. Gravetter and Forzano (2003: 60) advocate two types of responsibilities a researcher has in relation to ethics. First, the researcher has a responsibility to human and living beings who participate in a research study, and secondly a responsibility to the discipline of science with regard to reporting accurate and truthful findings. The following ethical concerns were considered and applied during the research study at hand.

5.9.1 Informed consent

Informed consent involves providing the research respondents with all the necessary information to assist them in their decision on whether or not to participate in the study (Barlow & Durand, 2009: 116). A comprehensive letter of informed consent was drafted and distributed to all the participants involved in the study (see Annexures B, E and H). This letter included the aim and objectives of the study, the anticipated duration of the research respondents' involvement in the study, the procedures that will be adhered to during the interviews and questionnaires, as well as the credibility of the researcher (Strydom, 2011: 117). Additionally, the letter of consent contained a section on voluntary participation and no harm to participants. It was also conveyed verbally and in writing that the research respondents have a right to withdraw from the study at any time, as well as to raise any questions or concerns pertaining to the study with the researcher. Moreover, if desired, the participants were guaranteed confidentiality. However, no names were requested from the research respondents who took part in the questionnaires. During the interviews, the researcher requested permission to use a tape recorder for accurate documentation and consent was received.

5.9.2 Voluntary participation

Participation in a research study should not be forced but rather be voluntary (Babbie, 2007: 67). In this study, all the research respondents were made aware of their individual right to choose to participate. This decision was entirely up to them and none of the research respondents were made to feel pressured to participate in the study.

5.9.3 Compensation

The researcher provided no physical or tangible compensation to any of the research respondents who chose to take part in the study, as a means of avoiding any ulterior motives by the participants. However, as anticipated, the researcher found that the mutual passion for academic knowledge that the SMEs and the researcher shared acted as a motivating factor for participation. On the other hand, the research respondents who completed the questionnaires were continuously thanked by the researcher for their participation in the study.

5.9.4 No deception of participants

According to Struwig and Stead (2001: 69) deception involves the misleading of participants by withholding information from them. There was no need for any form of deception during the research study at hand. The aim and objectives of the study were made clear to all of the research respondents involved by means of Annexures B, E and H.

5.9.5 Privacy, anonymity and confidentiality

Privacy is the capacity of an individual to selectively decide what information and aspects of their lives they are prepared to disclose (Strydom, 2011: 119). All of the research respondents have a right to privacy and were informed of the procedures involved in

ensuring that this principle would not be breached in any way. Confidentiality advocates the managing of information in a trustworthy way and is seen as an extension of privacy (Babbie, 2007: 65). The research respondents were assured that their contributions to the research study would be treated in a confidential manner.

5.9.6 Publication of the findings

A research study will have little to no meaning or value if it is not documented and recorded in an official manner available for public viewing. A written report of the research study should be clear and comprehensive to ensure that the reader knows exactly how the research was undertaken. It is ethically necessary to report accurate findings to avoid any deception, as other researchers might rely on the findings for their own research (Strydom, 2011: 126). The informed consent letter (see Annexures B, E and H) stipulated that the findings of the research will only be made public for statistical purposes and the name, affiliations or personnel of the organisation will not be publicised. As suggested by Bless et al (2006: 145), the research respondents were briefly informed about the findings of the study, bearing in mind issues surrounding confidentiality. In this way, the researcher acknowledged recognition of the involvement of the research respondents and maintains good relationships with all the stakeholders involved.

Often ethical conduct is formally addressed by means of professional codes of conduct (Davies & Francis, 2011: 283). The University of South Africa adheres to ethical considerations through its policy on research ethics (Unisa, 2007). The research study received ethical clearance (see Annexure A) from the College of Law Ethics Committee before the commencement of the empirical research.

5.10 CONCLUSION

The processes involved in conducting research function as the core of any research study. It is, therefore, of vital importance to explore, apply and document these processes clearly and systematically. This study was embedded in philosophical perspectives by

exploring the ontology and epistemology employed by the researcher. In order to successfully achieve the study's aim and objectives, the researcher used the mixed methods research approach by incorporating qualitative and quantitative strategies of inquiry. The researcher used non-probability sampling to extract sample groups. Semi-structured one-on-one interviews and qualitative questionnaires were used to gather data. The chapter provides a discussion on the strategies used to analyse and interpret data, which include content and descriptive analysis. In any research study, the assurance of validity and reliability is a key component. The components of validity and reliability were ensured by making use of deductive and inductive reasoning as well as through data triangulation. The research went to great lengths to ensure that the ethical considerations listed in the chapter were observed.

This chapter is paramount in directing the succeeding chapters (Chapters 6 and 7) in a methodological way in an effort to ensure the scientific validity and reliability of the empirical research undertaken.

CHAPTER 6

ANALYSIS AND INTERPRETATION OF DATA: A SUBJECT MATTER EXPERT AND BUSINESS PERSPECTIVE

6.1 INTRODUCTION

The current chapter should be viewed in conjunction with Chapters 3 and 4, as it is an extension of the data gathering process conducted on the topic at hand. These chapters form the foundation of the study, as illustrated in the triangulation of data depicted in Chapter 5 (vide figure 5.2, section 5.8.4). In this way, theoretical and empirical data are gathered to explore the phenomenon of social engineering.

As the current study is directed by its aims and objectives, this chapter seeks to achieve the following objectives:

- To explore and describe the occurrence and nature of social engineering attacks.
- To explore and describe the awareness of social engineering attacks and information security.
- To analyse and explain the contextual role of social engineering attacks within the various disciplines through MIT research.

This chapter provides an analysis of the data received from the SMEs as well as the businesses. The chapter will be divided into two main parts: Parts I and Part II. In terms of Part I the following themes will be discussed, in light of the responses received from the SMEs: the definition and occurrence of social engineering; vulnerable groups; the profile of a social engineer; and the types of social engineering attacks encountered. In addition, the impact that social engineering has on businesses and individuals is explored as well as the human element involved in maintaining a healthy information security

culture. Finally, legislative concerns regarding social engineering will be reviewed. Part II comprises the probable vulnerabilities, risks and consequences associated with social engineering attacks. The researcher embarked on uncovering these vulnerabilities, risks and consequences within a South African business context.

PART I: A SUBJECT MATTER EXPERT PERSPECTIVE

6.2 ANALYSIS AND INTERPRETATION OF SEMI-STRUCTURED ONE-ON-ONE INTERVIEWS

As informed by section 5.4 (vide Chapter 5), the researcher used key informant and snowball sampling to retrieve SMEs. The interviews were held between the months of April to June 2016. The sample consisted of three SMEs who specialise in information security, one SME whose research is based on an IT and psychological perspective on social engineering, and the final SME who is knowledgeable in legislative matters relating to information security. The research respondents requested that their anonymity be maintained and thus pseudonyms are used. The research respondents will be referred to as Research Respondent A to E (i.e. RRA, RRB, RRC, RRD and RRE). The data were collected through face-to-face interviews and one telephonic interview, which was followed by an e-mail interview (vide Chapter 5, section 5.5.1). A semi-structured interview schedule (vide Annexure C) was used as a guideline to interview the SMEs.

6.2.1 Defining social engineering

The phenomenon of social engineering was unpacked in section 2.3 (vide Chapter 2). The researcher was interested in how the SMEs would define social engineering, especially in a practical and operational context. Some of their verbatim responses are highlighted in the following extracts:

RRA: *“Social Engineering is where somebody would try to get information, about you, that’s going to help them either get into your account or get certain information. For*

example a phishing attack that is trending around the departments is the sending of e-mails that say please can you click on this link to approve a payment. The e-mail looks like it comes from their colleagues within the organisation but it is actually not. When you click on the link and then approve the payment, you are actually logging into a potentially fake website, where your username and your password are captured. And then they can actually use that to get a record of what the password is so that they can potentially log in themselves to do that. Social engineering is a way to get information about you and use it to the attacker's advantage."

RRB provided a more psychological definition of social engineering:

RRB: "I understand social engineering to be when people manipulate someone's inherent, trusting nature. As humans we are all kind of trusting to some degree. Social engineering is employing different tactics, to play on our trust and to get information, without us realising that we are disseminating potentially sensitive information."

Furthermore, RRC described social engineering as

RRC: "...manipulating a user to bypass security channels".

For the purpose of the current study, in essence, social engineering denotes the use of manipulative and deceptive techniques against human nature in order to access sensitive and confidential information as a means to achieve some sort of illegal action or omission of action.

6.2.2 Occurrence of social engineering

The researcher sought to establish the prominence of social engineering as perceived and experienced by the SMEs.

RRA: "It's definitely prominent, because when we do our IT security reviews, we look into a lot of technologies to see if there is good technology in place. But ultimately, you can

have great technology, you can have fire walls, you can have intrusion detection systems, you can have everything, but if your people are not aware of scams that are going out there, then it's probably the easiest way for any attacker to get in."

RRD: "We do penetration testing and part of it is social engineering penetration testing. We try to penetrate the human element and we regularly find flaws by probing on the human element to get into organisations. It's mostly due to a lack of policies and procedures and people not being aware of these policies and procedures."

This draws attention to the importance of clear policies and procedures pertaining to information security. However, employees should be adequately trained in terms of knowledge and application of these policies and procedures. Penetration testing exceeds vulnerability testing, as it involves simulated attacks by "malicious" external mediums which evaluate and test existing security structures (Whitman & Mattord, 2012: 529).

RRB noted that the biggest problem regarding social engineering is unawareness, as illustrated in the following excerpt:

RRB: "I think it's probably very much on the rise and I think the ability of most companies or people to realise that they've been socially engineered is probably the big problem, so we'll never really get an accurate [assessment] until the awareness of people increases. I do think it's on the rise because it's the easiest way to get information from a company or individual."

RRA also described attacks happening throughout various government departments currently trending in the news. He conveyed that due to the increasing nature of social engineering attacks, his organisation offers a service to conduct social engineering audits on institutions to test their information security. Furthermore, he shared that not only are his clients serviced with awareness training, but the institution itself takes such threats and attacks very seriously. This is substantiated through e-learning, information training and constant notifications and alerts of new social engineering attacks. RRB added to this

by acknowledging the alarming need for training and awareness for individuals and businesses to ensure effective information security. In addition, RRC explained that his organisation conducts social engineering audits for various companies and he has yet to find a client that has not succumbed to a social engineering attack. These social engineering audits take place in an online and offline context.

6.2.3 Vulnerable groups

RRA, RRB, RRC and RRD maintained that all people are vulnerable to social engineering attacks. This is highlighted through the following responses:

RRA: “People who are just not aware of secure information security. It could be older people or just people within. We do a lot of government work and I think some of the people within government aren’t aware of these things. Generally, any person that doesn’t know much about IT is probably vulnerable to this because they are not aware of the risks that are involved.”

RRD: “Almost everyone is vulnerable. There’s no limitation. You can’t ever say you are not vulnerable to an attack. If the attacker puts enough effort into his attack, he is able to manipulate you at the correct specified moment, when you are psychologically vulnerable to the attack and then you can potentially fall prey to such an attack.”

RRB noted that everyone is vulnerable to social engineering attacks, especially those who are uninformed. She said not only has she been exposed to such attacks, but so have family and friends as well as clients. As discussed in Chapter 2 of the current study, RRB mentioned whaling as a popular phishing scam circulating throughout organisations (vide section 2.6.1).

6.2.4 Profile of a social engineer

There are limited academic research studies available to provide a comprehensive profile of a social engineer. Alternatively, research (vide section 2.6) relies on a broad discussion of what constitutes as a social engineer. RRA and RRB shared their sentiments:

RRA: “Somebody who just wants to get an advantage, who has an agenda and wants to try and get extra information. The person would need to have good IT knowledge and wants a way to just get a financial advantage.”

RRB: “From a security and a hacking perspective, it would be any type of hacker, syndicate or maybe even a disgruntled employee that wants to get some information, and they know who to get it through. Actually, anyone that wants to get information from a company and use it for malicious intent is at risk.”

RRD: “In a malicious social engineering attack, the black hackers try to get financial gain or unauthorised access to an organisation for financial gain from an organisation. Social engineering in the good perspective is when you perform penetration testing - those are your whiteout hackers. That’s when you go into a company and try out the offensive techniques, to gain information from the company, but you report immediately back on how to patch the vulnerabilities and how people can be better educated, to be more vigilant against it.”

6.2.5 Types of social engineering attacks

The typology of social engineering attacks is discussed under the *modus operandi* of a social engineer in Chapter 2 (vide section 2.6.1). These can be seen as techniques used in order to carry out a social engineering attack. These attacks can occur in an online and offline context, as the main objective of an attack is to achieve the initial goal – be it access to sensitive information or financial gain. Consequently, as long as the end-goal is achieved, the means are simply a method of ascertaining it.

RRA mentioned that he had mostly seen phishing and spoofing attacks take place within his organisation and that of his clients. RRB discussed human-based social engineering attacks such as shoulder surfing and tailgating. This is illustrated in the following extract:

RRB: "...people just walking into buildings and shoulder surfing and tailgating. That's, another big risk, you sometimes just get random people walking around and it can lead to cell phones and actual hard copies of information being stolen."

6.2.6 The impact of social engineering on businesses

The SMEs were asked to describe the prospective impact of social engineering on businesses. RRA and RRB maintained that a successful social engineering attack would have huge financial and reputational consequences for any institution. Several mechanisms for businesses to safeguard themselves against social engineering attacks were suggested.

RRA, RRB, RRC and RRD emphasised the value of awareness training and penetration testing. RRA noted that many of the companies that he had audited ran information security awareness sessions. However, he estimated that about one per cent of the organisation will attend that specific training session, thus minimising the impact. He relayed that this shows that people are not taking information security seriously and his institution recommends that awareness training is made compulsory. RRA suggested that one of the best ways to provide training is to make it more practical. This will include conducting social engineering audits and penetration testing to show the institution where their risks and vulnerabilities lie. Additionally, RRA upheld that information security would most likely be breached and thus proper procedures and protocols should be designed, implemented and followed when such a breach takes place. Furthermore, RRD emphasised the importance of customised social engineering penetration testing. The penetration testing should be developed for the specific institution. After the penetration tests have been conducted, the results should be released without revealing the names of those who were vulnerable to the attacks.

Important to note, as explained by RRD, awareness campaigns alone do not suffice to guard against social engineering attacks. He explains this in the following extract:

RRD: "...you can train people to be aware of social engineering, but it doesn't mean they'll always be vigilant against it, one needs a more constant process where a whole mind set is changed in terms of thinking about a request to be really vigilant against social engineering."

RRB proposed that businesses should protect themselves against social engineering attacks through two elements. First, through strong technical controls; this will defend the perimeter and ensure that the right detection tools are in place to prevent attacks from coming in. However, not all information security breaches can be prevented. Thus, user awareness training is advised. RRC recommends that there should be consistent computer control in terms of job relation in key controls. In other words, only authorised persons should have access to certain information.

6.2.7 The impact of social engineering on individuals

The SMEs were asked to outline the potential impact of social engineering on individuals. Some of their responses are reflected below:

RRA: "The key thing is that most of the information is potentially sitting at organisations, and the client does not know to what extent that information is being protected. I think a lot of the general public probably isn't very aware of social engineering and they take it lightly. I don't think they realise the risks and implications of this. The known things that are being targeted in the public are attacks like the tax and banking scams."

RRD: "At any given moment if you receive communication that you need to perform an action based on something you are expecting to perform, the chances and likelihood of you performing the action is quite high. This is because it's more like a short circuit process in your brain as you know you are expected to perform this. You receive a request

to perform the action and then you immediately perform it without really thinking about it. So the public and businesses are equally vulnerable to it. It's just the companies are higher value targets to penetrate whereas some members of the public are lower value targets."

RRB raised an interesting perspective regarding the impact of social engineering on individuals as compared to businesses. This is summed up in the following extract:

RRB: "In a company you normally have network security measures in place that can mitigate some of the attacks. Thus, some of them will block phishing e-mails or spam e-mails. But if you are at home and you're not behind a firewall, the risk is much greater, so you could be downloading all sorts of malware onto a personal device which will not filter out information."

RRB further asserted that there is not much assistance for victims of social engineering attacks, as compared to when an attack happens on a larger scale such as in a company. RRB concurred with this as she asserted that the responsibility is on each individual to make sure that they are protected against social engineering attacks. She explained this in the following extract:

RRB: "...ultimately the onus is on yourself as a person, given that the way the world is changing and with the exposure to technology and the security risks we all face every day, I think the person's own responsibility is to become as aware as possible, and to find the avenues that will allow them to become aware."

In the case of individuals, RRA, RRB, RRC and RRD also strongly supported the value of awareness training among the public. RRA encouraged individuals to be more aware and alert and they should rather do verification and authentication tests before relying on links, e-mails or SMSs. Awareness campaigns should begin in schools and at universities.

6.2.8 Human element in information security

RRA shared that the human element is probably the biggest vulnerability in information security. He provided an example of an institution where it was evident that all the IT controls, firewalls and web servers were of exceptional quality and standard. However, he would overhear staff members sharing passwords in the corridors. He argued: “What use is good security technology when humans are easily sharing sensitive information?” He highlighted this through the following extract:

RRA: “...it’s a serious risk and I think people don’t understand it because ultimately if I’m sharing my user name and password with you that means that you can log in as me and do everything as me. I should be held accountable for that. How can I be comfortable to give another person that access to be able to do this?”

RRB sustained that information security is made up of a triangle: people, process, technology. This is expressed in the following extract:

RRB: “...you can have the best technology in place and you can have the best processes in place, but your people will be your weakest link. If they don’t use the technology and they bypass processes, these elements are worthless. People will always be the weakest link in information security, no matter what.”

Based on RRC’s operational experience he identified the following vulnerable persons susceptible to social engineering attacks: people hesitant to resist authority; people who are desperate; and disgruntled individuals.

RRD took an interesting stance on the human element in information security, drawing from his psychological and computer science background. He shared this insight through the following explanation:

RRD: *“...human susceptibility is something you cannot physically go out and patch. With normal computerised systems you can apply the latest patches and you can fix them up. This is something that cannot be done to humans. You need to educate them and there’s still always the human element, you can educate someone all you like and you can train them to use a certain tool and say this tool must always be used. However, if you are in a vulnerable emotional state, your ability to reason immediately drops and as soon as your ability to reason drops, you immediately start becoming more vulnerable to social engineering attacks. The human element is always something where flaws can mostly be found. Also, if you’re an already established organisation, you turn back to the unintentional insider threat, where you’re already in the organisation, people know you, there’s a trust relationship built up. You can exploit that trust relationship of the people because then they also tend to disregard the processes and procedures.”*

A security patch entails a software security update designed to cover vulnerabilities that have been exposed since the programme was launched (Ciampa, 2014: 89). RRD notes that humans cannot be easily “patched” in the same way as computer systems.

6.2.9 Legislation

A common theme extracted from the interview with RRE is that it is a challenge for legislation to regulate technology, as technology continuously changes. He also identifies the challenges faced at grass roots level. If the South African Police Service (SAPS) is not aware of legislation, how can reports be made on social engineering attacks?

RRA noted that some South African companies have international head offices and would most likely have guidelines directed by the PoPI Act already in place. Therefore, such transitions would be fairly simple. However, local companies would find it more difficult to adhere to the regulations as they have not done it in the past. He further sustained that PoPI legislation will have financial and reputational consequences for a company, but

once put into proper affect it will be effective. It will give individuals the right to insist that their information be kept confidential.

RRB questioned the effectiveness of current legislation, as explained in the following quotation:

RRB: “It’s all good and well for them to come up with the legislation around it like PoPI and Cybercrimes and Cybersecurity Bill, but until they put in the regulator for PoPI and the body or bodies behind the Cybercrimes and Cybersecurity Bill to make the structures effective, they are just pieces of paper and it has no real impact on companies. Companies are still asking “why do I need to get ready for PoPI?” but obviously when a regulator is appointed for PoPI, it’s going to have big financial consequences on organisations, especially if they, if they don’t have measures in place to detect breaches and, and it gets leaked through another means, that they’ve been breached. There are big financial implications, jail time for some of the people. It is a very real and serious element that companies need to be aware of. Social engineering is one element where it is kind of easy to get an information breach.”

Part I of the current chapter laid the foundation for specialists’ insight into social engineering. The following section will shed light on the empirical findings retrieved from three business institutions.

PART II: A BUSINESS PERSPECTIVE

Part II provides local businesses’ perspectives and experiences regarding social engineering and information security. As discussed in Chapter 5 (vide section 5.6), although the researcher used a group-administered questionnaire, the questionnaire has qualitative components in it. This chapter provides an insightful discussion of the data analysis and interpretation of the data retrieved from local businesses located in Tshwane.

6.3 ANALYSIS AND INTERPRETATION OF GROUP-ADMINISTERED QUESTIONNAIRES

As explained in Chapter 5 (vide 5.4.1.2) the researcher used purposive sampling in an effort to target small to medium sized businesses. The researcher approached 20 small to medium sized businesses in Tshwane via e-mail. However, only three businesses favourably responded to this request. This e-mail request consisted of a short description of the nature of the request as well as an attached letter of motivation (see Annexure D), informed consent letter (see Annexure E) and ethical clearance certificate (see Annexure A). The sample groups from each institution varied. Institution A is an institution which specialises in tax, audit and advisory services. Institution B specialises in consulting and analysis services in an effort to manage security risks. Institution C is an insurance company. Important to note is that data were collected from specific departments within these institutions, as elaborated on in section 6.4. The information security workshops took place in May (13 May 2016) and June (27 June 2016). Due to time constraints and institutional deadlines, institution C requested not to attend the information security presentation but completed the questionnaires and returned them to the researcher.

In brief, the researcher requested to hold a 60 minute information security workshop. The session consisted of two parts: a questionnaire (30 minutes) and a presentation (30 minutes) on social engineering and information security. The questionnaire was purposefully done before the presentation as to not influence the research respondents' answers. The group-administered questionnaire (see Annexure F) differs from the self-administered questionnaire (see Annexure I). Rather than asking the research respondents about their own social engineering exposure and victimisation, the researcher created hypothetical scenarios in order to evaluate their responses (see Annexure F question 38). Furthermore, the questionnaire was more business-orientated and posed questions about the specific institution's information security.

The researcher deemed this method of conducting research as being innovative and beneficial to both the businesses in question as well as to the study at hand. The

information security workshop provided insight on social engineering attacks, human vulnerability and applicable South African legislation (See Annexure G). In this way the researcher provided a means of applied capacity development by equipping local businesses, based on her studies. In turn, the researcher retrieved valuable data from the research respondents based on their personal perceptions and experiences in the workplace.

The mainly qualitative raw data received were categorised into relevant themes through Microsoft Excel. As each sample group is relatively small, and comprehensive data were obtained, the researcher presented the data descriptively. In order to conceptualise the crux of the responses, the researcher did not include all of the data received, as the responses given were quite comprehensive. Thus, some sections and questions found in Annexure F are not included in this chapter. The data are presented and discussed in terms of the institutions under investigation, namely: institution A, B and C. When citing a specific research respondent from a specific institution, the individual will be referred to according to their institution and respondent number allocated (i.e. Institution A Respondent 1 – IAR 1, Institution B Respondent 7 – IBR 7 or Institution C Respondent 9 – ICR 9).

In order to maximise the potential of the data, the data are authenticated by current literature. In addition, previous chapters and sections are cited to provide a holistic framework. The data will be presented and discussed in the following themes:

- SECTION A: Biographical details.
- SECTION B: Employment details.
- SECTION C: General use of communication through technology.
- SECTION D: Identification and authentication.
- SECTION E: Access control.
- SECTION F: Social engineering.
- SECTION G: Legislation related to information security.
- SECTION H: Impact on information security awareness.

SECTION A

6.4 BIOGRAPHICAL DATA

The study's topic and thus its aims and objectives were restricted to Tshwane, Gauteng in South Africa. Hence, the researcher sought out small to medium sized businesses only located in Tshwane. The researcher received consent from all of the participants who took part in the study. Their names were not requested, nor will their affiliations be published. All three of the sample group institutions specifically requested that their confidentiality and anonymity be maintained.

The biographical characteristics (gender, race, age and marital status) of the study groups are discussed below.

6.4.1 Biographical characteristics of the respondents (Annexure F question 1, 2, 3, 4)

- **Institution A**

Institution A is largely male-dominated, as the sample comprised mostly males (IAR 1,2,3,4,5,6,7 and 9) and only one female (IAR 8). The majority of the research respondents were black (IAR 3, 5, 7, 8 and 9), followed by Indians (IAR 1 and 2) and whites (IAR 4 and 6). No other race groups were represented in the sample. Most of the research respondents were classified as young adults (IAR 1, 2 3 and 6), closely followed by those whose ages ranged from 25-30 years old (IAR 5, 8 and 9). IAR 4 and 7 indicated that they were between the ages of 31-35 and 36-40 years old respectively. Bearing in mind that most of the research respondents were young, the majority of the respondents specified that they were single (IAR 1, 2, 3, 6, 8 and 9). IAR 4 and 7 responded that they were married and divorced respectively. IAR 5 did not indicate his marital status.

- **Institution B**

Institution B is largely female dominated, as there were six females (IBR 1, 2, 3, 4, 7 and 8) and two males (IBR 5 and 6). The sample included six whites (IBR 1, 3, 5, 6, 7 and 8), one black (IBR 2) and one coloured (IBR4). Most of the research respondents were younger than 30 years old (IBR 1, 2, 4, 5, 7 and 8). Two of the research respondents (IBR 3 and 6) specified that they were in the age group of 31-35 years old. Most of the research respondents indicated that they were single (IBR 1, 2, 3, 4, 5 and 7). IBR 6 and 8 indicated that they were married.

- **Institution C**

Institution C is a small sample consisting of four males (ICR 1, 3, 4 and 5) and one female (ICR 2). All of the respondents are white and married except for ICR 2 who indicated that she is divorced. ICR 1 and 5 specified that they were between 31-35 years old, while ICR 2, 3 and 4 shared that they are between 41-45 years old.

SECTION B

6.5 EMPLOYMENT DETAILS

The research respondents were requested to provide details about their occupation and time period of employment.

6.5.1 Occupation and time period of employment (Annexure F questions 5 and 6)

The occupations of each research respondent varied according to the institution they are employed at. Consequently, each institution will be discussed separately.

- **Institution A**

Institution A comprised the information security department within a financial institution. All of the research respondents thus worked in the information technology and security field. Thus, the sample was made up of IT consultants (IAR 1, 4 and 7), IT analysts (IAR 2, 3 and 6) and IT auditors (IAR 5, 8 and 9). The analysis of data

should be viewed in light of the occupations and operational functions of the research respondents. More than half of the research respondents indicated that they had been employed for a year or less (IAR 1, 2 3, 5, 6 and 7). This is followed by IAR 8 and 9 who indicated that they had been employed for two years or less. Only one research respondent (IAR 4) indicated that he had been employed for nine years.

- **Institution B**

Institution B wanted the sample to include various role players within their institution, thus the sample is quite diverse. The sample included a project leader (IBR 1), information analysts (IBR 2 and 4), an account manager (IBR 3), a crime analyst (IBR 5), heads of departments (IBR 6 and 7) and an information developer (IBR 8). Most of the research respondents (IBR 2,3 and 4) indicated that they had been employed for less than or equal to two years, while IBR 8 specified that she had been employed for less than or equal to three years. IBR 1 and 5 indicated that they had been employed for less than or equal to four years, and the heads of department (IBR 6 and 7) indicated that they had been employed for less than or equal to six and five years respectively.

- **Institution C**

Institution C's sample consisted of a forensic analyst (ICR 1), information security specialist (ICR 3), IT security consultant (ICR 5) and two managers (ICR 2 and 4). ICR 4 indicated that he had worked for his current employer for less than or equal to two years, ICR 1 less than or equal to three years, and ICR 5 less than or equal to eight years. ICR 2 and 3 both shared that they had worked for their current employer for more than 10 years.

Research indicates that the less time one is employed at a particular institution, the more at risk they are to a social engineering attack (Conteh & Royer, 2016: 4; Gardner & Thomas, 2014: 33; Lord, 2016). The longer an individual is employed at an institution, the less likely he or she will be a victim of a social engineering attack in the workplace, as such individuals are familiar with their institution's security procedures.

SECTION C

6.6 GENERAL USE OF COMMUNICATION THROUGH TECHNOLOGY

Online communication is a significant part of modern culture. This is specifically true for most business settings, as online communication can be an expedient and effective business tool. Balle (2016) supports this notion, as the author explains that the use of the internet can assist in propelling any business to the next level. As a result, the researcher posed questions regarding the research respondents' general use of communication through technology.

6.6.1 Technological devices, frequency of internet usage and reasons for internet usage (Annexure F questions 7, 8 and 9)

- **Institution A**

The research respondents indicated that they used most of the technological devices described in the questionnaire. IAR 6 also mentioned that he used the television to access the internet. The research respondents' answers varied in terms of their internet usage. Five of the research respondents indicated that they spent less than or equal to five hours on the internet per day (IAR 1, 4, 5, 6 and 8), while four of the research respondents specified that they spent between eight and 12 hours on the internet per day (IAR 2, 3, 7 and 9). The research respondents indicated that they used the internet for most of the reasons provided. IAR 8 indicated an additional reason for her internet usage, namely online shopping.

- **Institution B**

All of the research respondents indicated that they accessed the internet from their laptops and mobile phones. Most of the research respondents (IBR 2, 3, 4, 5, 6, 7 and 8) indicated that they used between nine and more than 12 hours of internet on a daily basis. IBR 1 indicated that she used less than or equal to six hours of internet per day. The research respondents indicated that they used the internet for most of the reasons

provided. All of the research respondents indicated that they used the internet for work and e-mail purposes.

- **Institution C**

All of the research respondents selected the laptop and mobile phone as technological devices from which they access the internet. ICR 3 specified that he accessed the internet from all the devices provided. In addition, he also accesses the internet from the television, multimedia entertainment devices and gaming consoles. Most of the research respondents (ICR 2, 3 and 5) spend less than or equal to six hours on the internet. ICR 1 spends less than or equal to nine hours and ICR 4 spends less than or equal to nine hours a day on the internet. All of the research respondents specified that they used the internet for work and e-mail purposes.

6.6.2 Accessibility of personal information (Annexure F question 10)

- **Institution A**

The majority of the research respondents (IAR 1, 2, 3, 5, 7 and 8) totally agreed with the perception that their personal information is available to the general public. This was closely followed by the remaining respondents (IAR 4, 6 and 9) who agreed with this notion. These respondents work in IT-related fields and know the extent of how their personal information can be accessed by the general public. IAR 2, 3, 5, 6, 7, 8 and 9 indicated that they were very aware that their personal information is available to the general public. IAR 6 specifically mentioned that laws which protect privacy are not enforced. This is substantiated by the discussion on legislation in Chapter 3 (vide section 3.3). IAR 7 and 8 mentioned security defects on websites while IAR 8 drew attention to the use of cookies and its role in compromising information security. Cookies are small files which are stored on a user's technological device. They are created to hold a small quantity of data specific to a particular user and website. They can be accessed by the web server (a system that distributes content or services to end users over the internet) or through the user's technological device. In this way, information can be carried from one website to another. Although cookies are not

malicious, they are able to store information given to a website such as credit card information or passwords. Thus, cookies can be a threat to privacy. This can be prevented by turning off the cookie feature in the browser (Safa, Von Solms & Futch, 2016: 15).

- **Institution B**

Most of the research respondents (IBR 2, 3, 4, 5 and 6) agreed that their personal information is accessible to the general public. IBR 5, 6 and 8 attributed this perception to social networking websites. IBR 2 conveyed that information would always be accessible if an individual produces personal information in the absence of proper security measures.

- **Institution C**

The research respondents either indicated that they totally agreed (ICR 2 and 4) or agreed (ICR 1 and 5) with the perception that their information is accessible to the general public. However, ICR 3 totally disagreed with this perception, as reflected in the following sentiments:

ICR 3: “All information used and accessed that is of a personal or semi-personal nature is ‘behind’ some form of authentication and therefore beyond the reach of the general public. The general public does not have the skill to go after specific personal information behind such services. I do agree that ‘anything’ on the internet is fair game for hackers, however I do not regard hackers as the general public.”

On the contrary, ICR 4 revealed that he had Googled himself and retrieved personal information, such as his personal telephone number.

6.6.3 Accessibility of telephone number and e-mail address (Annexure F questions 11 and 12)

- **Institution A**

Most of the research respondents indicated that their telephone number and e-mail addresses are accessible to the general public. In the case of telephone numbers,

they allocated their reasoning to receiving multiple calls from telemarketers, as explained by IAR 7:

IAR 7: “People that I know have provided my details to others. Many organisations have sold my personal details to telemarketers.”

Marketers can obtain information through customer loyalty cards, shared information from companies which are not rivals, or through public records. Information can be bought or rented. In some cases, lists are combined and scrutinised to provide a holistic representation of the individual (Patel, 2013). Accordingly, if marketers can easily retrieve personal contactable information, how much more so can a social engineer with malicious intent, access similar information.

The research respondents indicated that their e-mail address needed to be made public for work purpose. It was also noted that e-mail addresses are often mandatory fields. IAR 9 revealed that he generally registered on different websites without full knowledge of how his information is stored.

- **Institution B**

Most of the research respondents believed that their telephone numbers and e-mail addresses are accessible to the general public. IBR 2, 4, 5, 6 and 8 said that this was due to work reasons. IBR 2 and 4 mentioned that they may give their telephone number to someone and it might be passed on. With regard to e-mail addresses being known to the public, IBR 1, 2, 6 and 7 said that this information needs to be available for work and marketing purposes. IBR 7 conveyed that her e-mail address was available off her social networking accounts and she found it to be less pervasive than a telephone number.

- **Institution C**

Most of the research respondents perceived that their telephone numbers and e-mail addresses are accessible to the general public. They advocated that this was mostly due to work reasons.

SECTION D

6.7 ACCESS TO AND VERIFICATION OF PERSONAL INFORMATION

6.7.1 Access control procedures (Annexure F question 13)

The research respondents were asked if their institution has access control procedures in place to protect sensitive and personal information.

▪ Institution A

The majority of the research respondents (IAR 1, 2, 3, 4, 7, 8 and 9) indicated that their institutions did have access control procedures in place. Two of the research respondents (IAR 5 and 6) were uncertain of such procedures. Those (IAR 2, 3, 7, 8 and 9) who responded positively were asked to elaborate on their responses and listed the use of IT security policy, IP authentication, password-protected documents, authorisation in terms of access, and encryption as part of their institution's access control procedures. IAR 8 specifically mentioned the following:

IAR 8: "Our hard drives are encrypted and password rules are in place which requires for passwords to be changed every 30 days. Furthermore, we make use of software called Bitlocker which encrypts our memory sticks."

BitLocker is an encryption feature included with select editions of Windows Vista. It protects data by providing encryption mechanisms for entire volumes (Microsoft, 2016). Bitlocker is a program installed on computers which prevents the transferring of documents onto an external hard drive, unless an administrative password is inserted.

▪ Institution B

Most of the research respondents (IBR 1, 2, 3, 4, 5, and 6) specified that their institution adhered to access control procedures. This was illustrated by the following responses:

IBR 1: “Yes, only information needed is captured on systems accessed by other employees. All systems are password protected. All personal information only authorised persons have access.”

IBR 2: “We deal with clients' information and information as very personal and sensitive. All personal information is only accessible by the analyst and the client working with the information and not shared with other persons, as this is a breach of contract. Only parties who are allowed to access the information can. Most of the information is stored on the system and not attainable by other parties that are not allowed to access the information.”

IBR 4: “My institution complies with the PoPI Act. We have all signed confidentiality agreements and were made aware of the consequences one may face.”

IBR 5: “All information is given on a need-to-know basis and is protected strictly by individuals. All information is password secured.”

IBR 6: “Our institution is compliant as information is obtained with consent and clear purposes. The information is only kept for the time and reason applicable.”

The above responses show that the institution places priority on keeping personal information confidential. Measures and consequences are put in place to ensure compliance. IBR 6 responded “yes” and “no” to the question. He noted that his institution was in the process of implementing controls to be in line with PoPI legislation. This portrays that the institution wants to adhere to legislation and is taking the necessary steps to do so. IBR 8 was unsure if her institution had access control measures in place. All employees should be aware of this in order to minimise risks.

▪ **Institution C**

All of the research respondents were adamant that their institution adhered to access control procedures. The reasoning for this is evident in the below responses:

ICR 2: “Access depends on job grade or job description. Access to certain confidential data fields of clients such as ID number, bank account etc. needs approval, otherwise you can't see this information.”

ICR 3: “Policies, standards and guidelines exist to ensure that staff are aware of how sensitive and personal information needs to be handled and treated. Within IT, several controls have been implemented to limit access to this information to authorised individuals who in turn are monitored and audited on a regular basis.”

ICR 5: “Personal information is kept secure in a data base which requires the appropriate access to the data to be approved. The data itself is encrypted in the data base. Policy also states that personal information may not be stored on any location outside the network. Work stations are encrypted to prevent any leakage of information as well.”

6.7.2 Password management procedures (Annexure F questions 14, 14.1 and 15)

All of the research respondents (Institution A, B and C) shared that password management and network security were compulsory in their institution. From the current sample it appears to be common practice to exercise password management. Users have unique usernames and passwords, and passwords are complex and alphanumeric. In addition, users are technologically required to change passwords on a regular basis and the same password cannot be reused. Technology is also configured to allow authorised users to change passwords when the need arises.

6.7.3 Electronic signature (Annexure F question 25)

Most of the research respondents (IAR 1, 2, 3, 4, 5, 6, 8 and 9) used e-signatures while only one (IAR 7) specified that he did not use an e-signature. All of the research respondents in institution B and C indicated that they made use of e-signatures. The use of e-signatures is prevalent in the work place.

The risks associated with the use of e-signatures are highlighted in Chapter 7 (vide section 7.6.4). However, businesses can take specific steps to mitigate these risks by making use of digital signatures. A digital signature is a sub-category of an e-signature. It is an electronic expression attached to or associated with a document carried out by an individual with the intent to sign the document and thus agreeing to the content (Hullavarad, O'Hare & Roy, 2015: 36). Whitman and Mattord (2012: 586) describe a digital signature as a mathematically authenticated encrypted message. Digital signatures enhance security as they ensure signer authentication, data integrity and non-repudiation. Signer authentication provides evidence of who actually signed or approved a document. Thus, a digital signature links the user's signature to a detectable entity. A digital signature maintains data integrity as it cannot be re-attached to another document. Non-repudiation is effected as verification of who the sender is, cannot be contested.

SECTION E

6.8 ACCESS CONTROL

6.8.1 Similarity of passwords and frequency of password modification (Annexure F questions 29 and 30)

▪ Institution A

The research respondents expressed conflicting practices regarding the similarity of the passwords. Some of the research respondents (IAR 2, 3, 6 and 7) indicated that most of their passwords were the same, while others (IAR 1, 4 8 and 9) indicated that some of their passwords differed. IAR 5 shared that all of his passwords were different. The majority of the research respondents (IAR 1, 2, 4, 5, 7, 8 and 9) shared that they only changed their passwords when prompted to. While IAR 3 and 6 expressed that they did not change their passwords often.

▪ Institution B

Most of the research respondents (IBR 1, 4, 5, 7 and 8) indicated that their passwords were somewhat different. IBR 2 said that most of her passwords were the same, while

IBR 3 and 6 specified that their passwords were all different. The sample was split in the frequency of password modification. IBR 1, 4, 7 and 8 only change their passwords when prompted, while IBR 2, 3, 5 and 6 change their passwords often.

- **Institution C**

Most of the research respondents (ICR 1, 2 and 3) revealed that their passwords were somewhat different. ICR 4 and 5 specified that all of their passwords were different. ICR 1, 2 and 4 said that they changed their passwords often, while 3 and 5 revealed that they did not change their passwords often.

Analogous passwords and the infrequency of password modification increases risk to social engineering attacks.

6.8.2 Social networks applications (Annexure F question 31)

- **Institution A**

Most of the research respondents (IAR 1, 4, 5, 6 and 8) maintained that they kept their social networking applications logged in at all times. Two research respondents (IAR 3 and 7) shared that they kept these applications logged in most of the time, while the remaining two (IAR 2 and 9) indicated that they only kept these applications logged in sometimes.

- **Institution B**

IBR 1, 4, 7 and 8 always keep their social networks logged in, while IBR 2 keeps them logged in most times. IBR 1 and 3 seldom and never keep their social networks logged in respectively.

- **Institution C**

ICR 1, 2 and 4 never keep their social network applications logged in, while ICR 3 and 5 acknowledged to keeping their social network applications logged in most of the time.

6.8.3 Accessibility of passwords (Annexure F questions 33 and 33.1)

- **Institution A**

Only one research respondent (IAR 6) indicated that someone had access to his passwords, listing his girlfriend as the recipient.

- **Institution B**

Only two respondents (IBR 4 and 8) indicated that their spouses had access to their passwords. IBR 4 maintained that her boyfriend had access to her social networking passwords.

- **Institution C**

ICR 3 was the only research respondent who revealed that his spouse had access to his personal passwords, however stipulated that no one had access to his work passwords.

The more people who have access to an individual's passwords, the more vulnerable they are for third party social engineering attacks, as discussed in Chapter 2 (vide 2.6.1).

6.8.4 User access revoked (Annexure F question 34)

- **Institution A**

Most of the research respondents (IAR 4, 5, 7, 8 and 9) conveyed that user access was revoked immediately after the termination of a contract. IAR 6 indicated that termination would take place days after, while IAR 1, 2 and 3 were unsure. This can be linked to confusion and ignorance of the institutional policy.

- **Institution B**

IBR 2, 3 and 6 specified that access was revoked immediately after termination, while IBR 1 and 5 reported that this process took place a few days after termination. The responses were diverse on when user access is revoked. IBR 4, 7 and 8 responded

that they were unsure of this process. It can be deduced that staff members are not clear on this process within their institution.

- **Institution C**

The research respondents' answers varied and this may result in some confusion on when user access is revoked when no longer employed by the institution. ICR 1, 2 and 5 reported that access was revoked days after termination of a contract, whereas ICR 3 and 4 maintained that access was revoked immediately.

Staff at any institution should be well aware of when user access is revoked for ex-employees, to prevent disgruntled employees from causing harm to an institution as stated in Chapter 2 (vide 2.6).

SECTION F

6.9 SOCIAL ENGINEERING

Sections A to E provide a foundation to the remaining sections of the questionnaire. However, the researcher changed Section F of the group-administered questionnaires to better suit its unit of analysis.

6.9.1 Social engineering awareness (Annexure F questions 35 and 35.1)

The research respondents were asked if they knew what social engineering is. The different institutions responded accordingly.

- **Institution A**

Most of the research respondents (IAR 1, 2, 4, 7, 8 and 9) from institution A indicated that they knew what social engineering is. This could be attributed to their professional setting as they operate in an IT profession. They provided the following responses:

IAR 2: "The art of using social skills to obtain very sensitive data directly from people and they don't have a clue that it is happening."

IAR 4: "Manipulation of trust."

IAR 7: “Collecting sensitive social information through social means in order to gain unauthorised access.”

IAR 8: “The use of social "niceties" to get access to things that you usually shouldn't have access to/ bypass security measures that are in place.”

IAR 9: “The use of social contact to obtain information (personal/private) from other user implicitly.”

Only three research respondents (IAR 3, 5 and 6) indicated that they did not know what it is, even though they work as an IT analyst, IT auditor and IT analyst respectively. This reveals that even in IT-related fields, knowledge and awareness of social engineering can still be lacking. This finding contributed to the value of the study, further discussed in Chapter 8 (vide section 8.7).

▪ **Institution B**

IBR 1, 3, 6 and 7 indicated that they knew what social engineering is. IBR 1 and 6 provided the following definitions:

IBR 1: “Information security related - it is how information can be used which is not your own information.”

IBR 6: “It is the construction of social relations and perceptions to achieve a predetermined objective. These can have both a positive and negative impact.”

IBR 3 and 7 provided responses that display confusion regarding social engineering:

IBR 3: “Not really sure, guess it's about social networking.”

IBR 7: “Social engineering is building a 'picture' of a person via social media. I can build my social identity by taking part in social media or I can form an opinion of someone via their social media footprint with the intent of using the information for illegal purposes.”

However, through the responses provided in 6.9.1 it is apparent that although the research respondents were not familiar with the correct terminology, they were aware of the techniques associated with social engineering.

- **Institution C**

All of the research respondents relayed that they knew what social engineering is. Some of their responses are displayed below:

ICR 2: “Manipulation to get individuals to divulge sensitive or confidential information.”

ICR 3: “Social engineering is the manipulation of one person i.e. victim by another i.e. an attacker in order to obtain unauthorised access to confidential information and or physical access that would otherwise be limited to authorised individuals only for the purposes of selfish and malicious intent. This manipulation exploits weaknesses in the psychological behaviour of humans such as fear, greed, anger, embarrassment etc.”

ICR 4: “Someone trying to trick you into providing personal information (ID, password) or to install software to capture such information.”

ICR 3: ...captured the essence of social engineering in describing it as “human interaction component of a 'hack' attempt.”

The research respondents in institution C were very aware of what social engineering is, as well as the threats associated with it.

6.9.2 Awareness of social engineering threats (Annexure F question 36)

- **Institution A**

Most of the research respondents indicated that they were very aware of social engineering threats. IAR 8 and 9 shared that they were somewhat aware; IAR 6 indicated that he was somewhat unaware and IAR 3 specified that he was not aware at all.

- **Institution B**

The responses varied – IBR 6 reported that he was very aware of social engineering, IBR 1 and 7 noted to be somewhat aware, IBR 8 somewhat unaware and IBR 4 and 5 not aware at all. IBR 2 did not answer the question.

- **Institution C**

All of the research respondents indicated that they were very familiar with social engineering threats. This could be linked to their job titles discussed in section 7.4.1.

6.9.3 Social engineering hypothetical scenarios (Annexure F question 37)

Hypothetical scenarios were created based on the fundamental perspectives in social engineering (vide Chapter 2). This was done not only to extract hypothetical responses, but to also create awareness of various types of social engineering attacks. Moreover, the hypothetical scenarios can take place in a professional and personal capacity, thus creating further awareness. The scenarios found in question 37 (Annexure F), the research respondents' responses and the interpretation are presented below.

The Chief Financial Officer (CFO), of your company, whom you have never met before, is located in another province. The CFO is known, by those who have had an encounter with him, for his high-pitched voice. One morning a man speaking in a high-pitched voice phones you, identifying himself as the CFO, and requests confidential financial information from you.

- **Institution A**

Some of the research respondents (IAR 1, 4, 5) conveyed that they would seek authentication and permission before proceeding with the request. IAR 7 and 8 said that they would ask that the request be documented in e-mail. IAR 2 and 9 provided the following responses:

IAR 2: “I would give whatever is asked.”

IAR 9: “I would ask the person to confirm his identity before we speak further.”

Although authentic, IAR 2 and 9 provided responses which exhibit lack of good security practices.

▪ **Institution B**

All of the research respondents were adamant that company procedure should be followed which includes having the request be made via e-mail. In some cases, the research respondents conveyed that they would also inform their line manager about the request. These responses showed that the institution not only has policies and procedures in place but that the staff members are aware of them. Examples of this are highlighted in the responses below:

IBR 5: “I would request that an e-mail be sent in order to verify that it is in fact him and that he includes my manager in the e-mail.”

IBR 6: “I would revert him back to our policies and procedures requesting a written request and electronic ticket. The request would be subject to management approval.”

▪ **Institution C**

All of the research respondents maintained that they would decline the request and seek a written request. The following extracts highlight the stringent processes the research respondents would follow:

ICR 3: “I would explain that due to phishing concerns I am unable to assist telephonically but that I would be able to e-mail the requested information to his work e-mail address for later review. I would also report the attempt to solicit information to the Cyber Security Incident Response Team to follow-up and collate this information with any other such threat to the organisation.”

ICR 5: “I would request that the person follow the appropriate channel to obtain the information, by contacting me from his e-mail account to initiate the interaction so that I

may confirm this source of the e-mail via the headers in his e-mail. Additionally, I would request certain information (phone number/personal assistant) so that I may confirm his current state and the validity of the request via other channels.”

ICR 3 mentioned a Cyber Security Incident Response Team (CSIRT) which was also later mentioned by another participant. This shows that their institution takes cyber security seriously.

An authoritative figure, unknown to you, informs you that he has permission from an authorised person, known to you, to use confidential information. The known colleague is away on maternity leave and has requested not to be disturbed. The authoritative figure identifies your colleague and confirms her current whereabouts and subsequently requests confidential information from you.

- **Institution A**

All of the research respondents expressed that they would either not provide the information requested at all or wait for formal communication and higher authorisation before following through with the request. This is conceptualised in the following responses:

IAR 3: “I would ask what it is used for and why they need it. I will request a formal communication for the need of my information.”

IAR 4: “I would need authorisation first before providing any personal information.”

IAR 8: “I would not provide the information without some form of written consent from the colleague on maternity leave.”

IAR 9: “I would tell that person that I am not authorised to give out personal information.”

- **Institution B**

IBR 1, 2, 4, 7 and 8 expressed that they would first consult with management before they give over any information. Adhering to this process would include more than one input and allow time for the targets to ascertain a logical way of dealing with the request. IBR 6 extended an interesting view. Taking into consideration that he is in a management position, he maintained that he would decline the request and refer it to the authorised person. Furthermore, he conveyed that the request of the colleague on leave not to be disturbed would be overruled. This displays that good security measures override good etiquette.

- **Institution C**

None of the research respondents reported that they would adhere to the request but rather seek written permission to carry out the request. In addition, the request should be approved by the line manager. This is denoted in the following response:

ICR 3: “I would verify the legitimacy of the request with the line manager of the colleague who is away on leave. As part of the process I would also verify with the information security team if the requested information may be shared.”

You have been experiencing problems with your laptop and require urgent assistance. As such you receive a phone call from a technician at desktop support who, in an effort to solve your problem, requests for your login credentials.

- **Institution A**

More than half of the research respondents (IAR 2, 3, 7, 8, 9) disclosed that they would provide their credentials to desktop support. These responses are evident below:

IAR 2: “I would give whatever is asked.”

IAR 3: “I would ask them to confirm their occupation and hand my details if necessary.”

IAR 7: “If I know the technician I generally supply them with the details and change my password immediately after.”

IAR 8: “I would provide the login details and change them when I get my laptop back.”

IAR 9: “I would give them my details after confirming their identity.”

IAR 4 and 5 stated that they would only share their credentials once they had verified who the technician is. IAR 1 and 6 said that they would rather ask the technician if they could key in their credentials themselves.

▪ **Institution B**

Most of the research respondents (IBR 2, 3, 4, 7) sustained that they would request to type in their credentials themselves. IBR 5, 6 and 7 noted that their institution had specific guidelines for such a request, as outlined below:

IBR 5: “Most technical support will not request your credentials as they should have an administrator account. I will not give any credentials out.”

IBR 6: “This would be declined. Support staff is not allowed to have passwords for personal laptops. They can only assist once logged in by a specific user – either onsite support or rules-based remote support in presence.”

IBR 7: “I would deny giving my login credentials as they should have remote access to my laptop which will allow me to enter my own details.”

The above responses illustrate a sense of awareness on information security procedure. This information should be made known to all staff members.

▪ **Institution C**

All of the research respondents were adamant that they would not provide such details to a technician. ICR 5 went on to mention that she would report such a technician and had done so in the past. The responses are captured below:

ICR 2: “I will never provide login details, whether telephonically or to the technician in person.”

ICR 3: “Company policy prohibits us from sharing user credentials under any circumstances. The technician must solve the problem without these credentials or ask

me to log in myself. Desktop support technicians are equipped with administrative passwords that can help them avoid needing end user credentials.”

ICR 5: “I will never give my login credential and will (and have) reported such individuals to senior management to be dealt with appropriately.”

Many of the research respondents maintained that they would not provide their login credentials to the technician and rather key it in themselves. However, only one research respondent (IBR 3) noted that her laptop contained a lot of personal and sensitive information. In this scenario, not only are the target’s credentials at risk but also the information on the laptop, especially if it has not been protected.

A person unknown to you stands closely behind you as you key in personal identification and authentication credentials on your mobile phone, laptop or automated teller machine (ATM).

- **Institution A**

The research respondents provided various strategies for dealing with the above scenario. These include covering or protecting the password (IAR 1, 7, 8 and 9) intentionally typing in the incorrect password (IAR 2 and 6) or asking the person to stand back (IAR 4 and 7). IAR 3 and 5 shared that they would change their passwords immediately after the incident.

- **Institution B**

Most of the research respondents (IBR 1, 2, 3, 4, 5, 7 and 8) indicated that they would either shield their password or ask the person to stand back and thereafter change the password. IBR 6 said he would report this incident to the relevant bank. IBR 3 shared of previous victimisation in the following extract:

IBR 3: “I will stop with my transaction and request the person to move back as this is a concern. There are a lot of scams going around. I was a victim once, where they stole my card and emptied my account.”

- **Institution C**

The research respondents shared that they would either obstruct the unknown person’s view or ask them to stand back. If needs be, ICR 2 shared that she would report the incident.

A person you do not know asks you to kindly hold the door for him/her while accessing the building (where your offices are located).

- **Institution A**

Most of the research respondents (IAR 1, 3, 4, 6, 7, 8 and 9) detailed that they would try to authenticate the person by escorting or taking him/her to the reception or security. IBR 2 and 5 provided the following telling responses:

IAR 2: “I would comply, thinking he is an employee.”

IAR 5: “I would walk away, as I do not know the individual.”

- **Institution B**

The research respondents’ responses portrayed a client-central culture, while still maintaining good security procedures as represented below:

IAR3: “I will help the person, as this is a good deed for the company.”

IAR 4: “We have many clients who visit our offices; therefore I will hold the door open and take them to where they request to go. Most times the person will be let in and asked who they are there to see. If they do not provide the name they are asked to wait outside until they can be verified.”

IAR 6: “I would welcome them and ask whether I can assist. They would wait in the reception until escorted by the person hosting them to reception where they can be assisted.”

IAR 7: “Hold open the door and ensure the person remains in reception until assisted or escorted to/by the correct person.”

IAR 8: “As our offices are the entire building, I would escort them to reception or request their reason for visit and try to assist without leaving them unattended.”

▪ **Institution C**

All of the research respondents said that they would not honour the request. ICR 3 and four mentioned that tailgating was strictly against company policy as expressed below:

ICR 3: “It depends. If the door is under access control, company policy specifically prohibits tailgating and each person is expected to enter and exit their own credentials and or access cards.”

ICR 4: “Tailgating is not allowed and people should use reception for this in order to be properly signed in.”

You receive what appears to be a legitimate invitation to a job interview which you have recently applied for. As the job is in another country; the employer offers to pay for your travel arrangements. The invitation requests you to follow a link and subsequently requires you to enter your banking details so that payment can be made.

▪ **Institution A**

The research respondents revealed that they would not enter their banking details in the link provided, as expressed in the response provided by IAR 6:

IAR 6: “I would never provide my banking details to anyone – not even type it into a web page. It is a definite scam seeing that banks inform their customers not to do it.”

▪ **Institution B**

None of the research respondents indicated that they would enter their banking details and rather opted for alternative solutions such as:

IBR 7: “I will decline giving banking details, see additional information regarding the company or cut all ties and communication.”

IBR 8: “I would request the employer to buy the travel tickets and then forward it to me.”

▪ **Institution C**

All of the research respondents indicated that they would never put their banking details in a site given to them, as displayed below:

ICR 5: “I never put my banking details in on a site that I do not know is secure. I will also confirm with the company via another medium whether this is required.”

Your company credit card is about to expire and you have applied to renew it. You receive a phone call from a representative from your bank requesting that you confirm the following personal details: Identity number, telephone number, physical address, work address and all the information pertaining to your previous credit card.

▪ **Institution A**

Most of the research respondents (IAR 1, 3, 4, 5 and 8) maintained that they would not share the requested details. The following respondents shared that they would give out the information requested as displayed below:

IAR 2: “I would comply thinking that the person is really from the bank.”

IAR 6: “I would confirm it seeing that it is standard practice for banks to ask such questions.”

IAR 7: “I will only provide what is relevant to complete the security check.”

IAR 9: “I would give them my personal details.”

▪ **Institution B**

Most of the research respondents (IBR 2, 3, 4, and 5) indicated that they would not share the details and rather request to go into the bank. The following research respondents detailed their responses below through compliance or requesting verification:

IBR 1: “I would normally provide the information if they are able to provide some of the details for the previous cards.”

IBR 4: “I will inform the representative that I will rather go into the bank as I do not give out my personal information over the phone.”

IBR 6: “The representative would first need to qualify my information such as card number, ID number etc. I would phone back on the bank specific number to finalise any request.”

IBR 7: “I would refer the person to our finance department to verify the required information or decline providing the information and phone the bank directly.”

▪ **Institution C**

The research respondents specified that they would not give this information and would rather wait for the operator to supply the correct the information. In addition they would consult with the bank themselves to verify the legitimacy of the request. ICR 1 indicated the following:

ICR 1: “If they can supply the correct information I will confirm it, but will not correct them if they have the wrong information because then I will supply them with the info they do not have.”

You receive an e-mail from what appears to be a legitimate sender informing you that there is a virus circulating through the internet and that specific files should be deleted and security settings should be changed.

- **Institution A**

Most of the research respondents (IAR 1, 2, 4, 5, 6, 7, 8 and 9) answered that they would not comply, as embodied in the following response:

IAR 2: “I will ignore it. My own system is more reliable than an e-mail. My anti-virus will sort it out.”

IAR 3 responded that he would comply with the request. Interesting to note is that IAR 4, 6, 7 and 9 would seek further consultation regarding the matter.

- **Institution B**

All of the research respondents conveyed that they would refer the matter to their IT department. Some of the responses supporting this are captured below:

IBR 3: “If the e-mail was sent from our technical department, I think I would change my settings but most of the time the technical department deals with it. I do receive a lot of information regarding new scams. Before I open any link I will authenticate some things.”

IBR 5: “No changes will take place simply from an e-mail unless direction comes from a member of the technical team.”

IBR 6: “Refer to IT department and confirm legitimacy. I would not take action based on the e-mail.”

IBR 7: “I will forward the e-mail to the IT department, mark the mail as junk and block the sender. I will then delete the mail permanently.”

- **Institution C**

ICR 3: “I would verify the e-mail headers personally and see if fake values have been inserted. I would also then Google the alleged threat and determine if it is a hoax or not.

I would also research the proposed security changes in order to understand what they do and if they should be changed.”

ICR 4: “I would verify with an internet search to confirm if it is a hoax or not.”

ICR 5: “I would ignore such e-mails and would research such hoaxes.”

You find a USB flash drive with a company logo labelled “Executive Salary Summary” left in the bathroom cubicle

- **Institution A**

Only one research respondent (IAR 2) admitted that they would view the content contained on the USB flash drive. The rest of the respondents either said that they would leave it there or take it to reception or the IT or HR department.

- **Institution B**

None of the research respondents indicated that they would view the information contained on the USB flash drive, citing that they would take it to their Head of Department or HR department. IBR 6 detailed the following:

IBR 6: “I would hand in the USB to executive management and advise of the suspicious event. There should be an investigation done on persons coming and leaving the aforementioned area.”

The above response shows that the research respondent will take this matter further as executive management will be alerted and an investigation should be launched to find out where the USB came from.

- **Institution C**

None of the research respondents indicated that they would view the content on the USB flash drive. The research respondents immediately recognised this scenario as a typical social engineering attack:

ICR 2: “I will take it for safe keeping and then investigate to find the owner.”

ICR 3: “I would hand the flash drive to the cyber security incident response team for analysis. The drive is almost certainly bait to trick a user into putting it into a computer on the inside of the network and opening a file on it.”

ICR 4: “I would not insert it into any computer, as this is a trick to have spyware and key loggers installed.”

ICR 5: “Such devices should never be plugged into your computer as it may very likely be a form of social engineering.”

ICR 4 specifically mentioned the potential of having spyware and key loggers installed on his computer. Spyware denotes a type of technology that gathers information about an organisation or individual without their knowledge. A key logger is a type of surveillance software which has the ability to record every keystroke used to log into a file. It is especially beneficial when infiltrating encrypted files (Whitman & Mattord, 2012: 63).

You receive a pop-up window, while working on your company laptop, which advertises a special to a travel location that you have been researching. The pop-up screen conveys that this special is only valid for a limited time period.

▪ **Institution A**

None of the research respondents reported that they would open the pop-up. Coming from an IT-related background, this can be expected as conceptualised in IAR 6’s response below:

IAR 6: “I would rather make use of the well-known or trusted travel agencies for my travel arrangements, even if I have to pay more.”

- **Institution B**

Most of the respondents (IBR 1, 3, 4, 5, 6, and 7) indicated that they would not open this pop-up and provided reasons for this. Some of the responses are reflected below.

IBR1: “Because I have a technical background I would never open a pop-up. I will search for the location details from a search engine. All specials will be on the location website.”

IBR 3: “Most of the viruses and hacking are from these types of pop-ups. We only allow pop-ups from trusted sites.”

IBR 5: “The pop-up will be closed as it is most likely spam from my previous searches. No unknown pop-ups will be opened as per company policy.”

IBR 6: “I would close the pop-up. I would only click through if the pop-up was from the original site whilst browsing. I would only supply relevant information and check to ensure that the certificates and URL’s are correct.”

IBR 2 and 8 provided the following responses, revealing the enticing nature of the scenario:

IBR 2: “This is tempting. I will ignore it at first and then go and inquire from my technical team.”

IBR 8: “I would take note of the company and look again at home. I would not follow this link on the company laptop.”

- **Institution C**

The research respondents recognised the social engineering attack as conceptualised below:

IRC 5: “I never click on such pop-ups and anything that is a ‘limited’ offer is generally trying to get you to click on something to activate the malicious content.”

You, in your work e-mail, receive an influx of e-mails which appear to be spam.

- **Institution A**

All of the respondents indicated that they would simply delete it. IAR 3, 4, 8 and 9 shared that they would take the matter further and report the matter to the IT or security department.

- **Institution B**

All of the respondents indicated that they would delete the spam e-mail, but most of them (IBR 1, 2, 3, 5, 6, 7 and 8) shared that they would report it to the IT department.

- **Institution C**

The research respondents shared that their institution knows how to deal with the above the scenario as reflected below:

ICR 2: “I will report as per company IT security policy. I will not respond or send it at all.”

ICR 3: “I would flag these as spam in my e-mail and report them to e-mail administrators who will block them and prevent them from being delivered to the rest of the organisation. This is relatively rare as we use spam monitoring services to try and keep this under control.”

ICR 5: “I mark them as spam if the function is available or report to IT security for action to be blocked via content filtering.”

ICR 4 shared that he would report such an incident to the CSIRT as previously mentioned.

6.9.4 Motives behind social engineering attacks (Annexure F question 38)

The research respondents were asked to mention possible motives behind social engineering attacks. Their responses are relayed below. The research respondents grouped possible motives for social engineering attacks in the following themes: access

to personal information, financial reasons, and retrieval of valuable assets. Some of their responses are highlighted below:

IAR 2: “Access to personal information and to get an advantage over me. This is mostly for financial reasons.”

IAR 6: “To steal confidential information, money and or other valuable assets.”

IBR 3: “Personal wealth as they steal the information to mainly gain financially from this, not caring about the destruction caused by their actions.”

Institution B specifically mentioned the risk social engineering can have for businesses, as reflected below:

IBR 5: “To gain access to any sensitive information which could be used against a person individually or the company for some sort of gain, whether financial or other.”

IBR 8: “Access of personal information to steal money out of bank accounts etc. Access to professional information; to steal sensitive information regarding the company and confidential cases.”

ICR 3: “Greed. As far as I am concerned the only reason people do this is to profit financially in some way, shape or form. It drives everything. I also think that it is attractive because it is non-confrontational in the sense that one is not physically assaulting or mugging another person for their money.”

ICR 5: “To get you to open a security risk into the network. Steal your information to further obtain access to your information to commit further fraud or steal from you.”

ICR 3 made an interesting argument in that social engineering attacks are not as confrontational as physical violent attacks, and thus more attractive to certain types of non-violent perpetrators.

6.9.5 Vulnerable groups (Annexure F question 39)

The research respondents were asked to identify vulnerable individuals at risk to the hypothetical scenarios discussed in section 6.9.3.

- **Institution A**

Most of the research respondents (IAR 2, 3, 4, 5, 6, 7 and 8) shared that all the delegated vulnerable groups are susceptible to social engineering.

- **Institution B**

All of the research respondents specified that new employees are at risk to social engineering, while IBR 1, 5, 8 and 9 indicated that contract workers are at risk. IBR 2 explained that all people who are unaware of social engineering techniques are at risk.

- **Institution C**

The research respondents mentioned new employees and executive personnel and assistants as being at particular risk to social engineering attacks. ICR 3 believes that everyone is at risk to social engineering attacks. However, IT personnel are deemed ever so slightly less at risk, simply because in IT circles there is a slightly greater awareness of social engineering and what can in fact be done with stolen credentials.

It can be maintained that everyone is vulnerable to a social engineering attack; however, individuals who are not aware of the techniques may be more susceptible to victimisation. Those under possible threat are elaborated on in Chapter 2 (vide section 2.4).

6.9.6 Information security culture (Annexure F questions 40 and 40.1)

The research respondents were asked if they perceived their institution to have a healthy information security culture.

- **Institution A**

All of the research respondents believed that their institution exercises a healthy information security culture. Reasons for this included the use of automation, firewalls, authentication and encryption mechanisms. Security education is carried out frequently through workshops and e-mail notifications. Furthermore, strict induction programmes and regular updates are carried out.

- **Institution B**

All of the research respondents except IBR 1 believed that their institution has a healthy information security culture. IBR 1 said she was unsure as there could always be improvements to information security. The reasons for maintaining a healthy security culture were stated as sensitive data being protected and encrypted. Also, it is regarded as important to know that the institution deals responsibly with clients' data, which is very sensitive and should thus be protected.

- **Institution C**

All of the research respondents perceived their institution to exercise a healthy information security culture. The research respondents all agreed that regular awareness and education campaigns took place within their institution. However, ICR 4 mentioned that although his institution had continuous education campaigns, human nature may not always be manageable. The role of human nature is discussed at length in Chapter 3 and ultimately forms the core of this study.

SECTION G

6.10 LEGISLATION RELATED TO INFORMATION SECURITY

The research respondents were asked questions regarding their knowledge and awareness of South African legislation relating to information security.

6.10.1 Awareness of South African legislation relating to information security and social engineering (Annexure F question 41)

▪ Institution A

The majority of the research respondents (IAR 2, 5, 6 and 8) shared that they were unaware of any legislation regarding information security, while IAR 1 and IAR 9 left this section unanswered or indicated that they were uncertain respectively.

▪ Institution B

IBR 1, 5 and 6 maintained that they were familiar with legislation pertaining to information security and social engineering. The remaining research respondents either noted that they were unaware (IBR 2 and 3) or uncertain (4, 7 and 8) of such legislation.

▪ Institution C

All of the research respondents said that they were familiar with legislation regarding information security.

6.10.2 Familiarisation with the Protection of Personal Information Act 4 of 2013 (Annexure F question 41.1)

Regarding awareness and knowledge regarding the PoPI Act, the following was elaborated on by the research respondents:

▪ Institution A

IAR 3: “Peoples’ personal details should be protected and those in breach can be called to account.”

IAR 4: “Strict requirements and penalties for non-compliance.”

IAR 7: “Restricts access and retention of personal information.”

IAR 9: “I think it only covers a portion of information security but mostly focuses on personal information rather than company information.”

- **Institution B**

IBR 5: “It prohibits any personal information being given out without consent.”

IBR 6: “Unclear as regulations are still being drafted. Information security has become more impacted since the Act was brought in.”

IBR 7: “Information security measures will have to be improved to ensure compliance to PoPI.”

- **Institution C**

ICR 1: “Personal information in your possession needs to be protected and not shared without consent, for the intended use.”

ICR 2: “Restricting access of confidential information.”

ICR 3: “The purpose is to protect individual privacy but should be described in company policies.”

ICR 4: “This requires that the appropriate security measures are implemented to secure personal information. The appropriate processes need to be implemented and audits done to ensure compliance.”

6.10.3 Familiarisation with the Electronic Communications and Transactions Act 25 of 2002 (Annexure F question 41.2)

Regarding the awareness and knowledge regarding the ECT Act, the following was elaborated on by the research respondents:

- **Institution A**

IAR 4: “Not much as it is very vague at times and sub-regulations are not enforceable.”

- **Institution B**

IBR 6: “The Act sees information as private/confidential and may only be gained through legitimate processes.”

- **Institution C**

ICR 2: “One needs to state and safeguard any form of communication by e-mail, SMS etc.”

ICR 5: “It ensures the security of data in transit and that systems are kept secure and cannot easily be breached to get to data in transit. Patching and compliance applies here.”

Patching is an important tool used in computer security, as it is software constructed to update a computer program or its supporting data in order to repair and improve it.

6.10.4 Familiarisation with the Cybercrime and Cybersecurity Bill (Annexure F question 41.3)

The research respondents shared details on what they know about the Cybercrime and Cybersecurity Bill.

- **Institution A**

IAR 4: “As PoPI has very stringent requirements for both individuals and corporates, or controls with big penalties for non-compliance.”

IAR 7: “Limit and criminalise cybercrime and improve information security.”

IAR 9: “Focuses more on electronic information.”

- **Institution B**

None of the research respondents provided any comments on the Bill.

- **Institution C**

ICR 2: “New and improved processes and searching mechanisms may be required in reference to the expected number of new offences.”

ICR 5: “This will, if implemented, give a standard to the method of responding to cybercrime. Reporting of crime will be given a central point and cybercrime will be able to be prosecuted more effectively, which is currently done under normal law at the moment.”

SECTION H

6.11 IMPACT ON INFORMATION SECURITY AWARENESS (Annexure F question 41.3)

Most of the research respondents responded favourably to the impact the questionnaire had on their own information security awareness, as displayed below in some of the responses:

▪ Institution A

IAR 2: “Yes, it has made me more aware.”

IAR 3: “Raises awareness of the importance.”

IAR 6: “It reminded me of the importance of information security.”

IAR 7: “This enhanced my awareness.”

IAR 8: “It has made me more aware of what I should do if the hypothesised scenarios had to happen.”

IAR 9: “Social engineering is real and it happens to a lot of people. I think people need to be made more aware of social engineering.”

▪ Institution B

IBR 1: “This allows me to think again about all the threats in information sharing.”

IBR 2: “Completing this questionnaire has made me aware of the implication that may appear if my technological equipment is not secure.”

IBR 3: “To be more aware of calls and e-mails received and working with such information.”

IBR 4: “It has made me aware of other information regarding information security.”

IBR 5: “It made me more aware of the threats and dangers to information security.”

IBR 6: “Refreshed the importance of information security.”

IBR 8: “To question the true information security of the workplace just because someone says it’s safe, doesn’t mean it is.”

▪ **Institution C**

ICR 4: “I found the described scenarios thought-provoking. As I endeavour to keep raising awareness about information security related concepts, I would try to focus more on trying to distil the specific aspects of a scenario that make it a potentially dangerous situation.”

ICR 5: “The questionnaire brings to mind how easily we may personally get affected by theft of information and that we need to always keep our eyes open to this type of risk. It also shows how important the IT security department is and that the measures they implement are not to stop us from doing our work but to protect and secure it.”

Although many of the research respondents were quite accustomed to principles in information security, they still supported the relevance and need for the training provided by the researcher based on her studies.

6.12 CONCLUSION

Data analysis relies on a twofold process: reducing the data to manageable portions; and then identifying emerging patterns and themes. Chapter 6 was divided into Part I and Part II.

Part I provided an overview of the analysis and interpretation of perceptions and operational experiences of the identified SMEs who took part in the study. Themes were identified, as directed by the study’s aim and objectives, and discussed accordingly. These themes included defining social engineering, the occurrence of social engineering and the establishment of vulnerable groups associated with social engineering. Insight was gained into the profile of a social engineer, types of attacks and the impact of social engineering on businesses and individuals. This section particularly addressed the SMEs’

perspectives on the human element in protecting information, as well as the legislation allied with it. Subsequent themes emerged and are discussed further in Chapter 8 (vide Chapter 8 section 8.3). The SMEs agreed that social engineering is occurring on a micro and macro level. It was established that good technologies are inadequate in a good information security culture. Furthermore, it was put forth that no person is immune from a social engineering attack, and that it can occur in an online and offline setting.

Part II brought added meaning to the study as it provided a business perspective of social engineering. Through the innovative group-administered questionnaire and an informative presentation on social engineering, an interactive learning process was achieved. The instructive data received were analysed and interpreted. There was a wealth of data retrieved from the research respondents. This was presented according to the different institutions. The themes which emerged from the data collected were noted and unpacked. The awareness of social engineering varied according to the institutions. Vulnerability to social engineering attacks was discussed with regard to various variables, while the hypothetical scenarios extracted multiple vulnerabilities. Moreover, it became clear that most of the research respondents were unaware of legislation pertaining to information security. The responses received from the research respondents indicate that there is a need for awareness and training workshops equipping the workplace with knowledge regarding social engineering and best information security practices.

In light of the data analysed and interpreted from a SME and business perspective, the study is interested in investigating an individual's perspective on social engineering and its related aspects. This will follow in chapter 7.

CHAPTER 7

ANALYSIS AND INTERPRETATION OF DATA: AN INDIVIDUAL PERSPECTIVE

7.1 INTRODUCTION

The purpose of this study was to explore, describe, explain and analyse social engineering attacks through an integrated MIT approach. This was done to better understand, measure and explain such attacks as a means to formulate a proactive strategy (vide section 1.4.1) to prevent such attacks. In order to achieve this aim, the study needed to explore and describe the occurrence and nature of social engineering attacks, as well as to explore and describe the awareness of social engineering attacks and information security (vide section 1.4.2). These specific objectives were achieved through a business and an individual perspective, as explained in Chapter 5.

The process of analysis and interpretation is a process of finding meaning. This process can be likened to that of translation; the researcher engages in a process of transforming raw data into a meaningful depiction of patterns and relationships (Royse, 2008: 318). The analysis and interpretation of the raw data are mandatory requirements for answering the research questions. Thus, the raw data were described, analysed and interpreted.

In order to yield an individual perspective on social engineering and related information security matters, data were collected by means of a self-administered questionnaire (Annexure I) from respondents within the community of Tshwane located in Gauteng, South Africa. The researcher collected the data over a period of three months (March, April and May 2016) once ethical clearance had been obtained (see Annexure A). A total of 114 respondents completed the questionnaires satisfactorily, although 150 questionnaires were given out – rendering a response rate of 76 per cent. The reasons why the remaining questionnaires were left unanswered can be attributed to limited time or personal beliefs and/or lost or misplaced questionnaires.

As discussed in Chapter 5, descriptive statistics were used to analyse the quantitative data. The researcher made use of a spreadsheet program, Microsoft Excel, to organise the numerical data collected. Descriptive analysis was used to analyse the data, as the study is preoccupied on frequencies and central tendencies. This chapter provides a comprehensive discussion of the data analysis and interpretation of the data collected from the self-administered questionnaires (Annexure I).

7.2 ANALYSIS AND INTERPRETATION OF SELF-ADMINISTERED QUESTIONNAIRES

Data analysis entails correlating meaning to the findings collected and comparing those findings to other research studies (Bernard, 2013: 394). By making use of the self-administered questionnaires, two types of data were accumulated – categorical and numerical data. As explained in paragraph 5.6 (vide Chapter 5), the former denotes variables, while the latter provides measurements or counts. In addition, the univariate method of analysis was used as single variables were analysed in an effort to describe the variable (Fouché & Bartley, 2011: 249). In reference to section 5.8.4 (vide Chapter 5), data triangulation was achieved by making use of a mixed methods study. This was done by investigating various aspects relevant to the study – a literature study, interviews and questionnaires.

In order to allow for the simplification of data representation, the researcher rounded off the numerical data. Thus, in some cases the totals do not add up to 100 per cent. In some instances, the researcher deemed it necessary to quote the research respondents verbatim in order to exhibit accurate explanations. When directly citing the research respondents, the respondents are referred to according to the number allocated to their questionnaire, such as Research Respondent 1 (e.g.: RR1). For the purpose of this study, the researcher used both tables and charts to present the data collected from research respondents.

The data received were conceptualised into relevant themes. The tables and charts are designated under specific themes and presented, analysed and explained. Furthermore,

the data are substantiated by current literature and often cites previous chapters to determine the veracity of the findings. The data will be presented in the following eight sections:

- SECTION A: Biographical details.
- SECTION B: Employment details.
- SECTION C: General use of communication through technology.
- SECTION D: Identification and authentication.
- SECTION E: Access control.
- SECTION F: Social engineering.
- SECTION G: Legislation related to information security.
- SECTION H: Impact on information security awareness.

SECTION A

7.3 BIOGRAPHICAL DATA (Annexure I questions 1, 2, 3, and 4)

The sampling method employed to collect the data was discussed at length in paragraph 5.4.1.2 (vide Chapter 5). The study is characterised by a non-random sample, thus the comparisons and deductions made are limited to the group itself. All of the research respondents involved gave their consent to take part in the study, as the informed consent forms (Annexure H) were read, understood and signed. The biographical characteristics of the study group are presented in tabular format in an effort to describe the study group. The following demographic components were present in the sample:

Table 7.1: Biographic characteristics of the respondents (N=114)

Gender			
	Frequency	Percentage (%)	Rank
Male	52	46%	2
Female	62	54%	1
Race			
	Frequency	Percentage (%)	Rank
Black	54	47%	1
Coloured	13	11%	3
Indian	6	5%	4
White	41	36%	2
Age			
Age	Frequency	Percentage (%)	Rank
18 – 24 years	18	16%	3
25 – 30 years	36	32%	1
31 – 35 years	22	19%	2
36 – 40 years	11	10%	5
41 – 45 years	13	11%	4
46 – 50 years	2	2%	8
51 – 55 years	4	4%	6
56 – 60 years	3	3%	7
61 – 65 years	2	2%	8
65 <	1	1%	9
Marital status			
Marital Status	Frequency	Percentage (%)	Rank
Single	60	53%	1
Married	51	45%	2
Divorced	3	3%	3
Widow(er)	0	0%	4

▪ **Gender**

The research respondents were closely divided into male (46%) and female (54%).

- **Age**

The research respondents made up various age groups. The majority of the research respondents were between the ages of 25 and 30 years old, while only one was over the age of 65.

- **Race**

The majority of the research respondents were black, followed by white, coloured and Indian.

- **Marital status**

Most of the research respondents indicated that they were single (53%), closely followed by those who indicated that they were married (45%). Only three per cent of the research respondents specified that they were divorced.

The subsequent section denotes the employment details of the research respondents.

SECTION B

7.4 EMPLOYMENT DETAILS

The research respondents were asked to provide details about their employment status. The researcher asked the respondents to provide their job description (see Annexure I question 6) as a means to evaluate what the respondent's job entails if the job title was unclear. However, the job titles provided were clear and the detailed descriptions, in some cases, contributed further clarity.

7.4.1 Occupation (N = 112) (Annexure I question 5)

The research respondents indicated their employment status. These occupational ranks varied in terms of unemployment, full-time students, non-professionals, semi-professionals and professionals. The sample represented individuals who held managerial or director positions, safety and security officials, including SAPS officials and

teaching and training practitioners. In addition, financial practitioners, administrators, sales and marketing representatives and HR practitioners were sampled. Although all individuals are vulnerable to social engineering attacks, the following groups are particularly vulnerable, as outlined in Chapter 2 (vide section 2.5): management and executives, administrators, financial and HR practitioners.

7.4.2 Time period of employment (Annexure I question 7)

The research respondents were asked to document their time period of current employment. The responses indicated that 93 per cent (n = 106) of the research respondents answered this question satisfactorily. The results varied throughout the annual categories. However, most of the research respondents (25%) attested that their period of current employment was less than or equal to one year. As mentioned previously, (vide sections 2.4.3 and 2.8) new employees are most at risk to social engineering attacks, as they are not yet well-acquainted with fellow colleagues, structural components within the organisation or the organisational layout.

The following section represents the general use of communication through technology, as specified by the research respondents.

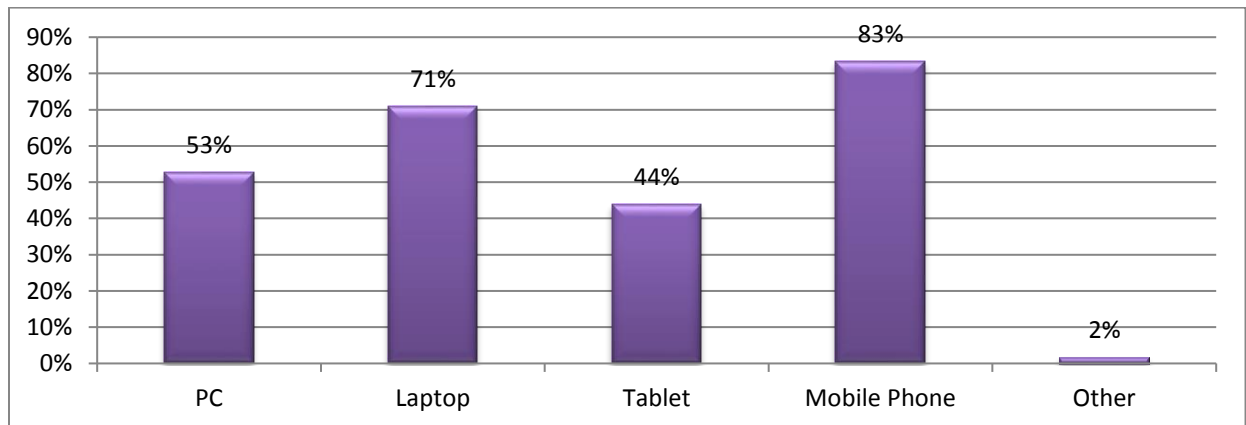
SECTION C

7.5 GENERAL USE OF COMMUNICATION THROUGH TECHNOLOGY

Online communication is a vital component of modern culture (Wood & Smith, 2014: 3). For this reason, the researcher enquired about the research respondents' general use of communication through technology.

7.5.1 Technological devices (Annexure I question 8)

Chart 7.1: Technological devices used by respondents (N = 114)



The research respondents were requested to indicate which technological devices they made use of when accessing the internet. The respondents were allowed to select more than one option, as many technological devices can be used. The average device usage was determined as follows: 21 per cent of the research respondents selected all four devices; 31 per cent selected three devices; 28 per cent two devices; while 20 per cent selected only one device. Thus, most of the research respondents verified that they either used four or three technological devices to access the internet. The more devices individuals use, the more vulnerability is increased as well as eventual risk endorsed.

Most of the research respondents shared that they made use of mobile phones and laptops to access the internet. This was closely followed by personal computers and laptops. Interesting to note is that one respondent (Research Respondent 14) indicated that he accessed the internet through the television and Playstation. If not properly guarded against, this could make him vulnerable to a social engineering attack illustrated in Chapter 3 (vide section 3.3.1.2).

In 2014, Statistics South Africa distributed the General Household Survey Report conducted in 2013. The report revealed that 40.9 per cent of South African households have at least one member who either used the internet at home or had access to it

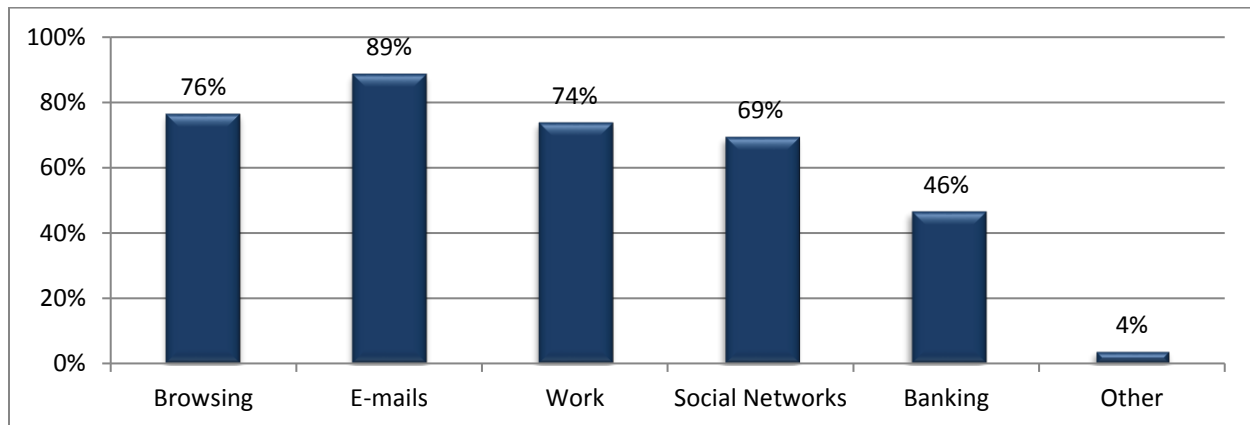
somewhere else. This statistic increases when Gauteng is reviewed, as 54.0 per cent have access to the internet (Duff, 2014). As mentioned in Chapter 5 (vide section 5.5.1), internationally people have more access to mobile phones than to working toilets (Wang, 2013). Similar to the results found in Chart 7.1, current studies in South Africa have shown that most South African internet users use their smartphones to access the internet (Alfreds, 2016; Thomas, 2014; Tubbs, 2015). The internet is one of the main tools used in social engineering attacks. This is illustrated through the various types of technology-based social engineering attacks (vide section 2.6.1).

7.5.2 Frequency of internet usage (Annexure I question 9)

The research respondents selected a wide range of options regarding the prevalence of internet usage. Two respondents did not indicate their daily internet usage (N = 112). The majority of research respondents (19%) indicated that they spent less or equal to two hours on the internet per day. These results are contrary to current literature, as modern culture denotes an increase of internet usage. This is supported by literature, as it is estimated that by 2019, internet traffic in South Africa will be approximately 267 times greater than the capacity of the entire South African internet in 2005 (Vodacom, 2016). However, by answering the question posed, the research respondents (98%) indicated that they used the internet on a daily basis. Thus, it can be proposed that the more one participates in internet-based activities, the more one is at risk to social engineering attacks.

7.5.3 Reasons for internet use (Annexure I question 10)

Chart 7.2: Reasons for internet use (N = 113)



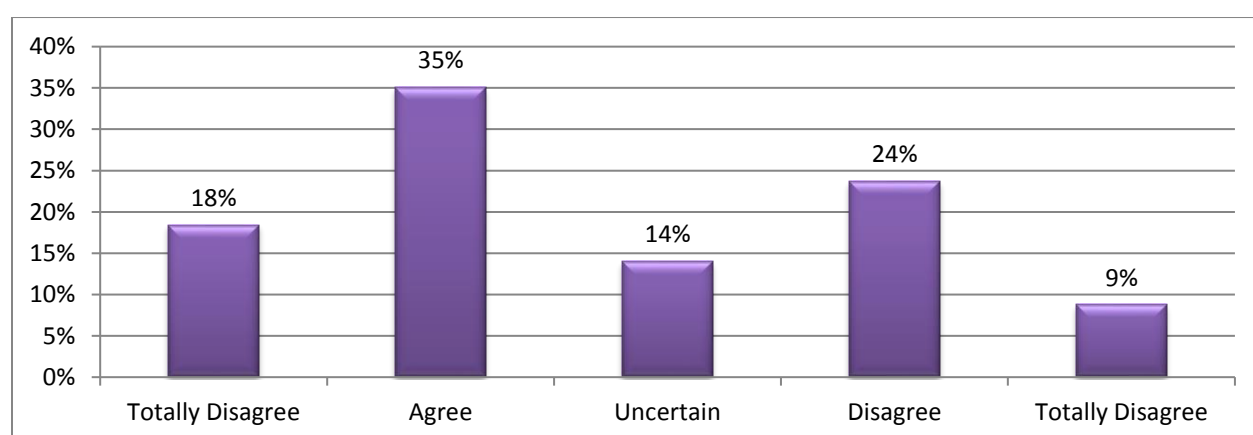
A large majority (99%) of the research respondents indicated reason(s) for using the internet. The research respondents were allowed to select more than one option. The average reasons for usage of the internet were indicated as follows: three per cent selected six reasons; 26 per cent selected five reasons; 29 per cent selected four reasons; and 24 per cent selected three reasons. Only 10 per cent and nine per cent selected two and one reason respectively.

Most of the research respondents indicated that they used the internet for e-mails (87%), browsing (76%), work purposes (74%) and social networking (69%). The minority of options selected, 46 per cent of the research respondents, indicated that they used the internet for banking purposes. Internet banking promotes convenience, accessibility and safety (in terms of avoidance of contact crime). Social engineers can target users who subscribe to internet banking through various methods. These include authorising false online payments or making an internet payment in order to cover the administration fees of a job offer or competition (Febelfin, 2014). A few research respondents (4%) indicated that they used the internet for online shopping. However, the various reasons for the use of the internet create a pervasive risk, as it depends on the users' behaviours and safety precautions taken.

7.5.4 Accessibility of personal information (Annexure I questions 11 and 11.1)

The research respondents were asked to specify the extent to which they considered their personal information accessible to the general public. Thus, the findings are based on the research respondents' own perceptions regarding the accessibility of their personal information. The results are depicted in the chart below.

Chart 7.3: Accessibility of personal information (N = 114)



Most of the research respondents (35%) agreed with the perception that their personal information is accessible by the general public. This was closely followed by 24 per cent of the research respondents disagreeing with the statement. However, 18 per cent of the research respondents totally agreed that their information is available to the general public, as opposed to nine per cent totally disagreeing to the statement. Interestingly, 14 per cent of the research respondents were uncertain about the accessibility of their personal information. This substantiates their unawareness of good information security practices in an effort to guard against social engineering attacks.

The respondents were asked a follow-up question (see Annexure I question 11.1) to provide reasons for their answers. Although some research respondents did not provide any explanation, the reasons that were provided are divided according to how the research respondents answered the question.

For those who answered “totally agree” and “agree” the following relevant reasons were extracted from the data obtained:

RR2: “Social networking makes my information readily available by means of a simple Google search.”

RR4: “I have attempted to Google myself and I have found my information and picture.”

RR5: “No personal firewall is activated on my devices.”

RR9: “As a real estate agent, clients must have your information.”

RR13: “Due to Facebook, people are able to access my personal information.”

RR24: “Most of my online activity requires my personal information and is thus accessible to the general public.”

RR30: “No matter the security, I am aware that there are ways to access anyone’s info.”

RR32: “Credit providers have my information.”

RR37: “My information is available for work purposes.”

RR49: “For work related purposes I have to disclose my cell number on internet documents that will be accessed by the public.”

RR58: “I check in on social networks and give my passwords to some of my family members.”

RR76: “I feel that any information that is done through/assessed through a network system (technology) can become assessable to the public.”

RR85: “When I Google search my name, a host of information comes up about me, such as my career and work details.”

RR99: “I have been a state witness in a fraud case whereby the bank sold personal information.”

RR111: “Because I know how easy it is to obtain information over the internet.”

The above excerpts provide clarity on why the research respondents perceived their information to be available to the general public. They cited networking, credit service providers and work purposes as the main reasons why they believed their personal information is available. These reasons are associated with one's way of living and may increase vulnerability to social engineering attacks as explained in Chapter 4 (vide section 4.2.1). Two respondents (RR4 and RR85) reported that they had Googled themselves and had seen the host of information it has generated. Research respondent 99 recounted that she had been a state witness in a fraud case where a particular bank sold personal information. Instances such as these expose that personal information is not as personal as it is assumed to be.

For those who answered "uncertain", the following relevant reasons were given:

RR1: "If it is anonymous, I don't mind."

RR8: "Personal information should be given or obtained with my consent."

RR75: "With hacking one may never know who has access to personal information."

RR95: "I am not confident that many of the agencies that request my information are able to have sufficient levels of security infrastructure to uphold or maintain confidentiality."

In the above extracts, uncertainty may fuel unhealthy information security practices, as the following question revealed. If an individual is unaware of their personal information being available to the general public, how then can they protect themselves against possible threats?

For those who answered "disagree" and "totally disagree", the subsequent applicable reasons were given:

RR15: "I always conduct a security check."

RR18: "It's dangerous in terms of fraud and safety."

RR43: “The internet is volatile and with a lot of IT tech specialists a lot of information is available to them. However, the general public may not have the necessary skills to hack your accounts.”

RR45: “I refrain from advertising personal information.”

RR73: “I consider myself a private person.”

RR80: “Only my work e-mail address and mobile number is posted on the web.”

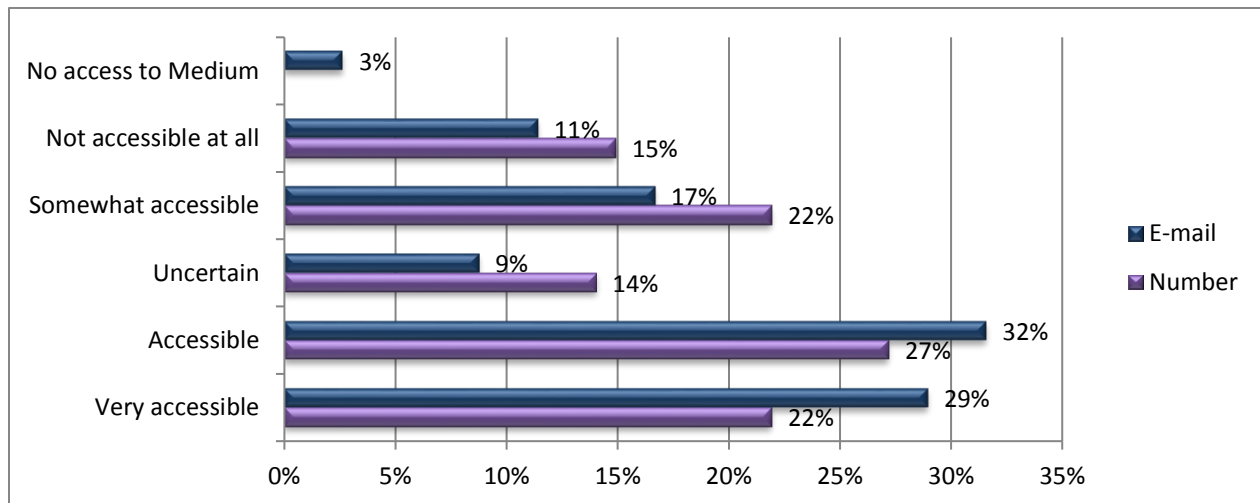
RR82: “Personal information, like login details, is usually encrypted and thus the average person in the general public wouldn’t be able to access it.”

RR108: “There is too much fraud and people misuse the information if it lands in the wrong hands.”

The citations provide insight as to why individuals believed their personal information to be unavailable to the general public. These responses disclose some form of awareness about good information security practices. However, RR80 clarified that only her work e-mail address and mobile number was posted online. This is enough information to carry out a successful social engineering attack if one is not cautious. In addition, RR43 and RR82 believed that the general public would not have enough skills to use their personal details against them. A social engineer merely needs to obtain such details to orchestrate an attack against an unsuspecting target.

7.5.5 Accessibility of telephone number and e-mail address (Annexure I questions 12 and 13)

Chart 7.4: Accessibility of telephone number (N = 114) and e-mail address (N = 111)



The research respondents were asked to indicate the extent to which they considered their telephone number and e-mail address to be accessible to the general public. The results of these questions posed are combined to display their comparative nature and because most of the research respondents allocated the same reasons for questions 12.1 and 13.1. The results are illustrated in the above bar chart. The reasons provided yield similar results for both telephone numbers and e-mail addresses. The majority of the research respondents indicated that they believed their e-mail address (32%) and telephone number (27%) are accessible to the general public. This was closely followed by the perception that these details are very accessible (29% and 22% respectively). Some of the research respondents believed this information to be somewhat accessible (17% and 22% respectively), whereas others reported it to be not accessible at all (11% and 15% respectively). A few research respondents (3%) indicated that they had no access to e-mail services.

The overall perception that the research respondents' contact details are accessible to the general public is rooted in the lifestyle exposure theory discussed in Chapter 4 (vide section 4.3.1). Whether personal information is being shared intentionally or unintentionally, personal information is becoming more accessible. Furthermore, this section highlights the absence of capable guardianship discussed earlier in section 4.3.2.

SECTION D

7.6 IDENTIFICATION AND AUTHENTICATION

7.6.1 Contact with personal information (Annexure I question 14)

Table 7.2: Contact with personal information (N = 112)

	Very often	Often	Seldom	Not at all
Biographical information	12%	27%	40%	21%
Information relating to the education or the medical, financial, criminal or employment history	11%	31%	29%	29%
Any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment	19%	32%	30%	19%
Personal opinions, views or preferences	30%	37%	20%	13%
Correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence	8%	22%	39%	30%

The research respondents were requested to indicate to what extent they come into contact with personal information that does not belong to them. The categories were derived from what the PoPI Act clarifies personal information to be (vide section 3.3.1.2). The majority of the research respondents shared that they came into contact with personal information of others the most, be it very often (30%) or often (37%). This could

be attributed to the variety of social networking applications where people can voice their opinions through text, pictures and videos.

7.6.2 Perception that personal information can be used in an attack (Annexure I question 15)

Table 7.3: Perception that personal information can be used in an attack (N = 111)

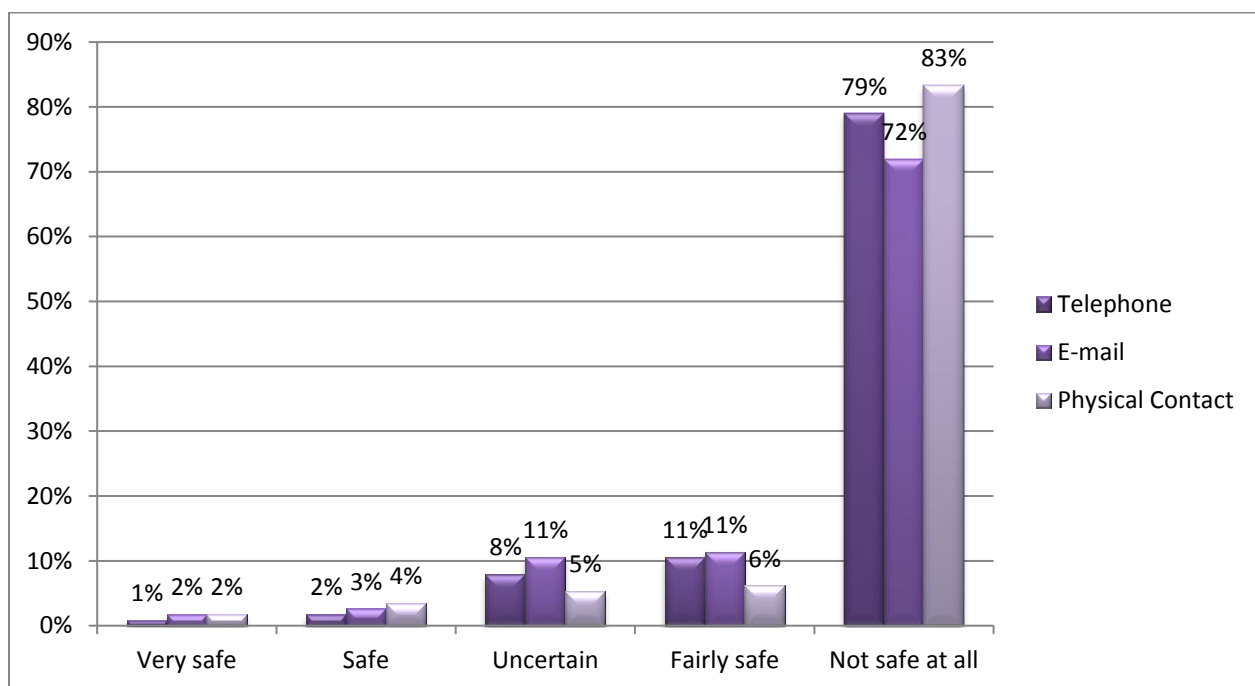
	Highly possible	Possible	Fairly possible	Impossible
Biographical information	30%	35%	23%	13%
Information relating to the education or the medical, financial, criminal or employment history	36%	32%	20%	13%
Any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment	46%	34%	11%	9%
Personal opinions, views or preferences	25%	30%	34%	11%
Correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence	28%	33%	27%	12%

The research respondents were requested to indicate to what extent they believed their personal information could be used against them. The categories were derived from what the PoPI Act denotes as personal information (vide section 3.3.1.2). The above table depicts that the research respondents (46%) regarded information such as any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment as highly possible to be used in an attack against them.

In a recent article written by Lotz (2016), South Africans are warned against the over-sharing of information. The article acknowledges that while a culture of information sharing is maintained in South Africa, South Africans are unaware of how this could be harmful to them. Lotz (2016) explains that every time an individual posts something online a digital footprint is generated.

7.6.3 Identification and authentication via telephone, e-mail and physical contact (Annexure I questions 16, 17 and 18)

Chart 7.5: Identification and authentication via telephone (N = 114), e-mail (N = 112) and physical contact (N = 114)



The research respondents were requested to specify the extent to which they perceived providing their identification and authentication via the telephone, e-mail and physical contact as safe. A large majority of the research respondents indicated that sharing of

such details is not safe at all. Identification and authentication via telephone, e-mail and physical contact were regarded as not safe at all by 79 per cent, 72 per cent and 73 per cent respectively. These results are contradictory to literature regarding the psychology of social engineering (vide Chapter 3). Human nature can be manipulated when elements such as trust, persuasion, conformation, compliance and ingratiation are exploited (vide section 3.2). However, some research respondents indicated that sharing personal details could be considered as fairly safe, especially via e-mail. This could be due to the paper trail left by e-mail communication. The research respondents who indicated that they were uncertain what to do when identification and authentication were requested, could be considered as being information security conscious. They would first need to analyse the situation before releasing personal information.

7.6.4 Electronic signature (Annexure I question 19)

The research respondents were asked to specify if they made use of an electronic signature (e-signature). All of the research respondents responded to the question (N = 114). The results were closely allied, as 50 per cent of the research respondents indicated that they did, while 47 per cent indicated that they did not. Most of the respondents who worked in professional or administrative settings made use of e-signatures.

South African legislation also makes provisions for the acceptance of e-signatures within the ECT Act (vide section 3.3.1.1). The accepted examples of e-signatures include a typed name at the end of an e-mail, a scanned image of a handwritten signature as well as a digital signature (Republic of South Africa, 2002). Wood (2010: 1) explains that a signature is pragmatic and valuable in that it is an illustrative mark used as a method of assurance that an object has been generated, approved or validated. In turn, e-signatures serve the same purpose. However, as sustained by Wood (2010: 1), e-signatures can be exploited through social engineering techniques in an effort to defraud the target. E-signatures can be easily copied if pasted in a Word Document or through a converted Portable Document Format (PDF). Furthermore, an e-signature which is handwritten and scanned to an e-mail address can still be copied. Thus, accompanied with legislation

accepting the legality of e-signatures and the ease in obtaining it, vulnerability is increased.

The following section discusses access control as practised by the research respondents.

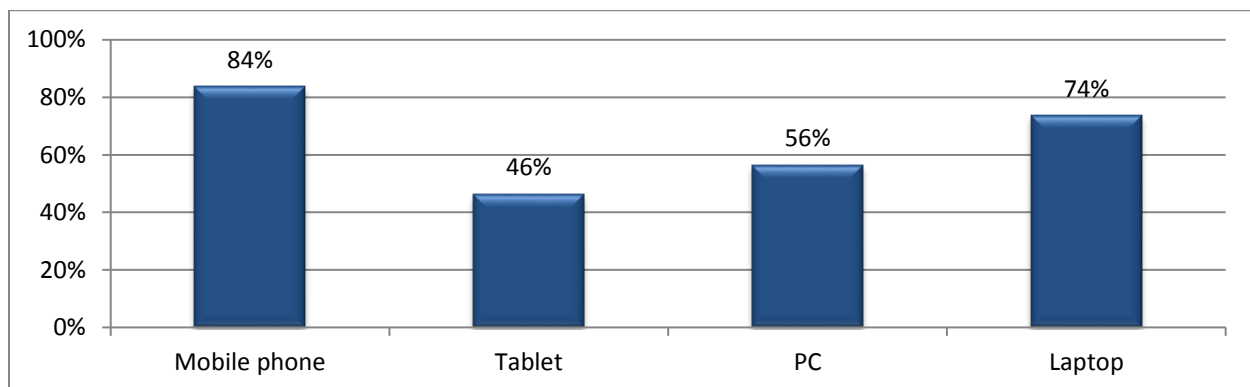
SECTION E

7.7 ACCESS CONTROL

Access control is a vital constituent in a successful social engineering attack. Accordingly, the research respondents were asked to provide clarity on the control of access regarding their personal information.

7.7.1 Password protection of technological devices (Annexure I question 21)

Chart 7.6: Password protection of technological devices (N = 110)

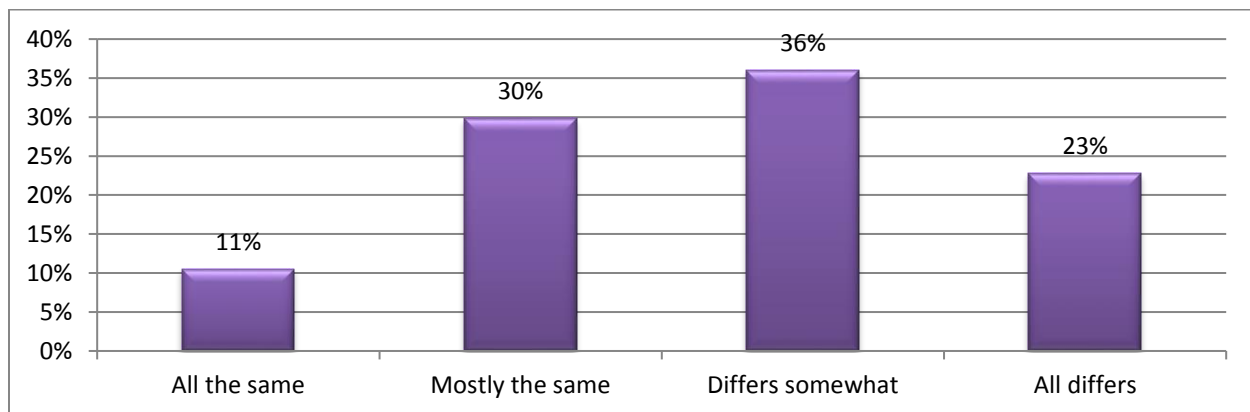


The research respondents were requested to indicate which of their devices were password-protected. The data yielded the following results: 84 per cent of the research respondents said that their mobile phones were password-protected, followed by the password protection of laptops (74%), personal computers (56%) and tablets (46%). The use of passwords for these technological devices can reduce the risk of being targeted in

a social engineering attack. However, these results are largely affected by several factors as elaborated on below(vide sections 7.7.2; 7.7.3 and 7.7.5)

7.7.2 Similarity of passwords (Annexure I question 22)

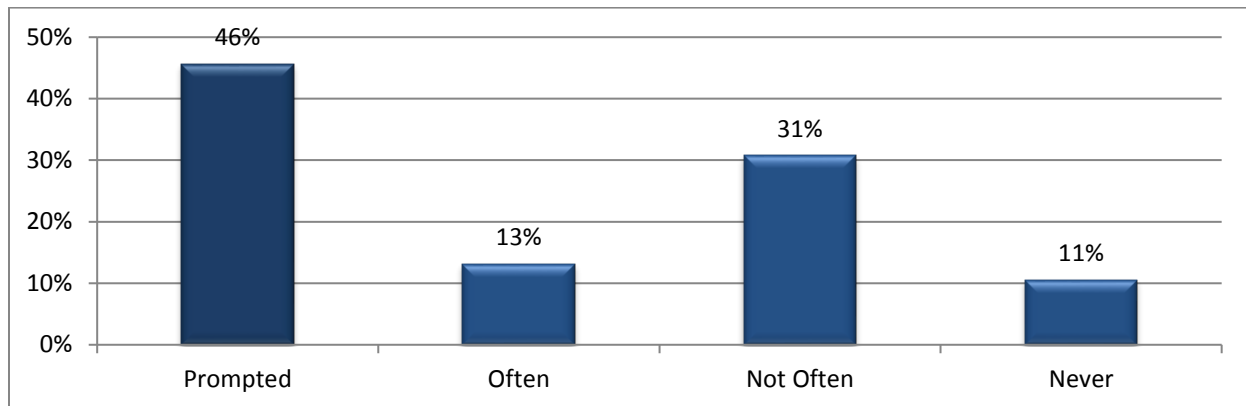
Chart 7.7: Similarity of passwords (N = 113)



The research respondents were asked about the extent of similarity between their passwords. Most of the research respondents (36%) indicated that their passwords differed somewhat, while this was closely followed by the response that most of the passwords were the same (30%). Though it is easier to use the same passwords for multiple sites or technological devices, passwords which are the same induce the ease of social engineering attacks. Once a social engineer has access to any password, they could test the same password on the site or technological device they seek access into. RR30 indicated in question 13.1 (see Annexure I question 13.1) that she regularly changed her passwords with symbols and number characters for safety reasons. This statement is very telling in that it shows how easily the research respondent can unintentionally reveal personal information.

7.7.3 Frequency of password modification (Annexure I question 23)

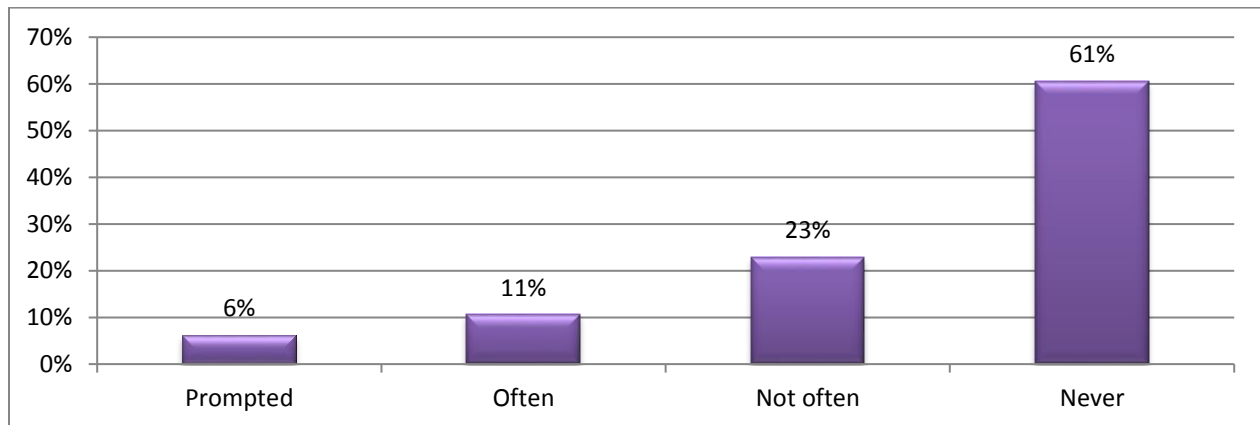
Chart 7.8: Frequency of password modification (N = 114)



The research respondents were asked how frequently they changed their passwords. The majority of the research respondents (46%) revealed that they only changed their passwords when prompted. The research respondents who indicated that they did not change their passwords often, totalled to 31 per cent of the sample. Interesting to note is that 11 per cent of the research respondents stated that they never changed their passwords, increasing their risk to various information security breaches. Only 13 per cent of the research respondents indicated that they changed their passwords often.

7.7.4 Websites and password control (Annexure I question 24)

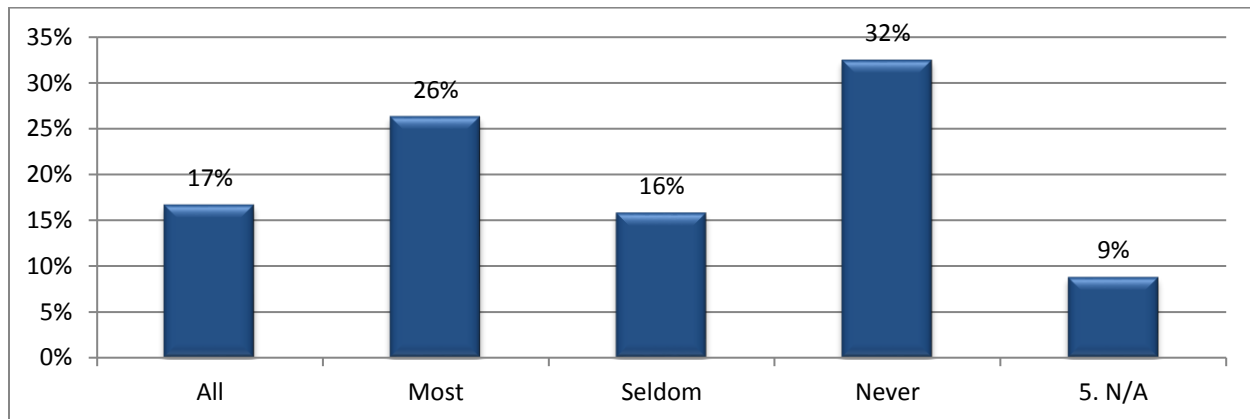
Chart 7.9: Websites and password control (N = 114)



The research respondents were asked how often they allowed websites to remember their usernames and passwords. Most of the research respondents (61%) answered that they never allowed websites to remember their password. This reveals good information security practice. The remaining research respondents indicated that they did not often (23%), often (11%) and only when prompted (6%) allow websites to remember their details. All of these research respondents are at risk to social engineering attacks and related information security breaches, especially if they use public or shared technological facilities. In addition, retrieving username and password details from websites causes increased risk when technological devices are lost or stolen.

7.7.5 Social network applications and password control (Annexure I question 25)

Chart 7.10: Social network applications and password control (N = 104)



The research respondents were asked how often they kept their social networking applications logged on. Most of the research respondents (33%) declared that they never kept their social networking application logged on, while 16 per cent indicated that they seldom kept these applications logged on. However, 26 per cent of the research respondents, the second highest percentage, revealed that they kept their social networking applications logged on most of the time, while 17 per cent of the research respondents said they kept their applications logged on all of the time. Due to the frequent use of social networking applications, users may prefer to keep these applications logged on all or most of the time. However, this could generate the same kind of risk, as discussed in section 6.8.2.

7.7.6 Accessibility of passwords (Annexure I question 27)

The research respondents were asked if anyone had access to their passwords. All of the research respondents answered the question (N = 114). A large majority of the research respondents (63%) indicated that no one had access to their passwords, while 37 per cent of the research respondents indicated that someone else did have access to their passwords. Most of the people who shared passwords attributed the known passwords

to their spouses, family members, colleagues or management. The sharing of passwords allows for more targets in a social engineering attack. Now, the social engineer can use other people to retrieve sensitive information.

SECTION F

7.8 SOCIAL ENGINEERING

Section A to E set the tone for the remaining part of the questionnaire. It allowed the research respondents to be acquainted with the nature of the research study. Section F specifically asked questions regarding social engineering threats and attacks experienced by the research respondents.

7.8.1 Social engineering awareness (Annexure I questions 28 and 28.1)

All of the research respondents answered this question (N = 114). Most of the research respondents (73%) indicated that they did not know what the term social engineering meant while 27 per cent indicated that they were familiar with the terminology. Knowledge is power; the more people who are educated on social engineering and information security practices, the less risk they will be at falling victim to an attack.

The following responses represent the research respondents who, to some extent, correctly indicated what social engineering is:

RR2: “When someone pretends to be someone they are not in an attempt to gain access to your personal information, to use in an attack against you or your company or anything you might have access to.”

RR6: “When people access your personal e-mail or social network account. Hacking account – bank (credit card scam or social – post things using your account without permission).”

RR8: “Social engineering is when a person is hacked through the internet, e-mail cell phone and their personal information is obtained.”

RR14: “Tricking people into giving up their personal information (i.e. bank details, e-mail account information.”

RR15: “An attack that normally involves tricking people with the aim of gaining personal information.”

RR31: “Gathering information about a person using social media.”

RR33: “Social engineering is the act of trying to get information about you or your company in an attempt to perform an act to their own benefit e.g. to hack your account.”

RR36: “It’s a new way...maybe not that new, but it’s pretty much online scamming and hacking.”

RR44: “Tricking people into breaking normal security procedures.”

RR71: “To use psychology in order to gain access to personal information.”

RR72: “It is an attack vector used heavily on human interaction involving tricking people into breaking normal security procedures.”

RR73: “Social engineering is a way of manipulating people into providing or giving up confidential information.”

RR79: “Social engineering is the art of manipulating people so that they give up confidential information.”

RR81: “The retrieving of an unaware person’s personal information for one’s own financial gain or for malicious use.”

RR88: “Social engineering can be defined as using social media platforms to gain unauthorised access to private and confidential information of individuals.”

RR89: “Using personal relationships to gain trust and extract personal information from somebody that they would otherwise divulge.”

RR93: “Soliciting information (personal or sensitive) through normal courses of interaction and conversation. The end goal is to obtain certain information.”

RR97: “Misleading people to obtain information. Example: phishing.”

RR98: “Techniques used to obtain information that can be used to gain access to the computers that access personal information.”

RR99: “If someone manipulates another to give confidential information.”

RR111: “It is the way that attackers get unexpected users to break normal security procedure (human responses).”

Although some research respondents believed they knew what social engineering is, their responses proved this to be a misconception:

RR7: “Theft via electronic devices.”

RR9: “The use of propaganda by an authoritarian government to sway perceptions and attitudes of its own citizens.”

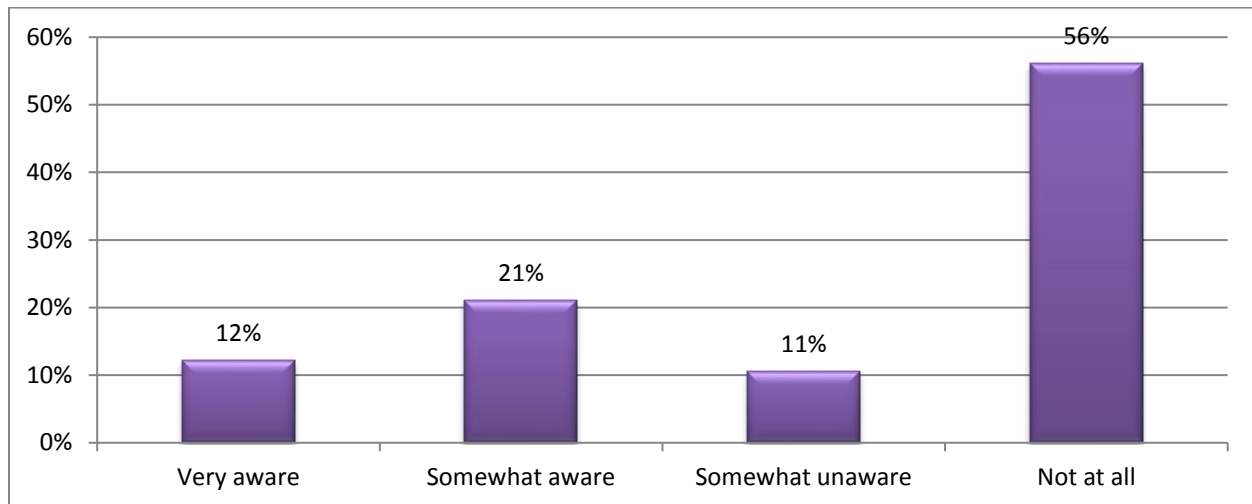
RR37: “It is all social network systems like Whatsapp, Facebook and Instagram.”

RR38: “Social media like Whatsapp or Facebook.”

RR40: “I do not know what the exact term is, but I assume it has to do with everyday contact via technology, sharing information etc.”

7.8.2 Awareness of social engineering threats (Annexure I question 29)

Chart 7.11: Social engineering awareness (N = 114)



The research respondents were asked if they were aware of social engineering threats. Most of the research respondents (56%) indicated that they were not at all aware of any social engineering threats. The remaining respondents indicated that they were very aware (12%), somewhat aware (21%) and somewhat unaware (11%) of social engineering threats.

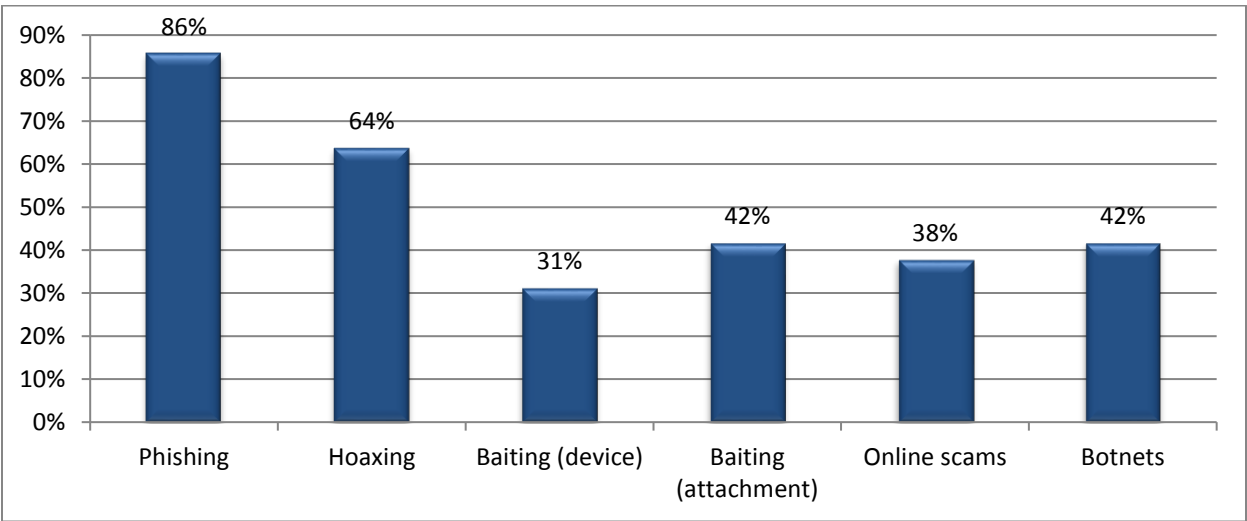
7.8.3 Exposure to social engineering threats (Annexure I question 30)

The researcher was aware that the research respondents might not be familiar with terminology relating to social engineering threats and attacks, therefore refrained from using it. Alternatively, the researcher used explanations and examples to retrieve information from the research respondents. All of the research respondents answered the question (N = 114). The large majority of the research respondents (70%) had been exposed to some sort of social engineering attack based on questions 31, 31.2, 32 and 32.1 (see Annexure I questions 31, 31.2, 32 and 32.1). Only 19 per cent of the research

respondents confirmed that they had never been exposed to a social engineering attack, while 11 per cent indicated that they were unsure.

7.8.4 Technology-based social engineering (Annexure I questions 31 and 31.2)

Chart 7.12: Technology-based social engineering (N = 77)



The above bar chart represents the types of technology-based social engineering attacks the research respondents had been exposed to. Technology-based social engineering threats were much more prominent than human-based social engineering. This is evident as more research respondents indicated that they had been exposed to technology-based threats, as opposed to human-based social engineering. In most instances, even though the research respondent selected a particular option within question 31 (see Annexure I question 31), they did not elaborate on it in question 31.1 (see Annexure I question 31.1). The research respondents were allowed to select more than one option.

Details of the attacks, as explained by the research respondents, can be divided into categories as informed by section 2.6.1 (vide Chapter 2).

7.8.4.1 Phishing (N = 66)

The majority of the research respondents (86%) reported having been exposed to a phishing attack. Many research respondents (RR81, RR82, RR83, RR85, RR93, RR95, RR96, RR97 and RR113) detailed similar explanations in this section, thus these recurring responses were not included.

RR1: “I have experienced this every week in some form or other.”

RR4: “I have received fake e-mails from people saying that I have inherited money and asking for my banking details.”

RR9: “Received SMSs indicating that I have won a large amount of money and that I would have to contact them to claim the funds.”

RR10: “Once I was phoned by someone from a bank wanting to confirm details which I started doing but then realised that it didn’t sound right so I cut the call.”

RR15: “I have received an SMS with the details that I had entered a competition that I never entered.”

RR17: “I have received e-mails claiming that I have a refund from SARS requesting to click on the link, which I didn’t do. I have also received e-mails from FnB asking for personal information, which I ignored.”

RR18: “SMSs saying “You have won R950000 in the Rica promotion. Please contact...to claim prize”. I have also received e-mails from people who claim to be dying and would like to leave their millions to me.”

RR27: “I received an e-mail claiming that someone had passed away and left me an inheritance. I just needed to send my banking details and ID number.”

RR30: “E-mails received from unknown sources, but I did not open them and deleted them straight away.”

RR31: “I have received an SMS saying I have won the UK lottery.”

RR33: “I have received e-mails from ‘SARS’ claiming that they owe me money and asked me to click on the link.”

RR39: “I have received an SMS claiming that I won a big amount of money from Omo. I read in the newspaper that this is a hoax. On a weekly basis I receive an SMS claiming that I won R10000.”

RR40: “I usually receive e-mails claiming to come from legitimate banks such as ABSA or Nedbank (where I do not nor have ever banked before) prompting me to provide information. I also receive the occasional e-mail from SARS stating that I have unclaimed money (or something to that affect) and to click on the provided link.”

RR49: “I have received an SMS that my bank has been hacked; then I went to the bank to find out if it was true. I did that because the SMS said that I must put down my ID number for identification. My bank informed me that they had not been hacked.”

RR57: “It was in the form of winning a competition. When going through the details of the competition, it required me to enter my personal details - then my curiosity [suspicion] was alerted – how did I win a competition if my details are not with them.”

RR88: “I received e-mails from an address claiming to be from SARS. The e-mail advised that a refund is due to me and I need to provide my banking details. This happened on a few occasions. I received e-mails from unknown persons claiming I have inherited a huge amount of money. The unknown person says before funds can be released I need to pay a fee. This happened on a few occasions.”

RR100: “I received fake e-mails trying to gain my banking details. I moved or deleted it and added it to my spam inbox. I received a few SMSs from a bank that claimed I had a loan with them and I needed to pay it or else I will be handed over. I ignored the SMS.”

7.8.4.2 Hoaxing (N = 49)

Although 64 per cent of the research respondents selected the category referring to hoaxing, none of them gave an explanation of the attack. This could be because the attack

stipulated in the question may have described what happened to the respondents, therefore they did not see a need to elaborate on this.

7.8.4.3 Baiting (N = 56)

The category of baiting was divided into baiting through a device (31%) or baiting through an attachment (42%). The following extracts denote the research respondents' elucidation on baiting attacks:

RR17: "I once accidentally opened a file which had a virus and it corrupted my computer."

RR18: "I have had a virus on my laptop from clicking on an unknown link and I had to send it in for repairs."

RR100: "A flash drive from one of my classmates added a virus to my laptop. I receive e-mails that automatically go to my spam inbox."

To determine whether these attacks were intentional or malicious in nature would be difficult, since no further information is provided.

7.8.4.4 Online scams (N = 29)

The research respondents (38%) selected having been exposed to an online scam. The following extracts describe experiences by research respondents 40 and 42:

RR40: "This happened when I was still unaware of such threats and was downloading a computer program when the ad popped up. The ad stated that someone is trying to intercept my computer or that my computer has detected a virus and that I must click the button. Fortunately my brother is an IT specialist and was able to assist and recover my information without intrusion."

RR42: “The pop up I clicked affected my documents on my desktop and they couldn’t open.”

7.8.4.5 Botnets (N = 32)

The research respondents were asked if they had received any attacks through botnets. The research respondents (42%) who selected this option elaborated on it as follows:

RR9: “I receive spam which I am unable to stop receiving.”

RR10: “I receive numerous spam e-mails where they ask you to click on a certain link. Also, e-mails that you have won money where they ask you for your banking details. I have never responded to these.”

RR21: “Spam and fake e-mail. I did not follow the link.”

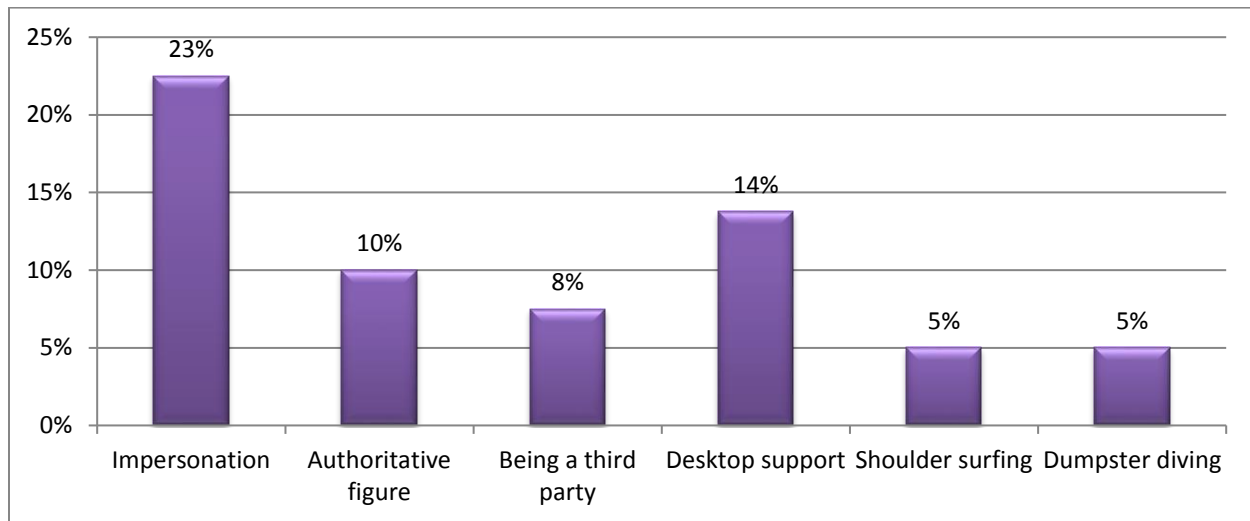
RR29: “I often get spam e-mails or links in e-mails from friends to click on links leading to hacking.”

RR32: “I can’t stop messages from coming to my phone. Sometimes I get an SMS asking me to give money or to release large sums of money from a ‘family member’ who is deceased.”

RR76: “Spam e-mails constantly pop up on my e-mail, sometimes containing malicious software.”

7.8.5 Human-based social engineering (Annexure I questions 32 and 32.2)

Chart 7.13: Human-based social engineering (N = 34)



The above chart depicts the types of human-based social engineering attacks the research respondents had been exposed to. The research respondents were allowed to select more than one option.

Details of the attacks can be divided into categories as set out in Chapter 2 (vide section 2.6.1).

7.8.5.1 Impersonation (N = 18)

Most of the research respondents (23%) who selected the impersonation category likened it to a phishing scam (see 6.8.4). This is understandable, as a successful social engineering attack incorporates various techniques. The research respondents shared the following experiences:

RR29: “Someone called pretending to be from a bank to get my personal information.”

RR30: “A person pretending to be from an insurance company tried to gain personal information from me and get payment from me but I did not give up any information and ended the call.”

RR37: “Once I was phoned by someone who told me that she is from Standard Bank. I asked her where is she phoning from and she said Johannesburg, although the number on my phone showed Bisho’s area code in the Eastern Cape.”

RR44: “I got a call from someone claiming to work at SARS. They asked for my ID and phone number and I was not comfortable with this. I told them to rather send my statement and I would take it from there.”

RR61: “My brother’s son pretended to be a consultant from Ackermans and asked me for my banking details in order to debit money I owe from the bank. But I caught him by voice before giving him my details.”

7.8.5.2 Authoritative figure (N = 8)

Although 10 per cent of the research respondents chose the authoritative figure example as an explanation of their own experiences, none of them shed light on this.

7.8.5.3 Being a third party (N = 6)

Only a few research respondents (8%) indicated that they had been exposed to social engineering through a third party. One respondent gave an account of this:

RR92: “Someone called about funds that were in my account incorrectly that I needed to reverse it as they were incorrectly in my account.”

7.8.5.4 Desktop support (N = 11)

The research respondents (14%) indicated that they had been exposed to social engineering through desktop support. Their responses reflect the following:

RR76: “I have received SMSs or e-mails saying that this is a member of technical support and I need to send personal information or provide personal information for the problem to be fixed.”

RR82: “A man messaged me on Facebook and told me he was with technical support. They apparently needed a password because I won a competition.”

RR111: ““Microsoft Call Centre”” call received explaining that Microsoft has to verify my details to be able to assist me in the future and Microsoft technical support requesting personal details to assist with activation of OS on my personal computer at home.”

7.8.5.5 Shoulder surfing (N = 4)

Only five per cent of the research respondents indicated that according to their knowledge they had experienced shoulder surfing:

RR10: “Once someone pretended to help me at an ATM machine in order to obtain my pin but I refused his help and had to do this twice before he left. At this stage I aborted the transaction and walked away.”

RR32: “Someone stole R2000 from me when I was at the ATM. They looked over my shoulder to see my ATM password.”

Research respondent 32 indicated that through shoulder surfing, money was stolen from his account. He also reported in question 35 (see Annexure I) that he did not report this as he had no faith in the Criminal Justice System.

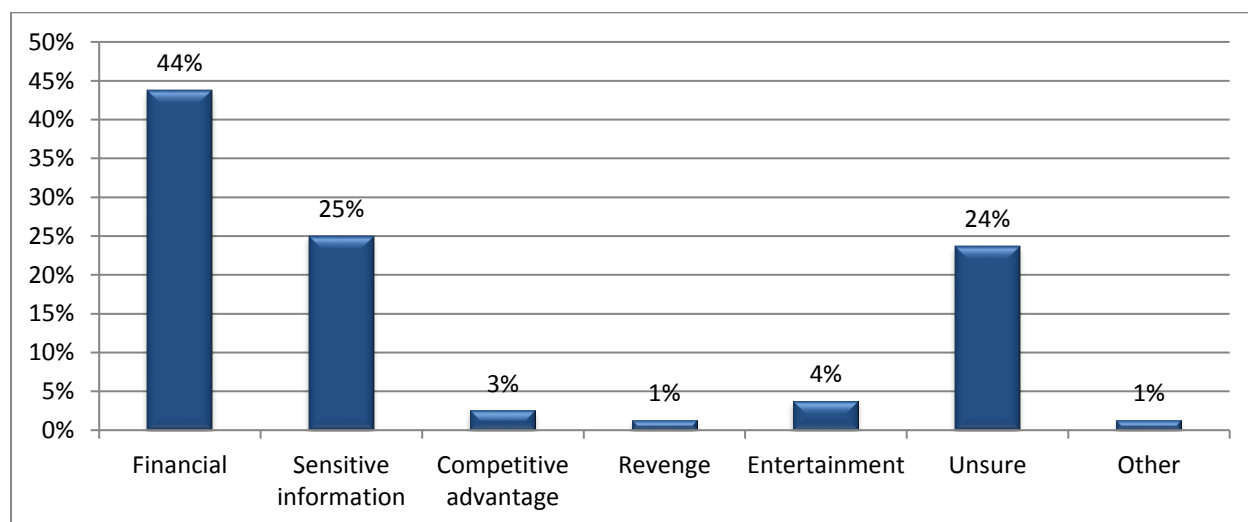
7.8.5.6 Dumpster diving (N = 4)

The research respondents (5%) who selected dumpster diving as an attack they had been exposed to, did not provide clarity on this matter. However, research respondent 49 elaborated on her experience in this regard:

RR49: “As a security manager, we discourage staff from tearing documents and throwing them in the bin. One of the colleagues did this and I collected the pieces and was able to read the content. I went to this person and he was surprised as to how I knew this information.”

7.8.6 Motives behind social engineering attacks (Annexure I question 33)

Chart 7.14: Motives for social engineering attacks (N = 63)

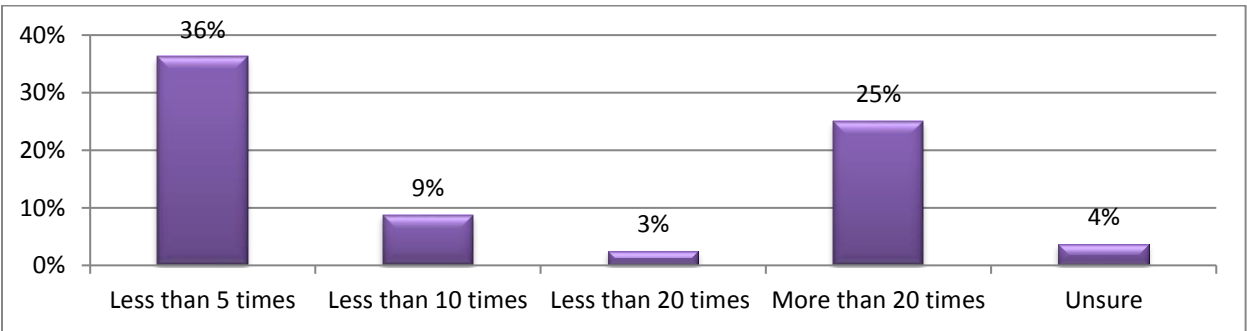


The research respondents were asked to provide insight on what they thought the motive for the social engineering attack(s) experienced in section 7.8.4 and 7.8.5 had been (see section 7.8.4 and 7.8.5). Granted, this section was not answered by all of the research respondents, but those who did answer indicated financial motives (56%) to be the main

motive, followed by access to sensitive information (32%), and 30 per cent indicated that they were unsure of the motives.

7.8.7 Frequency of threats received (Annexure I question 34)

Chart 7.15: Frequency of threats received (N = 62)



Only 62 research respondents of the 80 who acknowledged having been exposed to a social engineering attack, commented on the frequency of threats received. Most of the research respondents reported that they had received such threats fewer than five times (36%), followed by more than 20 times (25%) and fewer than 10 times (9%).

7.8.8 Reporting of social engineering attacks (Annexure I question 35)

This question was answered by 67 of the research respondents who answered “yes” to having been exposed to a social engineering attack. The majority of the research respondents (93%) who answered this question indicated that they had never reported an attack. The respondents cited reasons such as they simply ignored the threats or that the threat was not successful, so they did not see the need to report it. Moreover, the respondents indicated they did not know who to report it to and also maintained that no one would do anything about it if the incident was reported. The few respondents (7%) who did report the social engineering threats, conveyed the following:

RR49: “At the bank and to SAPS.”

RR51: “I called the police but no action was taken.”

RR89: “I have forwarded spam e-mails to the banks/SARS or any other organisation they were claiming to be from. I have also reported SMSs received from the network providers.”

RR111: “I reported the attacks to the relevant institution, including all parties implicated, along with the SAPS.”

RR113: “I reported it to the bank which I received the message from.”

The minority of research respondents who reported the social engineering attack helps in generating awareness to the relevant stakeholders.

7.8.9 Importance of information security (Annexure I question 36)

The research respondents were requested to share the level of importance they placed on their own information security. All of the research respondents answered this question (N = 114). The large majority (71%) of the research respondents clarified that they viewed information security to be very important, while 27 per cent of the respondents viewed it as important.

The section below provides an overview of the research respondents’ perceptions regarding legislation relating to information security.

SECTION G

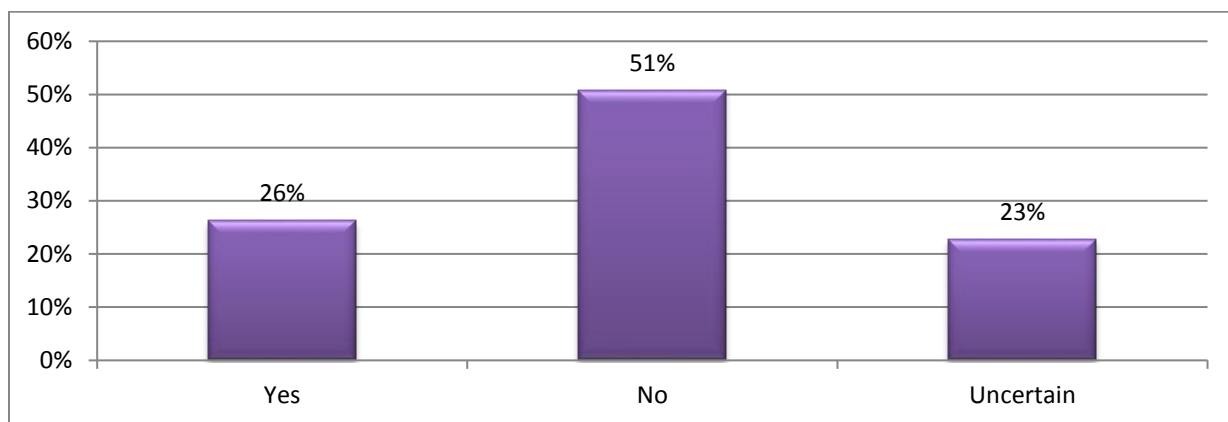
7.9 LEGISLATION RELATED TO INFORMATION SECURITY

As outlined in Chapter 3 (vide section 3.3), legislation is an important aspect in reviewing the topic under investigation holistically. The research respondents indicated their

awareness of South African legislation regarding information security and social engineering.

7.9.1 Awareness of South African legislation relating to information security and social engineering (Annexure I question 37)

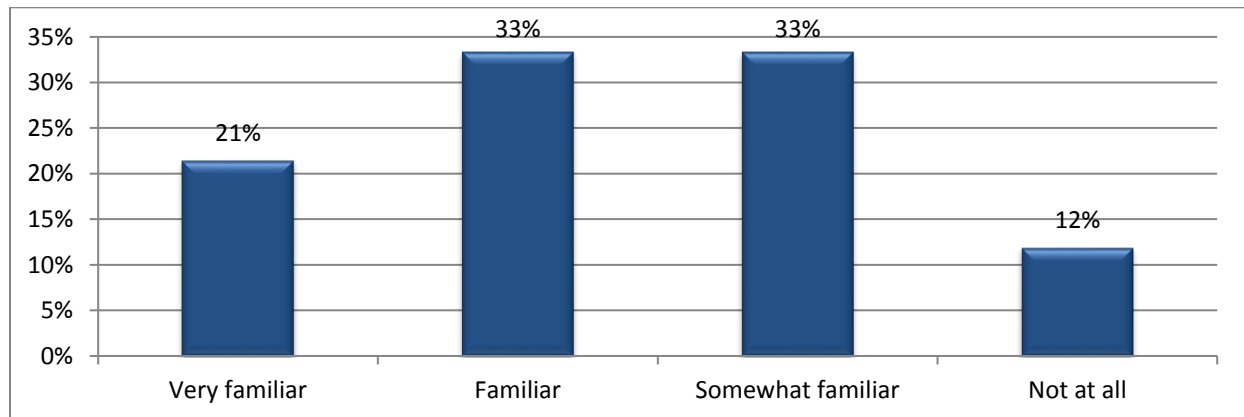
Chart 7.16: Awareness of South African legislation (N = 114)



Most of the research respondents (51%) revealed that they were not aware of any legislation addressing social engineering and information security. The results indicated that 26 per cent reported that they were aware of legislation, whereas 23 per cent were unsure.

7.9.1.1 Familiarisation with the Protection of Personal Information Act 4 of 20 (Annexure I question 37.1)

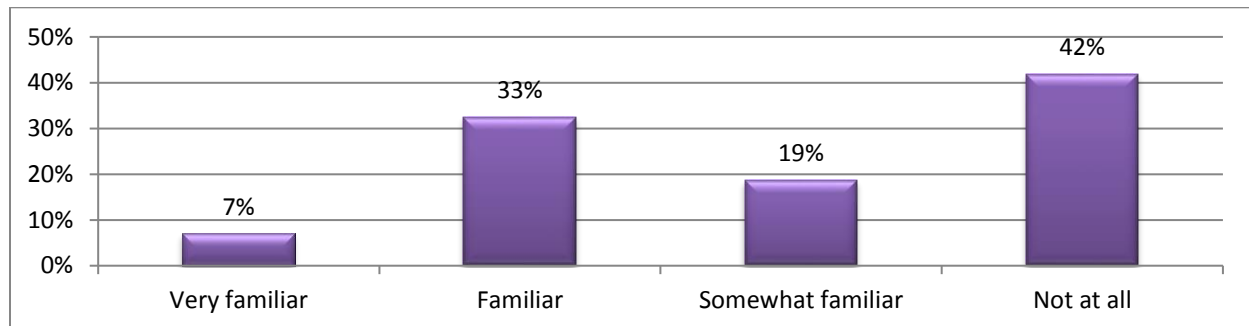
Chart 7.17: Familiarisation with the Protection of Personal Information Act (N = 42)



The research respondents who indicated that they were aware of South African legislation pertaining to social engineering and information security, were asked to specify their extent of familiarity with the PoPI Act. Equally, some of the research respondents indicated that they were familiar (33%) or somewhat familiar (33%) with the PoPI Act.

7.9.1.2 Familiarisation with the Electronic Communications and Transactions Act 25 of 2002 (Annexure I question 37.2)

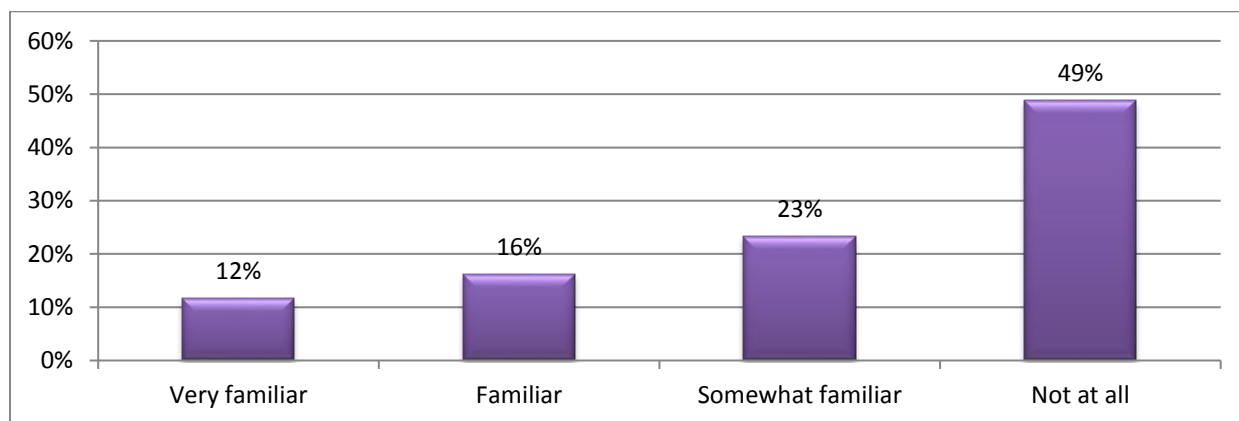
Chart 7.18: Familiarisation with the Electronic Communications and Transactions Act (N = 43)



The research respondents who reported that they were aware of South African legislation relating to social engineering and information security, were asked to specify their extent of familiarity with the ECT Act. Most of the research respondents (42%) indicated that they were not aware at all of the ECT Act, while 33% of the research respondents indicated that they were familiar with the Act.

7.9.1.3 Familiarisation with the Cybercrime and Cybersecurity Bill (Annexure I question 37.3)

Chart 7.19: Familiarisation with the Cybercrime and Cybersecurity Bill (N = 43)



The research respondents who conveyed that they were aware of South African legislation pertaining to social engineering and information security, were asked to specify their extent of familiarity with the Cybercrime and Cybersecurity Bill. Most of the research respondents (49%) revealed that they were least familiar with the Bill. Perhaps this can be attributed to the fact that the Bill has not yet been enacted and is fairly new.

The lack of awareness regarding South African legislation by the research respondents increases their vulnerability towards social engineering attacks. Furthermore, the actual extent of familiarisation with any of the legislation cannot be determined, as the research respondents were not asked to elaborate on their knowledge of legislation.

The final section elaborated on the impact the questionnaire had on the research respondents' own information security awareness.

SECTION H

7.10 IMPACT ON INFORMATION SECURITY AWARENESS (N = 96) (Annexure I question 38)

The research respondents were asked to convey the impact (if any) that the questionnaire had on their own information security awareness. Some research respondents (9%) indicated that the questionnaire had either no impact on their own information security awareness, or left the question unanswered. However, most of the research respondents (91%) shared that the questionnaire had a positive impact on their own information security awareness. Many of the respondents indicated that the questionnaire made them more cognisant of their own information security awareness. This is evident in the following excerpts:

RR2: “It made me realise how easily someone could gain access to my personal information and use it against me.”

RR11: “It makes me want to pay more attention.”

RR12: “It made me aware that I should be more careful with my personal information and that I should be more careful with my passwords.”

RR34: “It made me aware of simple everyday things people can say or do to obtain my information.”

RR44: “It made me realise that I need to adopt a more vigilant attitude with regard to information security awareness.”

RR45: “I learnt new Acts regarding security and social engineering.”

RR64: “It raised awareness on something that is very important but I didn’t know about.”

RR74: “One becomes aware of own negligence towards something that should be taken more seriously.”

RR76: “It made me more aware, usually I’d brush it off but this made me think I should probably care more about my information security.”

RR79: “I have gained knowledge about the importance of security awareness and the risks of social engineering.”

RR80: “Broadened my knowledge and awareness of threats.”

RR100: “I learnt about social engineering, which I have never heard of before.”

The above excerpts revealed that the questionnaire had a positive impact on the research respondents, as it enlightened them on matters pertaining to information security. The legislation presented in the questionnaire (vide Annexure I question 37) was of particular significance, as some of the research respondents mentioned it specifically. The indication that awareness will counteract against negligence and ignorance is a strong theme which emerged from the responses.

Important to note is that some research respondents indicated that the questionnaire reiterated their own sentiments on information security.

RR6: “The questionnaire reinforced the importance of keeping my passwords secret and my personal information protected all the time, at all costs.”

RR33: “Created further awareness.”

RR73: “Reminded me about the threat as it became something I ignored and just left aside.”

RR95: “It re-affirmed my perception that information security awareness is imperative.”

RR97: “Reminds me to be more aware of potential dangers.”

RR111: “Confirmed my awareness and preparedness to the threats that do exist out there in today’s digital age.”

This reconfirmation of knowledge already known, demonstrates that the questionnaire assisted the research respondents in this regard.

The research respondents also indicated that the questionnaire made them more aware of how little they actually knew and encouraged them to educate themselves further on the matter. This is illustrated in the following extracts:

RR4: “I am not that aware of my security, I need to expand my knowledge on that.”

RR7: “I realise I should educate myself better on the subject.”

RR8: “It’s made me realise that I should be more aware and I should probably become more aware of legislation regarding information security.”

RR17: “How little I know and how much I should learn and take precautions.”

RR26: “I think I’d like to know more and take a safer stance towards my interaction on the internet.”

RR28: “It made me realise that I need to research more on information security because currently I am not informed.”

RR36: “I am more alert now of threats. I am also going to familiarise myself more with the Acts.”

RR71: “A concerted effort needs to be made on my part to be informed on these topics.”

RR84: “How ignorant I am or little I know about social engineering.”

RR104: “It made me more aware and made me want to do more research regarding the topic.”

RR106: “It made me realise that I need to sharpen my knowledge in this field.”

RR108: “I will start to Google social engineering after this. I still have a lot to learn and I need to be more alert.”

Based on the above excerpts, the questionnaire helped mobilise the respondents to educate themselves on social engineering and information security. It provoked their

perceptions on the matter and inspired them to do something about their lack of knowledge.

In addition, some of the research respondents explained that answering the questionnaire has now motivated them to perform some kind of action as a preventative measure.

RR12: “It made me aware that I should be more careful with my personal information and that I should be more careful with my passwords.”

RR15: “I must always make sure that I do not give out my personal information without checking whether the person I am giving my details to is legit because they can use it against me.”

RR34: “It made me aware of simple everyday things people can say or do to obtain my information.”

RR40: “It reminds me to be cautious and not to give out information if it is not necessary or required.”

RR89: “It made me more aware of instances where I may be putting personal information at risk without realising it and also that there is other legislation around this of which I am not aware.”

The questionnaire displayed particular value in that it advocated the need for improved personal security measures. The above excerpts denote the practical implications the questionnaire had on some of the respondents. The relevant preventative measures are discussed in Chapter 8.

7.11 CONCLUSION

In this chapter, the self-administered questionnaires retrieved from members of the Tshwane community were presented, interpreted and analysed. This was done by developing themes and categories which were numerically and or descriptively analysed.

The study's aims and objectives set out in Chapter 1 (vide section 1.4) were explored and interpreted in light of the data received.

Descriptive statistics were used to analyse the data, as 114 self-administered questionnaires were received. The analysis and interpretation began with the establishment of the biographic and employment details of the sample group. Furthermore, insight was gained into individuals' perspectives on social engineering through the following themes and patterns which emerged: the general use of communication through technology; identification and authentication; access control; social engineering; legislation related to information security; and the impact on information security awareness. The data retrieved from the research respondents were allied to current literature in order to strengthen the findings. By examining the dynamic impact the self-administered questionnaire had on the research respondents, it is evident that there is a need for awareness campaigns and relevant training.

The self-administered qualitative questionnaire provided evidence that social engineering attacks are taking place. Most of the attacks were technology-based, while the nature of the attacks varied according to the end goal. The respondents listed the main motives behind the attacks to be financial and access to sensitive information. The majority of the respondents indicated that they had never reported a social engineering attack. The various levels of vulnerability were determined, while very few research respondents were aware of any legislation regarding information security. This chapter also presents a necessity for a preventative strategy to be developed against social engineering attacks.

The final chapter seeks to synthesise the study by conferring the achievement of aim and objects, providing practicable recommendations and making relevant conclusions. This chapter will also present the integrative MIT social engineering model, which the former chapters provided the foundation to.

CHAPTER 8

ACHIEVEMENT OF AIM AND OBJECTIVES, RECOMMENDATIONS AND CONCLUSION

8.1 INTRODUCTION

The current study was rooted in its aim and objectives established in Chapter 1 (vide section 1.4). The directive of the study was to explore, describe, explain and analyse social engineering attacks through an integrated MIT approach in order to better understand, measure and explain such attacks. This was done as a means to formulate a proactive strategy against such attacks.

As social engineering was the topic of interest, two comprehensive literature reviews were undertaken (vide Chapter 2 and Chapter 3). As a result, the fundamental perspectives, drawing from the disciplines of criminology, security science and computer science on social engineering were inducted, as well as exploring the psychological and legislative perspectives on the topic at hand. The study found its meaning through criminological theories as both the Classical school of thought and the Positivist school of thought were discussed in terms of their applied relevance to social engineering. These schools of thought were incorporated to demonstrate a victim and perpetrator frame of reference.

The study outlined the research methodology assimilated in the study expansively (vide Chapter 5), as its philosophical framework guided the researcher. The research was navigated by the mixed methods approach, as various research methods were used to investigate the phenomenon. The researcher made use of semi-structured interviews, questionnaires and workshops in order to achieve the study's aim and objectives.

The preceding chapters (vide Chapters 1 to 7) functioned as a milieu to the design of an integrative multi-inter-transdisciplinary (MIT) social engineering model (vide section 8.2).

8.2 MULTI-INTER-TRANSDISCIPLINARY (MIT) SOCIAL ENGINEERING PROTECTION MODEL

The MIT social engineering protection model is contextualised in a scientific locale, illustrated and then further explained.

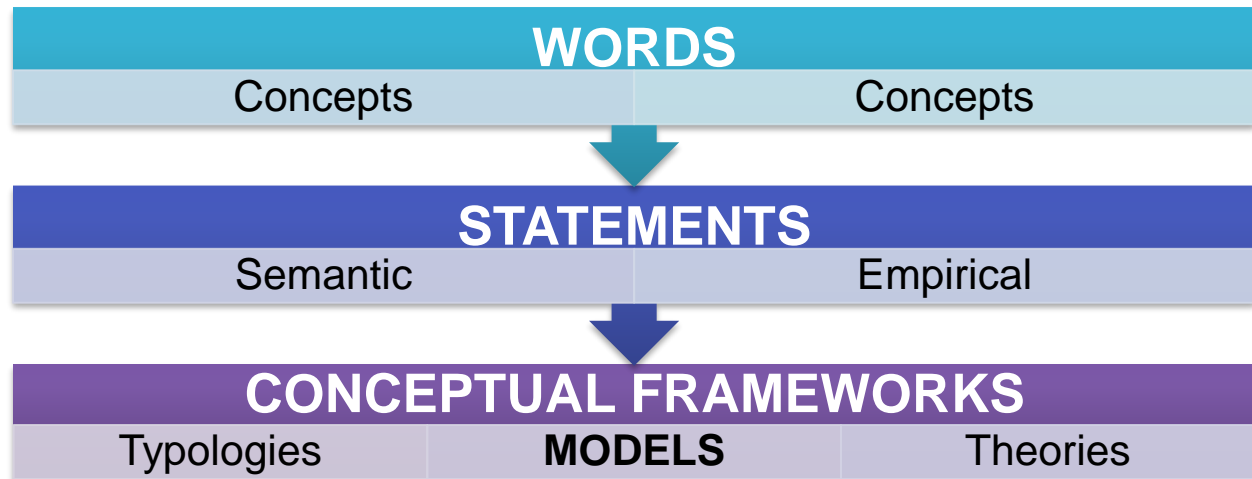
8.2.1 Scientific context of the model

In the research methodology chapter (vide Chapter 5 section 5.2), the framework of social knowledge was alluded to. It was maintained that scientific concepts are not enough to create a body of knowledge. Rather, scientific concepts need to be transformed into statements with semantic meanings and epistemic knowledge. However, this would still not be enough to understand and explain social phenomena. Thus, these statements need to be used to create typologies, models and/or theories (Mouton, 1998: 181). These conceptual frameworks can be differentiated accordingly. Typologies classify or categorise information based on single variables. Models create a methodical illustration of phenomena by exposing patterns and regularities between variables. Theories yield explanations of phenomena by proposing an underlying interconnection (Mouton, 1998: 195).

Although theories and models share many similarities, they differ in degree. A model's greatest distinction is that it is heuristic in nature in that it empowers people to ascertain or learn something for themselves, whereas theories are largely explanatory. Often, in the case of developing new models, current models are examined and built upon in an effort to improve them. By studying a specific phenomenon, the researcher presents certain likenesses or relationships and illustrates them in a simplified model. This model can be described as an "*as-if* framework"; suggesting that the model is structured in the same way as the phenomena under investigation (Mouton, 1998: 197). Nonetheless, models claim to be a mere representation of a phenomenon. Only the most important elements of a model are categorised in order to highlight specific themes. As a consequence, its heuristic nature permits new areas of research to be discovered (Mouton, 1998: 198).

This study is interested in a social engineering protection model and consequently used words and statements to generate a model for its conceptual framework as illustrated below.

Figure 8.1: The framework of social knowledge



(Source: Author's own elaboration as adapted from Mouton, 1998: 180)

8.2.2 The MIT social engineering protection model

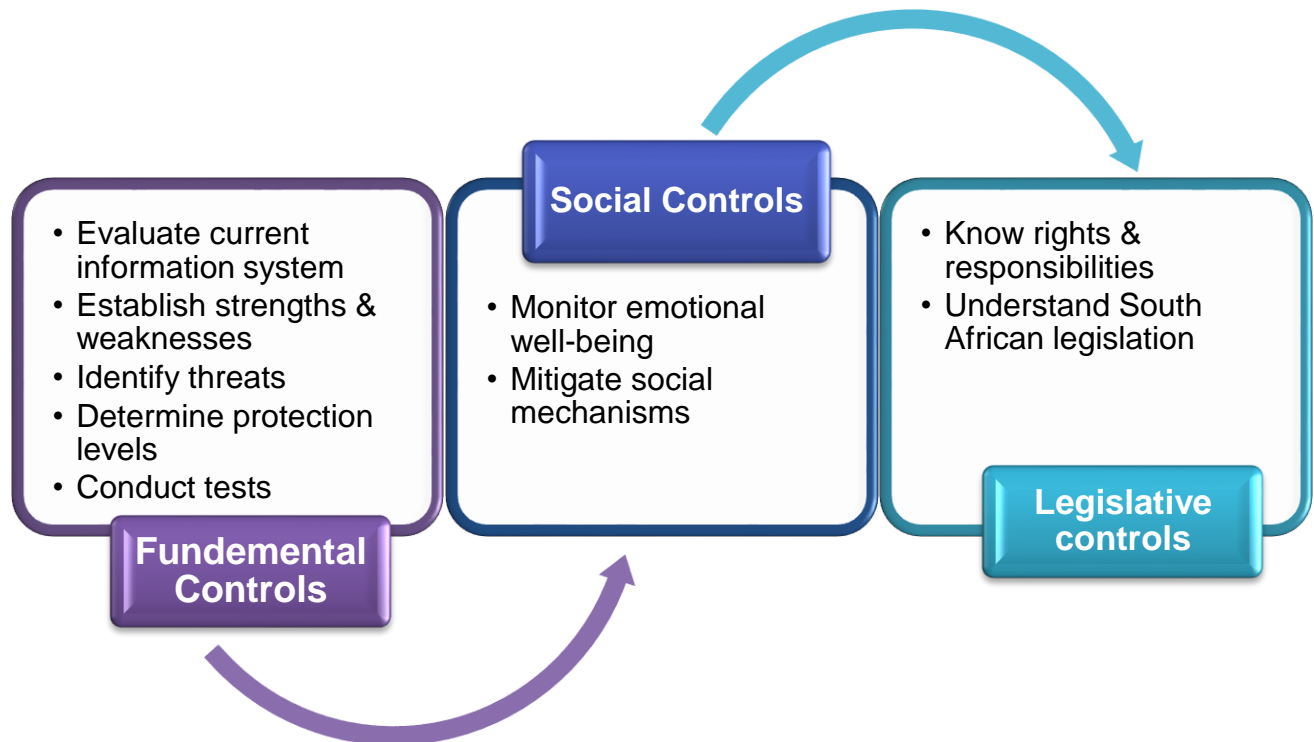
It has been established and sustained throughout the study that social engineering is multi-inter-transdisciplinary in nature, thus the researcher sought to develop a protection model guarding against social engineering attacks. This model is designed to be practically applicable to businesses and individuals when interpreted accordingly. The model is based on the disciplines of criminology, security science, computer science, psychology and law as informed by the previous chapters (vide Chapters 1, 2, 3, 4, 6 and 7) as well as additional literature. In literature, models regarding social engineering are mostly focused on the actual attacks involved and are thus not protective or multi-disciplinary in nature (cf. Mann, 2008; Mitnick & Simon, 2002 Mouton et al, 2014a; Mouton

et al, 2014b; Nohlberg, 2008). Therefore, the researcher sought to bridge this gap in research by creating a protective and integrative MIT model.

Mouton (1998: 80) argues that in empirical research it is becoming increasingly prevalent in quantitative research to select samples from cases, as opposed to endeavouring to retrieve data from the entire population. Inductive generalisation permits the researcher to generalise the findings to the intended population. Furthermore, it can be maintained that representative samples are not needed for generalisation. Similarly, in qualitative research, through analytic induction, generalisation from small samples is permissible, as it can be accepted that a small number of studied cases can be generalised to the larger targeted population (Mouton, 1998: 81; Schwandt, 2007: 1). Moreover, Polit and Beck (2010: 1453) explain that through analytic generalisation enlightening, inductive generalisation can be made on the phenomenon under investigation. This is achieved through meticulous inductive analysis and the maintenance of valid and reliable conclusions. This notion is further sustained by Thorne, Armstrong, Harris, Hislop, Kim-Sung and Oglov (2009: 1385) in that when documented and conveyed authentically and plausibly, the richness and depth of the data can license generalisation with regard to the study at hand.

The researcher used this stance when developing the integrative MIT social engineering model.

Figure 8.2. The multi-inter-transdisciplinary (MIT) social engineering model



8.2.3 Explanation of model

The following analysis provides an explanation of the integrative MIT social engineering model designed and developed by the researcher as it can be applied to businesses and individuals to different degrees.

8.2.3.1 Fundamental controls

The fundamental controls are based on the disciplines of criminology, security science and computer science as outlined in Chapter 2. Social engineering is rooted in these disciplines and thus makes up the most integral part of the model. The fundamental controls are based on the following elements:

8.2.3.1.1 Evaluate current information system

- **Business perspective**

A current information system implemented needs to be evaluated; even if there is not a formal system in place, this needs to be determined and assessed accordingly. A graphic indication of the various information systems within the institution should be illustrated. Thus, the current information security protection system will be identified (Mann, 2008: 160, Whitman & Mattord, 2012: 419).

- **Individual perspective**

Individuals should evaluate their own information security system by asking themselves: “What am I doing to protect my information security?” This question should resound in all aspects of their lives, inclusive of password protection, banking, social media, and online posts (vide Chapter 7 sections 7.5, 7.6, 7.7 and 7.8). Consequently, the individual’s current state of information security should be determined.

8.2.3.1.2 Establish strengths and weaknesses

- **Business perspective**

The current status of protection should be established by determining the human and technical strengths that can be used to detect and deter against social engineering attacks. These human strengths include the capacity of the personnel to detect, deter and withstand a social engineering attack. The systematic strength entails the capacity of an information system to intercept a social engineering attack in the absence of human involvement (Mann, 2008: 160; vide section 6.2.6). Weaknesses should be identified in order to manage and minimise risk.

- **Individual perspective**

Individuals should determine their strengths and weaknesses regarding their information protection. Their strengths can also be divided into their human and technical strengths. For instance, their human strengths could be the ability to determine the legitimacy of a spoofed website and their technical strength could be the pop-up blocker they installed on their technological systems. This can be determined once individuals are aware of the current state of their information security awareness, as shared in Chapter 7 (vide section 7.10).

8.2.3.1.3 Identify threats

- **Business perspective**

The classification of threats will allow the institution to determine the areas which need most attention in terms of the greatest and most perceivable threats. Here, knowledge of social engineering attacks (vide section 2.6.1) is beneficial in order to adequately guard against them.

- **Individual perspective**

Individuals should identify the possible threats (vide section 2.6.1) they could face with regard to social engineering attacks. Through a process of vigorous introspection, these threats should also be assessed in relation to the individual's own weaknesses, as identified earlier.

8.2.3.1.4 Determine protection levels

- **Business perspective**

An in-depth analysis of the current systematic measures implemented in order to protect human and system vulnerabilities should be reviewed. These vulnerabilities should be viewed in light of the potential threats identified (Mann, 2008: 160). These protections levels should be evaluated in terms of their general use of communication through technology, identification and authentication processes, access control and social engineering risks specifically relevant to businesses (vide Chapter 6 section 6.3).

- **Individual perspective**

Individuals should determine their current levels of protection in terms of their general use of communication through technology, identification and authentication processes, access control and social engineering risks (vide Chapter 7 sections 7.5, 7.6, 7.7 and 7.8).

8.2.3.1.5 Conduct tests

- **Business perspective**

Specialised and orchestrated testing of current systems should be done regularly to accurately assess current levels of security. This will be discussed in more detail under section 8.4.1. A clear action plan can be designed which will comprise an array of improvement strategies. These strategies should be executed in view of providing a return on the security investments identified (Mann, 2008: 160; vide section 6.2.6).

- **Individual perspective**

Individuals can test their level of protection by observing their own fundamental controls and determining the effectiveness thereof (vide section 7.10).

8.2.3.2 Social controls

The social controls are based on the psychological principles of social engineering established in Chapter 3 (vide section 3.2). The social controls are similarly applicable to businesses and individuals and will consequently be discussed together.

8.2.3.2.1 Monitor emotional well-being

As the human element plays a key role in a successful social engineering attack, it is important to monitor employees' well-being. The manipulation of psychological factors such as desperation, fear, naivety and anxiety plays a crucial role in a successful social engineering attack. It is suggested that these human vulnerabilities are considered when encountering any suspicious activity (Mouton, Leenen & Venter 2016: 202; vide section 6.2.8).

8.2.3.2.2 Mitigate social mechanisms

The social mechanisms crucial to a social engineering attack were outlined in Chapter 3 (vide section 3.2). The model (figure 8.2) suggests that businesses and individuals identify these social mechanisms and develop countermeasures to guard against them. Psychological variables such as trust, persuasion and compliance should be examined and contextualised in light of the businesses' and individuals' circumstances.

8.2.3.3 Legislative controls

The legislative controls are based on policies and legislation outlined in Chapter 3 (vide section 3.3).

8.2.3.3.1 Know rights and responsibilities

- **Business perspective**

Businesses should be well aware of their rights and responsibilities regarding the protection of their security. These rights and responsibilities should be documented in an information security policy which will guide and govern the way employees protect the businesses' information. The findings portrayed in the business perspective provide insight into the significance of employees knowing and understanding their rights and responsibilities regarding the institution's information protection (vide section 6. 3).

- **Individual perspective**

In order to protect themselves, individuals should know their rights and responsibilities with regard to their own information security. The findings presented in Chapter 7 expressed that the more individuals know about matters pertaining to social engineering, the more they can protect themselves.

8.2.3.3.2 Understand South African legislation

- **Business perspective**

Knowing, understanding and adhering to South African legislation regarding information security are vital for the longevity of any business. The information security policy developed by the specific institution should take the South African legislation into account as discussed in Chapter 3 (vide section 3.3). Businesses cannot expect their employees to be experts in legislative matters, however, an intentional effort should be made so that all employees understand and comply with legislation.

- **Individual perspective**

It is the responsibility of each individual to be aware of legislation affecting to their own information security. It was found that most of the research respondents (74%) were not aware or were uncertain of any legislation pertaining to information security (vide section 7.9.1) and thus a conscious effort to know and understand legislation is advocated for.

8.3 ACHIEVEMENT OF AIMS AND OBJECTIVES OF THE STUDY

The study's aim and objectives functioned as a map navigating the research expedition, as cited throughout the study. The realisation of the aim and objectives, as established in section 1.4 (vide Chapter 1) will now be reviewed.

8.3.1 Achievement of aim

The following denotes the aim of the study which guided the research.

- **The exploration, description, explanation and analysis of social engineering attacks through an integrated MIT approach in order to better understand, measure and explain such attacks as a means to formulate a protection strategy.**

The aim of the study is twofold. First, to explore, describe, explain and analyse social engineering attacks through an integrated MIT approach. Thereafter, a proactive strategy of protection was designed to understand, measure and explain such attacks. The aim of any research study is attained through its objectives (Fouché & Delport, 2011: 108), thus the achievement of the study's aim will be unpacked within the scope of its objectives.

8.3.2 Achievement of objectives

The following discussion represents the achievement of the objectives as outlined by the study.

8.3.2.1 The occurrence and nature of social engineering attacks

In order to describe the phenomenon, the occurrence and nature of social engineering attacks needed to be established. Thus, the study set out to answer the following two questions: Is there an occurrence of social engineering attacks in South Africa? and What is the nature of social engineering? The study commenced with a literature review to determine the occurrence and nature of social engineering. As social engineering falls in the scope of various disciplines, there is quite a substantial amount of literature regarding it. Thus, the researcher compiled two literature reviews (vide Chapter 2 and 3) to adequately capture the intricate nature of the phenomenon. The literature review operated as a precept to the empirical research. The researcher used three different modes of conducting empirical research. The mixed methods approach was employed in that both qualitative and quantitative methodology was used to better explore, describe, explain and analyse social engineering. Important to reiterate is that the study's aim was not to make blanket generalisations. Conversely, it aimed to investigate the phenomenon of social engineering as experienced by the chosen sample groups. Chapter 6 (Part I) and Chapter 7 best investigated this objective and are discussed below.

All of the SMEs established that social engineering is occurring in South Africa – not only in business enterprises but also in the lives of individuals. They brought forth that despite the presence of good technologies, there is an absence of good information security awareness and practices. The main type of social engineering attacks were noted as phishing attacks. The SMEs specified that no person is exempt from a social engineering attack, as all people can be targeted and are thus vulnerable. A social engineer constitutes any group or individual who wants to obtain personal information from their target in order to use it deceitfully and maliciously. Social engineering attacks can occur in an online and offline environment. The end goal dictates the means. It was established that social engineering attacks can have extensive impacts on businesses and individuals. The main consequences were noted to be financial losses and reputational harm. The SMEs concurred that the human element is the leading vulnerability factor in information security and needs to be intentionally and effectively guarded against.

The self-administered qualitative questionnaire established that social engineering attacks are taking place. It was found that 70 per cent of the research respondents had

been exposed to a social engineering attack. Most of the attacks were technology-based as compared to human-based attacks. The technology-based social engineering attacks were dominated by phishing attacks and methods of hoaxing, while the human-based attacks were reported mostly be done through impersonation and desktop support. The details and nature of the attacks varied according to the end goal. The respondents listed the main motives behind the attacks to be financial gain and access to sensitive information. The majority of the respondents indicated that they had never reported a social engineering attack. However, those who did report it, reported it to the SAPS or the institution the attack claimed to have come from.

Grounded on the above discussion, the objective to ascertain the occurrence and nature of social engineering attacks was achieved.

8.3.2.2 The awareness of social engineering attacks and information security

The second objective of the study was to determine the current awareness of social engineering attacks and information security among the research respondents. This objective was best ascertained through the qualitative questionnaires administered to the businesses and individuals.

Within the business perspective, the awareness of and vulnerability to social engineering attacks were established. The awareness of social engineering varied according to the institution, as portrayed in Chapter 6 (vide section 6.9). It was found that not all of the research respondents from institution A knew what social engineering was, despite coming from an IT department. In institution B it was found that although some of the research respondents indicated that they were aware of social engineering, their responses did not provide the appropriate correlation. Thus, advocating the need for awareness campaigns and training programmes required for local businesses.

With regard to the individual perspective, the awareness of social engineering attacks was uncovered. The majority (73%) of the research respondents specified that they did not know what the term social engineering meant, whereas 27 per cent shared that they were familiar with the terminology. Despite this result, it was found that the research

respondents were familiar with the techniques associated with social engineering, as 70 per cent of the research respondents had been exposed to some manifestation of a social engineering attack, thus indicating that although the research respondents were not familiar with the terminology, they were aware of the examples posed. In addition, they descriptively shared their exposure to social engineering attacks as documented in Chapter 7 (vide section 7.8).

8.3.2.3 The state of vulnerability to social engineering attacks

The study sought to determine the vulnerability of the research respondents to social engineering attacks. This was done by examining the research respondents' general use of communication, identification and authentication systems and measures used to control access. The following significant themes were determined in terms of vulnerability from the business and individual perspective.

- **Business perspective:**

- Most of the research respondents indicated that they were fairly new to their current employment. It was established that the less time one is employed at an institution, the more vulnerable one is to a social engineering attack.
- All of the research respondents indicated that they used the internet for work and e-mail purposes, thus using it on a daily basis. The internet is a common medium used in social engineering attacks, thus increasing vulnerability.
- The accessibility of personal information varied according to the research respondent and institution. However, interesting discussions regarding the use of cookies, social network sites and personal online searches were raised. These factors increase vulnerability.
- In all of the institutions, most of the research respondents perceived that their telephone number and e-mail addresses were accessible to the general public, thus, increasing vulnerability.
- The research respondents provided comprehensive evidence that their institutions

adhered to access control procedures, thus decreasing vulnerability to social engineering attacks.

- In all of the institutions, password management was made compulsory, consequently reducing their vulnerability to social engineering attacks.
- Most of the research respondents used e-signatures. It was determined that in business, the use of e-signatures is necessary but steps should be taken to mitigate associated risks.
- The safe use of access control varied according to the different institutions.
- There were disparities regarding when access control is revoked. This increases vulnerability to social engineering attacks conducted by disgruntled employees.
- The social engineering hypothetical scenarios presented in Chapter 6 (vide section 6.9.3) disclosed multiple potential vulnerabilities within the institutions.

▪ **Individual perspective:**

- The majority (98%) of the research respondents indicated that they used the internet on a daily basis. Thus, as the internet is a popular medium used in social engineering attacks, it can be proposed that the more one participates in internet-based activities, the more vulnerability is increased.
- The reasons for internet use varied exposing different levels of vulnerability. It was noted that reasons for internet usage create a pervasive risk which is dependent on the users' behaviours and precautions taken.
- Most of the research respondents (35%) considered their personal information to be accessible to the general public, while 14 per cent were uncertain thereof. This finding increases the research respondents' vulnerability, as the former indicates that they are comfortable with the accessibility of their personal information. The latter indicates that their unawareness of good information security practices increases their vulnerability to social engineering attacks.
- Half of the research respondents (50%) indicated that they made use of an e-signature. Most of these respondents worked in professional or administrative capacities. It was determined that vulnerability is increased through the ease of obtaining an e-signature and the current legislation accepting the legality of it.

- Although it was found that most of the research respondents (see section 7.7.1) protected their technological devices through password control, the degree of safety was compromised. This was compromised through the similarity of passwords, the (in)frequency in changing passwords and password control.

8.3.2.4 The contextual role of social engineering attacks within the various disciplines through MIT research

As established in the beginning of this study (vide section 1.2) the nature of the phenomenon under investigation was found to be multi-inter-transdisciplinary. It was established that social engineering cannot be boxed into a single discipline but in fact crosses the boundaries of many disciplines. For the purpose of this study it was found that social engineering can be embedded in the disciplines of criminology, security science, computer science, psychology and law. The contextual role of social engineering attacks was investigated through an integrated MIT approach. This was done by examining the fundamental perspectives (vide Chapter 2) as well as the psychological and legislative perspectives (vide Chapter 3) on social engineering

The fundamental perspectives on social engineering are rooted in the fields of criminology, security science and computer science. Through these disciplines, social engineering could be conceptualised. It was found that a healthy information security culture needs to be actively maintained and the consequences thereof were discussed if this is not done. In these disciplines, the occurrence and nature of social engineering attacks were narrated at length. In addition, both international and local research provided evidence of the nature and extent of social engineering attacks. It is within these disciplines where the risks, perpetrator characteristics, attack framework and impact associated with social engineering attacks were identified and construed. Moreover, as represented in Chapter 4; social engineering was applied to traditional criminological theories. Hence, the Classical and Positivist schools of thought were incorporated to find plausible explanations for social engineering attacks.

Through the review of literature, it was established that the disciplines of psychology and law are paramount in understanding social engineering attacks. More specifically, it was

evident that techniques found in social psychology are used in social engineering attacks. Elements such as trust, persuasion and compliance were critically reviewed as linked to social engineering attacks. Furthermore, South African legislation pertaining to social engineering attacks was analysed in terms of its effectiveness and practicality. The legislation that was reviewed included the following:

- The Electronic Communications and Transactions (ECT) Act 25 of 2002.
- The Protection of Personal Information Act 4 of 2013.
- The Cybercrime and Cybersecurity Bill.

Through the qualitative questionnaires, it was found that the majority of the research respondents were not aware of legislation addressing social engineering attacks. Within the business perspective, it was uncovered that most of the research respondents were unfamiliar with legislation. Through the individual perspective, it was found that only 26 per cent of the research respondents claimed to know about legislation governing social engineering.

8.3.2.5 The MIT social engineering protection model

The study substantially contributed to scientific scholarship through the interpretation and expansion of knowledge in a specialised area of research. This was highlighted through the model illustrated and explained in section 8.2.2. The model is multi-interdisciplinary (MIT) in nature, as it integrated the disciplines of criminology, security science, computer science, psychology and law. It can be applied to businesses and individuals, as described in the explanation of the model (vide section 8.2.3). The model attempts to fill a gap in scientific research as a protection model of its standard and capability could not be found in literature. It is based on literature and empirical research and used words and statements to develop the conceptual framework. Thus, the study successfully achieved the objective of designing an integrative MIT social engineering protection model as a means of a protective strategy.

8.4 LIMITATIONS OF THE STUDY

Limitations of the study include any components of the research inquiry which have an effect on the application and interpretation of the findings (Labaree, 2013: np). Similarly to any human initiative, Bachman and Schutt (2014: 14) argue that any research study will have limitations. Furthermore, findings are subjective as they are dependent on diverse interpretations. Admittedly, a single research study in the social sciences will not resolve all arguments. Social scientists tend to differ based on their research opportunities, methodological approaches and policy inclinations. However, the research inquiry should allow the researcher to see more, discern with fewer misrepresentations and provide rich descriptions of what her opinions are founded on. In this way, understanding issues in the social sciences, and more specifically criminology, is not reliant on the outcome of any research study but rather the accretion of evidence from various studies about a similar topic. Thus, any limitations found in a study should be taken into consideration when designing a similar study in the future. This will aid in intensifying the knowledge base and should settle any disagreements thereof (Bachman & Schutt, 2014: 14).

Heeding the above discussion, the researcher identified the following limitations in the current study:

8.4.1 Contemporary framework of the study

Chapter 2 (vide section 2.3.2 and 2.3.3) provided an overview of local and international research conducted on social engineering. As highlighted throughout the study and later on substantiated by the empirical research undertaken, the terminology associated with social engineering is not well known. It was also found that although the topic is rooted in criminology, it transcends various other disciplines. Hence, the MIT approach was adopted to investigate the topic. In addition, the inherent complex and clandestine nature of social engineering and its related techniques, makes it difficult to statistically document

it. It is not specifically addressed in legislation or policies but the tactics used in a social engineering attack are specified in South African legislation, as elaborated on in Chapter 3 (vide section 3.3).

8.4.2 Sample size

As advocated by Mouton (1998: 174) a general guideline in the philosophy of science is that no empirical research findings can be proven irrefutably. The study used a mixed methods research approach. From its conception, the study did not aspire to make generalisations (vide Chapter 1 section 1.3.3). On the contrary, the study sought to achieve data triangulation by making use of various research methods to achieve the aim and objectives.

The foundation of the study rested on its literature review and insight and experiences gained from the identified SMEs. The researcher found that a substantial volume of the literature on social engineering was generated by international sources, thus locating these experts proved to be difficult. In addition, the researcher found extensive bodies of knowledge regarding social engineering in literature and thus deemed the number of SMEs interviewed as sufficient.

The use of qualitative questionnaires was explicitly chosen to investigate the businesses' and individuals' perspectives on social engineering. The researcher struggled to find research respondents, especially from a business perspective. The potential reasons for the low response rate can be allocated to the ambiguity concomitant with social engineering, in that not many people are aware of what it entails, its significance and how it can impact them. Although confidentiality and anonymity were guaranteed, businesses may not have wanted to risk their information being published. Additionally, in the business world time is money; consequently businesses may not have wanted to take part in the study in fear of "misusing" valuable time and resources. The researcher tried to alleviate these factors by introducing training as part of her research study to better equip local businesses. It can be noted that the data retrieved from the businesses and individuals were very descriptive and lengthy in nature – so much so that the researcher

could not include all the sections retrieved from the questionnaires in the analysis chapters.

8.4.3 Self-appraisal data

The information retrieved from the qualitative questionnaires can be considered to be self-appraisal data. As previously mentioned in Chapter 5 (section 5.4.1.2), self-appraisal data are useful in that it will allow for participant reflection and introspection. However, self-appraisal data can generate certain biases which may lead to a misrepresentation of data. In order to mitigate such factors, the researcher did not ask for any names, contact details or affiliations from the research respondents. This was done in order to encourage the research respondents to be as truthful as possible.

In view of the aim, objectives and limitations of the study assessed above, the researcher was able to make recommendations for both protection and response methods, as well as suggestions for future research concerning the study.

8.5 RECOMMENDATIONS FOR PREVENTION OF AND RESPONSE TO SOCIAL ENGINEERING ATTACKS

Crime against persons and property remains a constant concern for members of society. The illegal techniques associated with social engineering have generated a need for innovative security measures in an effort to deter, detect and deny criminal access (Collins, Ricks & Van Meter, 2015: 26). Moreover, as advocated by Du Plessis and Holtmann (2005:152), the reduction of victimisation is the product of amplified crime prevention and response strategies. The following section will provide a discussion on recommendations for businesses and individuals in terms of protective responses to social engineering attacks.

8.5.1 Recommendations for businesses

Social engineering attacks can have colossal effects on businesses (vide Chapter 2 section 2.8), and thus comprehensive recommendations based on literature and the findings of the current study are discussed below.

8.5.1.1 Measuring vulnerability

Similarly to any area which is undergoing early stages of development, there is no scientifically accepted unequivocal systematic framework of analysis for social engineering (Mann, 2008: 155; Mitnick & Simon, 2002: 259). It is advantageous to determine the human strengths and systematic strengths within an institution (vide section 8.2.3.1.1). As mentioned in Chapter 6 (vide 6.2.2), often social engineering attacks are successful due to a lack of recognised and implemented policies and procedures.

8.5.1.2 Data classification

It has been established that social engineers seek to obtain critical and sensitive information. Thus, it would be vital to establish protection of key data through a classification system. Data classification entails categorising data according to its levels of confidentiality (Whitman & Mattord, 2012: 585). There are various data classification systems available, and a customised specific one should be compiled according to the needs of an institution. The classification of what constitutes key information should not be left to the individual discernment of personnel (Mann, 2008: 181; Whitman & Mattord, 2012: 124). As established by Mitnick and Simon (2002: 264), the following information classification system is recommended for small to medium sized institutions:

- *Confidential:* Confidential information is limited to very few people within an institution and should only be given on a need-to-know basis. Any information

which is vital to the operation of a business, as well as future strategies, can be seen as confidential.

- *Private:* Private information refers to personal information (medical history, back account information or remuneration packages) which should only be known within an institution. This information can be of particular value to social engineers.
- *Internal:* Internal information can be shared among all members of staff. This information should not be given to any third parties outside of the institution.
- *Public:* Public information can be freely distributed. Any information that is not classified as public should be regarded as sensitive and protected accordingly.

8.5.1.3 Awareness and targeted training

A persistent theme documented throughout the study and established in the analysis chapters (vide Chapters 6 and 7) of this dissertation, is allied to the need for awareness campaigns and training with regard to social engineering. The implementation of such campaigns and programmes will assist in raising awareness of the threat of social engineering and should escalate the probability of an attack being deterred, detected and denied. In addition, personnel can be trained to comply with the ISMS.

8.5.1.3.1 Awareness building campaigns

The following awareness building campaigns should be considered within any institution:

- **Induction programmes**

Induction programmes provide an opportune time for an institution to orient new staff members with their specialised ISMS. It can be assumed that new employees are

inundated with information during these induction sessions, thus the initial training on the institution's ISMS should be dynamic and pertinent. The inclusion of ISMS training in the induction programme should have a dual role. It should convey the message that information security is taken seriously within the institution. Moreover, it should provide an orientation of social engineering and the specific threats the institution can face. However, in order to sustain a culture of information security practices, a perpetual and persistent environment of follow-up activities, as discussed below, should be mandated (Conteh & Royer, 2016: 6; Mann, 2008: 195).

- **Group training**

Group training sets aside an allocated time slot to engage in interactive, content-relevant, interesting and critically meaningful training on social engineering (Mann 2008: 197). Although institutional training can be expensive, time-consuming and overall resource intensive, it can be highly effective when implemented appropriately (Mann 2008: 197). In chapter 6 (vide section 6.2.6) it was raised that although many companies do run information security awareness sessions, very few staff members actually attend. These sessions should be made compulsory and linked to performance agreements.

- **E-mail and intranet notifications**

E-mail and intranet notifications can provide a cost-effective way for updating staff on information security, specifically regarding social engineering. Bulletins of this nature can be delivered in informative and innovative ways and will reach large numbers of people (Mann, 2008: 197). However, shortcomings of this approach may be the low review rate of people who actually read and internalise the information. In addition, this approach may increase social engineering vulnerabilities as it standardises e-mail communication and instructions. These limitations can be addressed by using technological systems to track down who actually opens the e-mails and intranet links, as well as by filtering internal communication in an effort to identify any spoofed e-mails (Mann 2008: 198).

- **Login screen messages and posters**

Login screen messages are a useful tool to deliver communication concerning information security. Although it does not guarantee that personnel will actually read these messages, this approach is attention-driven, economical and can be modified and updated frequently. Furthermore, the continuous repetition of information security principles is likely to create a subconscious absorption of the information relayed. Posters displayed in an institution can also reiterate the importance of information security, as well as convey a message that information security is taken seriously (Mann, 2008: 199).

- **E-learning**

With the rise of the internet, many institutions are opting for online interactive learning resources as a means to raise awareness and the capacity to reach large numbers of personnel. These programmes can guide content for large groups, monitor usage and provide assessments to evaluate understanding (Mann, 2008: 198). E-learning and evaluation can be executed securely, proficiently, and can produce amplified user motivation (Woit & Mason, 2003: 137). Some concerns can be raised regarding this approach. The content is usually assessed directly after the content is taught, thus it cannot be determined if lasting retention has been achieved. The autonomous nature of the e-learning system can allow the users to cheat, such as finding the answers to the assessment through an internet search or by asking someone else to complete the assessment for them (Mann, 2008: 198).

- **Institutional campaigners**

In large institutions, a local information security champion can be enlisted to generate support and interest among personnel. This could be done through the organisation of workshops and seminars dedicated to best practices regarding information security and social engineering. In this way, information security training can be aligned to the business strategy of the institution.

8.5.1.3.2 Targeted training

- **Categorised training**

Despite its importance, it cannot be expected that all institutions should just focus on information security. Thus, to maximise the effectiveness of training, employees can be classified into three risk clusters according to their job description – high, medium and low. High-risk employees have direct access to integral information and will require systematic, targeted and preventative specific training. Medium-risk employees have the potential to access pivotal information and thus require induction and regular follow-up training. Low-risk employees have little to no access to critical information and would merely require role specific directions (Mann, 2008: 202). This categorised training should also be linked to the data classification system decided by the organisation, as discussed in section 8.5.1.2.

- **Training for IT specialists**

Often IT personnel are not regarded as being at risk to social engineering attacks, because it is assumed that they already are implementing good information security practices. However, this is not always the case and they may be at risk to proficient social engineering attacks (Mann, 2008: 201). Moreover, it cannot be assumed that all IT personnel are experts in information security, especially in a specialised category of social engineering. Even if this personnel group is highly technical in understanding information security, it does not necessarily mean that they understand human vulnerabilities. In addition, most institutions give their IT personnel full administration rights, thereby generating increased risk. IT personnel should be involved in the institution's social engineering protection plan and not be exempt from related training (Mann, 2008: 203). Within the data analysis of the current study (vide chapter 6 section 6.3), it was found that even IT professionals did not uphold information security efficiently; a finding which supports the recommendation that IT specialists also need training in social engineering prevention.

- **Guidelines for training programmes:**

The following guidelines, founded on literature and the findings of the current study, were compiled to assist institutions in designing their social engineering training programmes.

1. *Develop conscious awareness of social engineering threats:* This can be achieved through the range of training programmes discussed in section 8.5.1.3.1. However, caution should be exercised in preventing these initiatives from becoming too technical. These programmes should be designed with the intention of helping the targeted audience to understand social engineering in a way that is easy to grasp and apply (Mann, 2008: 204).
2. *Cultivate an information security culture:* A healthy security culture enables personnel to activate discernment on when to comply with information security principles, and when to question these principles (vide section 2.2). It is important to create a working environment where people are comfortable to challenge security-related concerns when necessary. Senior staff members should not only adhere to information security practices, but should also attend training sessions to publically reinforce their support to other personnel. In Chapter 6 (vide section 6.2.8) it was found that although an institution can have good technical control, human vulnerabilities can still be present where a healthy information security culture is not maintained.
3. *Be aware of triggers:* Personnel should be trained in being mindful of certain triggers and techniques associated with social engineering (Mann, 2008: 205). These techniques are discussed in Chapter 2 and 3 of the current study.

8.5.1.4 Penetration testing

Penetration testing was previously mentioned in Chapter 6 (vide section 6.2.2). A common trend entails institutions hiring an external security company to conduct social engineering penetration testing. Based on the current study, penetration testing should be customised to suite a specific institution and should include the following elements:

- **Attack formulation**

The types of attack which would make the institution vulnerable should be framed. This could range from specific attacks or a combination of attacks.

- **Information gathering through public platforms**

An institution may be astounded by how much information there is about their institution on public platforms. Information can be found on the websites of suppliers and partners, internet postings that employees make, or even from technical staff asking questions on online forums (Mann, 2008: 213). These questions could include explanations of current problems with security, consequently increasing vulnerability to social engineering attacks (Barrett, 2003: 57).

- **Information gathering through people**

Personnel can unknowingly reveal a lot of sensitive information about their institution. A database of retrieved information should be created (Barnett, 2003: 59; Mann, 2008: 213).

- **Target selection**

During penetration testing, specific personnel are targeted (as relevant to their job description and role) and tested for their possible vulnerability to social engineering or exploitation. (Barrett, 2003: 59; Mann, 2008: 214).

- **Target testing**

During penetration testing, the specified targets must be assessed by using aspects of both technological and physical social engineering attacks.

- **Debriefing**

All the personnel involved in penetration testing should be debriefed after the exploitation has taken place. It should be emphasised that none of the targets will be penalised in any way based on the findings of the penetration test. In contrast, the targets will be made aware of their own human vulnerabilities with regard to the protection of information, and they will be given strategies to prevent and overcome social engineering.

- **Reporting**

A risk analysis report should be generated on completion of the penetration test. Within this report, the following variables should be outlined: risks identified; testing scope and limitations; methodology employed; the results of the penetration test; as well as recommendations for improvement (Mann, 2008: 215). Within the reporting

phase, a guideline document should be compiled to guide the organisation on what to do if the institution ever falls prey to a social engineering attack. This document should be free from technical jargon and outline the consequences of information security breaches (Mitnick & Simon, 2002: 261). In addition, the institution should be well aware of their rights and responsibilities based on South African legislation, as outlined in Chapter 3 (vide section 3.3).

8.5.2 Recommendations for individuals

The recommendations for individuals are based on preventative measures and are determined by current literature and the findings of the present study. The following recommendations were devised to assist individuals in protection against social engineering attacks:

- **Education and awareness**

Education and awareness are instrumental in the prevention of successful social engineering attacks (Olavsrud, 2010). If people are not aware of the potential dangers to their personal information, they will not be able to adequately defend themselves against these attacks. Moreover, social engineering relies on naivety and ignorance, thus the need for education and awareness rises (Pinola, 2012). As previously indicated in Chapter 7 (vide section 7.8), 73 per cent of the research respondents did not know what social engineering is, while 56 per cent were not aware at all of the threats associated with social engineering. Organisations associated with common social engineering attacks, such as banks and tax revenue service providers, are actively campaigning against social engineering through online portals (vide Chapter 4 section 4.2.1). However, as emphasised in Chapter 6 (vide section 6.2.7), each individual has the responsibility to educate themselves of the security threats they may face. Overall, a positive response was extracted from the research participants in terms of how the self-administered questionnaire informed their own information security awareness (vide Chapter 7 section 7.10).

- **Control online presence**

As eluded through the lifestyle exposure theory discussed in Chapter 4 (vide section 4.3.1), individuals are more prone to sharing personal information over the internet. Caution should be exercised when creating an online persona. Often individuals are surprised as to how much information is available, as experienced by some of the research respondents. Thus, regular checks through popular search engines should be made.

- **Update software**

Although anti-virus software is particularly expensive for the average individual, it is necessary. Without the proper technical controls, the likelihood of a successful social engineering attack is increased. As maintained by Olavsrud (2010) regular patch checks and software updates can alleviate a lot of risk. In Chapter 6 (vide section 6.2.7) it was established that there is not much support for individual victims of social engineering attacks, as compared to when an attack happens on a greater scale such as in a big institution.

- **Limit unfamiliar applications and online links**

Individuals should take caution to avoid unknown applications and should not click on unknown links. The URLs should always be considered when checking for legitimacy. Moreover, when clicking on links in e-mails and websites, users should look out for automatic downloads containing malware or ransomware (Perlman, 2014).

- **Password protection**

In the current study, most of the individuals' (84%) devices were password protected. However, only 23 per cent of the research respondents specified that all their passwords differed, whereas 46 per cent indicated that they only changed their passwords when prompted. Passwords should be complex and strong and should be modified frequently. Individuals should try not to use the same password for different applications. In order to make it more difficult to gain access to any system, two-phase authentication should be used. Individuals should add additional security questions to their security systems. These questions should be difficult to answer, unless answered by the legitimate user. In addition, users should avoid having a single point of

reference for their password storage. The more entwined an individual's accounts are, the more vulnerability is increased (Cobb, 2012; Pinola, 2012). A password management system can also be used, which usually contains a password generator (Ciampa, 2014: 53).

- **Credit and debit card usage**

When using credit and debit cards, online or offline, caution should always be maintained. Individuals should be cautious that their information is not susceptible to attacks such as dumpster diving or shoulder surfing. In addition, credit card and debit card information should not be saved on websites. Individuals should also be on the lookout for identity theft or any other suspicious activity (Pinola, 2012).

- **Data backups**

Data backups entail duplicating files from a computer's hard drive onto other digital media systems (Ciampa, 2014: 94). In order to safely keep any valuable information, data should be copied and archived on an external source. To maximise efficiency, individuals should back-up their data on an external hard drive as well as online platforms. Ciampa (2014: 96) suggests using automatic backup, universal access (data backed up through online service providers) and delayed deletion systems (files will remain accessible for a limited time after deletion).

- **Intuition**

In support of a robust information security culture, it would be advisable to embrace a healthy sense of scepticism and vigilance (Perlman, 2014; Pinola, 2012). Throughout literature it is also highlighted as important for an individual to determine their current emotional status before attempting to comply with any suspicious request.

- **Response**

The intervention for social engineering will depend on the type of attack suffered. However, it is important to try and minimise any damage done, be it financial, reputational or time lost in recovery of data (vide section 2.8). The majority of the research respondents (93%) indicated that they had never reported their exposure to a social engineering attack (vide section 7.8.8). It is important to report any incident

relating to social engineering in order to inform the relevant stakeholders. This will help to better understand and measure these attacks as well as make the public aware thereof.

8.6 RECOMMENDATIONS FOR FURTHER RESEARCH

There is a need for further scientific research to be conducted regarding social engineering and its related facets. Based on the current research study, the following research areas were identified as possible avenues to consider when conducting future research:

- A quantitative analysis of social engineering, specifically investigating its impact on business and trade. This study will be able to determine the statistical occurrence and nature of social engineering. The current study's research methodology regarding the business perspective can be replicated on a larger scale to deduce trends and generalisations.
- A quantitative examination of social engineering as it affects individuals. This study will be able to determine the statistical occurrence and exposure of social engineering among individuals. The study should be conducted across provinces and employ cluster sampling, as the population is too big.
- A qualitative inquiry into the victims of social engineering attacks on a micro and macro level should be undertaken. The study will shed light on the devastating impact a social engineering attack can have on an individual or business.
- A qualitative exposé into phishing attacks. The study should provide an in-depth analysis on the nature and extent of phishing attacks, inclusive of the victimisation associated with it.

8.7 CONCLUSION

This chapter illustrated the study's successful achievement of the aim and objectives as set out in the commencement of the study. Chapter 8 also made applicable recommendations to businesses and individuals regarding social engineering. Of particular significance in the chapter is the attention given to the MIT social engineering prevention model. The model sought to bridge a scientific gap found in literature in a valuable and practical way. A detailed account was given of how the aim and objectives were achieved by referring to the theoretical and empirical aspects of the study. The chapter acknowledged the limitations pertinent to the study, as it was found that all social science studies will have shortcomings. Furthermore, recommendations were made for businesses and individuals in terms of prevention and response strategies. The chapter concludes with recommendations for further research relevant to the topic at hand.

The study demonstrated its capacity to competently and innovatively apply knowledge, criminological theory and relevant research methodology to the complex and specialised phenomenon of social engineering. The study maintains that a conscious endeavour should be undertaken to create and maintain a healthy information security culture in order to prevent successful social engineering attacks. The study advocates the need for additional academic inquiries into social engineering to further expand the knowledge base on it.

LIST OF REFERENCES

- Adam, M.E., Yousif, O., al-Amodi, Y. and Ibrahim, J. 2011. Awareness of social engineering among IIUM students. *World of Computer Science and Information Technology Journal*, 1(9): 409-413.
- Alfreds, D. 2015. *Your credit card could fund cybercrime*. Available at: <http://m.news24.com/fin24/tech/news/your-credit-card-could-fund-cybercrime-20150819> (retrieved: 3 February 2016).
- Alfreds, D. 2016. *Internet use dominates SA smartphones: Research*. Available at: <http://www.fin24.com/Tech/Mobile/internet-use-dominates-sa-smartphones-research-20160405> (retrieved: 24 May 2016).
- Alston, M. and Bowles, W. 2003. *Research for caring professionals: An introduction to methods*. London: Routledge Taylor & Francis Group.
- Anderson, 2015. PoPI: *The race to data safety*. Available at: http://www.itweb.co.za/index.php?option=com_content&view=article&id=143711 (retrieved: 23 January 2016).
- Andress, J. 2014. *The basics of information security: Understanding the fundamentals of InfoSec in theory and practice* (2nd edition). Massachusetts: Elsevier.
- Anon. 2010. *419 Scam: The dead foreigner scam*. Available at: <http://419scam.org/419-barrister-lome-togo.htm> (retrieved: 23 January 2016).
- Anon. 2015. *Ransomware*. Available at: <http://carteblanche.dstv.com/player/916354> (retrieved: 29 December 2015).
- Anon. 2016. *Avoid sharing personal info on social media*. 16 February. Available at: <http://www.iol.co.za/capetimes/avoid-sharing-personal-info-on-social-media-1985363> (retrieved: 18 February 2016).
- Arce, I. and Levy, E. 2003. *The weakest link revisited*. Available at: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1193216> (retrieved: 18 February 2016).
- Babbie, E. 2007. *The practice of social research* (11th edition). Belmont: Thomson Wadsworth.
- Babbie, E. 2010. *The practice of social research* (12th edition). Wadsworth: Cengage Learning.
- Babbie, E. and Mouton, J. 2001. *The practice of social research*. Cape Town: Oxford University Press.
- Bachman, R. and Schutt, R.K. 2014. *The practice of research in criminology and criminal justice* (5th edition). Los Angeles: Sage.
- Balle, L. 2016. *How do businesses use the internet?* Available at: <http://smallbusiness.chron.com/businesses-use-internet-752.html> (retrieved: 14 June 2016).

- Bampton, R. and Cowton, C.J. 2002. The e-interview. *Forum: Qualitative Social Sciences*, 3(2), May. Available at: <http://www.qualitative-research.net/fqs/> (retrieved: 20 January 2016).
- Barnett, N. 2003. Penetration testing and social engineering: Hacking the weakest link. *Information Security Technical Report*, (8): 56-64.
- Barkhuizen, M. 2004. *Professional women as victims of emotional abuse within marriage or cohabitating relationships: A victimology study*. Unpublished MA dissertation, University of Pretoria, Pretoria.
- Barlow, D.H. and Durand, V.M. 2009. *Abnormal psychology: An integrative approach* (5th edition). Belmont: Wadsworth Thomson Learning.
- Bechan, U. 2008. *Towards a framework for securing a business against electronic identity theft*. Unpublished MA dissertation, University of South Africa, Pretoria.
- Bergman, M.M. 2008. *Advances in mixed methods research*. London: Sage.
- Bernard, H.R. 2013. *Social research methods: Qualitative and quantitative approaches* (2nd edition). California: Sage.
- Berscheid, E. 1992. A glance back at a quarter century of social psychology. *Journal of Personality and Social Psychology*, 63: 525-533.
- Bezuidenhout, C. 2011. Elementary research methods in criminology. In C. Bezuidenhout. *A Southern African perspective on fundamental criminology*. Cape Town: Pearson Education South Africa.
- Bezuidenhout, M., Mouton, F. and Venter, H.S. 2010. Social engineering attack detection model: SEADM. Available at: <http://ieeexplore.ieee.org/document/5588500/references> (retrieved: 20 September 2015).
- Björck, F. 2005. *Discovering information security management*. Unpublished PhD thesis, University of Stockholm and Royal Institute of Technology, Stockholm.
- Bless, C., Higson-Smith, C. and Kagee, A. 2006. *Fundamentals of social research methods: An African perspective* (4th edition). Cape Town: Juta.
- Bopape, H.M. 2008. *Social impact of information technology: Implication for a tertiary institute*. Unpublished MA dissertation, University of South Africa, Pretoria.
- Botha, C. 2011. *A gap analysis to compare best practice recommendations and legal requirements when raising information security awareness amongst home users of online banking*. Unpublished MA dissertation, University of South Africa, Pretoria.
- Boyd, D.M. and Ellison, N.B. 2008. Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, 13(1): 210-230.
- Brostoff, S., Sasse, A. and Weirich, D. 2002. Transforming the weakest link: A human-computer interaction approach to usable and effective security. *BT Technology Journal*, 19(3): 122-131.

- Brown, S.E., Esbensen, F.A. and Geis, G. 2013. *Criminology: Explaining crime and its context* (8th edition). Massachusetts: Anderson Publishing.
- Bryant, R.B. 2008. The challenge of digital crime. In R.B. Bryant. *Investigating digital crime*. London: Wiley & Sons.
- Bryman, A. 2012. *Social research methods* (4th edition). Oxford: Oxford University Press.
- Bulgurcu, B., Cavusoglu, H. and Benbasat, I. 2010. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, (34): 523-548.
- Burrows, T. 2014. *SA enterprise unprepared for breaches*. Available at: http://www.itweb.co.za/index.php?option=com_content&view=article&id=71977 (retrieved: 17 July 2015).
- Buunk, A.P. and Van Vugt, M. 2008. *Applying social psychology: From problems to solutions*. London: Sage.
- Canter, D.V. 2013, *Criminal psychology: Topics in applied psychology*. London: Routledge.
- Cartwright, D. 1979. Contemporary social psychology in social perspective. *Social Psychology Quarterly*, 42: 82-93.
- Casmir, R. 2005. *A dynamic and adaptive information security awareness (DAISA) approach*. Published thesis, Stockholm University, Sweden.
- Check Point Software Technologies Ltd. 2011. Check Point survey reveals nearly half of enterprises are victims of social engineering. Available at: <http://www.marketwired.com/press-release/check-point-survey-reveals-nearly-half-enterprises-are-victims-social-engineering-nasdaq-chkp-1563778.htm> (retrieved: 20 September 2015).
- Cialdini, R.B. 2001. *Influence: Science and practice* (4th edition). Massachussets: Allyn & Bacon.
- Ciampa, M. 2014. *Security awareness: Applying practical security in your world* (4th edition). Boston: Course Technology Cengage Learning.
- Clark, R. 2010. *Intelligence analysis: A target centric approach* (3rd edition). Washington: CQ Press.
- Cobb, M. 2012. *Password security best practices: Change passwords to passphrases*. 12 June. Available at: <http://www.computerweekly.com/tip/Password-security-best-practices-Change-passwords-to-passphrases> (retrieved: 30 August 2016).
- Cohen, L.E. and Felson, M. 1979. Social change and crime rate trends: A routine activity approach. *American Sociological Review*, August, 44: 588-608.
- Collins, P.A., Ricks, T.A. and Van Meter, C.W. 2015. *Principles of security and crime prevention* (4th edition). London: Routledge.
- Computer Security Institute. 2011. 2010/2011 Computer crime and security survey. Available at: <https://cours.etsmtl.ca/gti619/documents/divers/CSIsurvey2010.pdf> (retrieved 17 February 2014).

- Contech, N. and Royer, M.D. 2016. The rise in cybercrime and the dynamics of exploiting the human vulnerability factor. *International Journal of Computer* (20): 1-12.
- Corey, R. 2015. *What is the CIA triad? Confidentiality, integrity and availability*. 9 June. Available at: <https://www.cybrary.it/2015/06/what-is-the-cia-triad-confidentiality-integrity-and-availability/> (retrieved: 12 October 2015).
- Correa, D. 2016. *2015 saw nearly 407k attempted ransomware infections*. 4 August. Available at: <http://www.scmagazine.com/2015-saw-nearly-407k-attempted-ransomware-infections/article/514086/> (retrieved: 6 August 2016).
- Creswell, J.W. 2013. *Qualitative inquiry and research design: Choosing among five approaches* (3rd edition). Los Angeles: Sage.
- Creswell, J.W. and Plano Clark, V.L. 2007. *Designing and conducting mixed methods research*. Thousand Oaks, CA: Sage.
- CyberArk Labs. 2016. *Analysing ransomware and potential mitigation strategies*. Available at: <http://www.cyberark.com/resource/cyberark-labs-ransomware/> (retrieved: 6 August 2016).
- Dagada, R. 2014. *Legal and policy aspects to consider when providing information security in the corporate environment*. Unpublished PhD thesis, University of South Africa, Pretoria.
- Davies, P. and Francis, P. 2011. Preparing criminological research. In P. Davies (Ed.), P. Francis and V. Jupp. *Doing criminological research* (2nd edition). London: Sage.
- Davis, L. 2005. Theoretical approaches and perspectives in victimology. In L. Davis and R. Snyman. *Victimology in South Africa*. Pretoria: Van Schaik.
- Davis, B.J. 2007. Situational prevention and penetration testing: A proactive approach to social engineering in organisations. In A.W. Merkidze. *Terrorism issues: Threat assessment, consequences and prevention*. New York: Nova Science Publishers.
- De Vos, A.S. and Strydom, H. 2005. Scientific theory and professional research. In A.S. de Vos (Ed.), H. Strydom, C.B. Fouché and C.S.L. Delport. *Research at grass roots: For the social sciences and human service professions* (3rd edition). Pretoria: Van Schaik.
- De Vos, A.S., Strydom, H., Schulze, S. and Patel, L. 2011. The sciences and the professions. In A.S. de Vos, H. Strydom, C.B. Fouché and C.S.L. Delport (Eds). *Research at grass roots: For the social sciences and human service professions*. Pretoria: Van Schaik.
- Delport, C.S.L. and De Vos, A.S. 2011. Professional research and professional practice. In A.S. de Vos (Ed.), H. Strydom, C.B. Fouché and C.S.L. Delport. *Research at grass roots: For the social sciences and human service professions* (4th edition). Pretoria: Van Schaik.
- Delport, C.S.L. and Roestenburg, W.J.H. 2011. Quantitative data-collection methods: Questionnaires, checklists, structured observation and structured interview schedules. In A.S. de Vos (Ed.), H. Strydom, C.B. Fouché and C.S.L. Delport.

- Research at grass roots: For the social sciences and human service professions* (4th edition). Pretoria: Van Schaik.
- Denzin, N.K. and Lincoln, Y.S. 2003. *Collecting and interpreting qualitative materials*. Thousand Oaks, CA: Sage.
- Department of Justice and Constitutional Development, South Africa. 2015. *Justice publishes draft Cybercrimes and Cybersecurity Bill for public comments*. Available at: <http://www.gov.za/speeches/justice-publishes-cybercrimes-and-cybersecurity-bill-public-comments-28-aug-2015-0000> (retrieved: 3 February 2016).
- Deyzel, L. 2014. *Client experience of e-counselling*. Unpublished MA dissertation, University of South Africa, Pretoria.
- Dhillon, G. and Backhouse, J. 2001. Current directions in information security research: Toward socio-organizational perspectives. *Information Systems Journal*, (11): 127-153.
- Du Plessis, M. and Holtmann, B. 2005. Victimisation reduction and prevention. In L. Davis and R. Snyman. *Victimology in South Africa*. Pretoria: Van Schaik.
- Durrheim, K. 2006. Research design. In M. Terre Blanche (Ed.), K. Durrheim and D. Painter. *Research in practice: Applied methods for the social science*. Cape Town: University of Cape Town Press.
- Duff, S. 2014. *The latest statistics on South African internet penetration*. Available at: <https://www.webafrica.co.za/blog/general/latest-statistics-south-african-internet-penetration/> (retrieved: 24 May 2016).
- Eck, J.E. and Clarke, R.V. 2003. Classifying common police problems: A routine activity approach. *Crime Prevention Studies*, 16: 7-39.
- Egan, M. 2015. *What is the Dark Web? How to access the Dark Web. What's the difference between the Dark Web and the Deep Web?* 23 November 2015. Available at: <http://www.pcadvisor.co.uk/how-to/internet/what-is-dark-web-how-access-dark-web-deep-joc-3593569/> (retrieved: 20 February 2016).
- Evans, N.J. 2009. *Information technology social engineering: An academic definition and study of social engineering - analysing the human firewall*. Unpublished PhD thesis, Iowa State University, Iowa.
- Febelfin. 2016. Fraud techniques. Available at: <https://www.safeinternetbanking.be/en/fraud-techniques> (retrieved: 17 August 2016).
- Felson, M. and Cohen, L.E. 1980. Human ecology and crime: A routine activity approach. *Human Ecology*, 4: 389-406.
- Fitzgerald, J.D. and Cox, S.M. 2002. *Research methods and statistics in criminal justice*. London: Wadsworth.
- Forouzan, B. 2014. *Foundations of computer science* (3rd edition). Hampshire: Cengage Learning.

- Fouché, C.B. and Bartley, A. 2011. Quantitative data analysis and interpretation. In A.S. de Vos, H. Strydom, C.B. Fouché and C.S.L. Delport (Eds). *Research at grass roots: For the social sciences and human service professions*. Pretoria: Van Schaik.
- Fouché, C.B. and Delport, C.S.L. 2011. Writing the research proposal. In A.S. de Vos, H. Strydom, C.B. Fouché and C.S.L. Delport (Eds). *Research at grass roots: For the social sciences and human service professions*. Pretoria: Van Schaik.
- Fouché, C.B. and De Vos, A.S. 2011. Formal formulations. In A.S. de Vos (Ed.), H. Strydom, C.B. Fouché and C.S.L. Delport. *Research at grass roots: For the social sciences and human service professions* (3rd edition). Pretoria: Van Schaik.
- Fouché, C.B. and Schurink, W. 2011. Qualitative research designs. In A.S. de Vos (Ed.), H. Strydom, C.B. Fouché and C.S.L. Delport. 2011. *Research at grass roots: For the social sciences and human service professions* (4th edition). Pretoria: Van Schaik.
- Frangopoulos, E.D. 2007. *Social engineering and the ISO/IEC 1799:2005 Security Standard: A study on effectiveness*. Unpublished MA dissertation, University of South Africa, Pretoria.
- Furnell, S. and Clarke, N. 2012. Power to the people? The evolving recognition of human aspects of security. *Computers & Security*, 31: 983-988.
- Garcia, M.L. 2008. *The design and evaluation of physical protection systems* (2nd edition). Boston: Butterworth/Heinemann.
- Gardner, B. and Thomas, V. 2014. *Building an information security awareness program: Defending against social engineering and technical threats*. Waltham: Elsevier.
- Germaner, S. 2011. *Thousands in SA hit by PlayStation breach*. Available at: <http://www.iol.co.za/scitech/technology/security/thousands-in-sa-hit-by-playstation-breach-1.1062066> (retrieved: 3 February 2016).
- Gibson, D. 2011. *Understanding the security triad: Confidentiality*. 27 May. Available at: <http://www.pearsonitcertification.com/articles/article.aspx?p=1708668> (retrieved: 17 July 2015).
- Global Economic Crime Survey. 2016. *Adjusting the lens on economic crime: Preparation brings opportunity back into focus*. Available at: <https://www.pwc.com/gx/en/economiccrimesurvey/pdf/GlobalEconomicCrimeSurvey2016.pdf> (retrieved: 3 September 2016).
- Goethals, G.R. 2003. A century of social psychology: Individuals, ideas, and investigations. In M. Hogg and J. Cooper. *The Sage handbook of social psychology*. London: Sage.
- Gold, S. 2010. Social engineering today: Psychology, strategies and tricks. *Network Security Journal*, (11): 11-14.
- Goman, C.K. 2011. *The art and science of mirroring*. Available at: <http://www.forbes.com/sites/carolkinseygoman/2011/05/31/the-art-and-science-of-mirroring/#2715e4857a0b24357ac356be> (retrieved: 14 January 2016).

- Gonzalez, J. 2002. *A framework for human factors in information security*. Available at: https://www.researchgate.net/profile/Jose_Gonzalez74/publication/228684288_A_framework_for_human_factors_in_information_security/links/02e7e53720ad4cfbb3000000.pdf (retrieved: 19 October 2015).
- Goodchild, J. 2010. *Protect your company against social engineering*. 11 January. Available at: <http://www.computerworld.com/article/2522443/security0/protect-your-company-from-social-engineering.html> (retrieved: 13 October 2015).
- Goodin, D. 2013. *You're infected: If you want to see your data again, pay us \$300 in Bitcoins*. Available at: <http://arstechnica.com/security/2013/10/youre-infected-if-you-want-to-see-your-data-again-pay-us-300-in-bitcoins/> (retrieved: 12 October 2015).
- Gragg, D. 2003. *A multi-level defense against social engineering*. SANS Institute: As part of Information Security Reading Room. Available at: http://www.sans.org/reading_room/whitepapers/engineering/ (retrieved: 12 October 2015).
- Granger, S. 2001. *Social engineering fundamentals, Part I: Hacker tactics*. 18 December. Available at: <http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics> (retrieved: 9 January 2016).
- Gravetter, F.J. and Forzano, L.B. 2003. *Research methods for the behavioural sciences*. Belmont: Wadsworth/Thomson Learning.
- Greeff, M. 2011. Information collection: Interviewing. In A.S. de Vos (Ed.), H. Strydom, C.B. Fouché and C.S.L. Delport. *Research at grass roots: For the social sciences and human service professions* (4th edition). Pretoria: Van Schaik
- Grinnel, R.M. and Unrau, Y.A. 2008. *Social work research and evaluation: Foundations of evidence-based practice*. New York: Oxford University Press.
- Gross, R. and Acquisti, A. 2005. *Information revelation and privacy in online social networks*. New York: ACM.
- Guenther, M. 2001. *Social engineering: LLC*. Available at: <http://www.iwar.org.uk/comsec/resources/security-awareness/social-engineering-generic.pdf> (retrieved: 27 June 2014).
- Hadnagy, C. 2011. *Social engineering: The art of human hacking*. Indianapolis: Wiley Publishing.
- Handel, S. 2013. *The unconscious influence of mirroring*. Available at: <http://www.theemotionmachine.com/the-unconscious-influence-of-mirroring> (retrieved: 14 January 2016).
- Hanson, W.E., Creswell, J.W., Plano Clark, V.L., Petska, K.S. and Creswell, J.D. 2005. Mixed methods research designs in counselling psychology. *Journal of Counselling Psychology*, 52(2): 224-235.
- Harley, D. 1998. *Re-floating the Titanic: Dealing with social engineering attacks*. Available at: <http://smallbluegreenblog.files.wordpress.com/2010/04/eicar98.pdf> (retrieved: 27 June 2014).

- Hennik, M., Hutter, I. and Bailey, A. 2011. *Qualitative research methods*. London: Sage.
- Henning, E., Van Rensburg, W. and Smit, B. 2004. *Finding your way in qualitative research*. Pretoria: Van Schaik.
- Henry, S. and Einstadter, W. 1998. Introduction: Criminology and criminological theory. In S. Henry and W. Einstadter. *The criminology theory reader*. New York: New York University Press.
- Hill, S. 2010. *Social networking websites encourage stalking*. Available at: <http://cyberpaths.blogspot.com/2009/02/social-networking-web-sites-encourage.html> (retrieved: 7 March 2012).
- Hindelang, M.J., Gottfredson, M.R. and Garofalo, J. 1978. *Victims of personal crime: An empirical foundation for a theory of personal victimisation* 1978. Cambridge: Ballinger.
- Holtfreter, K., Reisig, M.D. and Pratt, T.C. 2008. Low self-control, routine activities, and fraud victimization. *Criminology*, 46: 189-220.
- Hullavarad, S., O'Hare, R. and Roy, A. 2015. Digital signatures deciphered. Available at: <https://www.alaska.edu/files/finance/Audit-DigitalSignaturesApril2015.pdf> (retrieved: 23 September 2016).
- Hunt, N. and McHale, S. 2008. A practical guide to e-mail interview. *Qualitative Health Research*, 17(10): 1415-1421.
- ISO/IEC. 2005. *International Standard ISO/IEC 17799:2005. Information technology security techniques: Code of practice for information security management*. Geneva: ISO Copyright Office.
- Issac, R.M. 2011. *Application of cybernetics in cyber criminology*. Available at: https://www.researchgate.net/profile/Reji_Issac/publication/235443417_Application_of_Cybernetics_in_Cyber_Criminology/links/0fcfd511b40532c21b000000.pdf (retrieved: 7 April 2016).
- Jewkes, Y. and Sharp, K. 2003. Crime, deviance and the disembodied self: Transcending the dangers of corporeality. In Y. Jewkes. *Dot. Cons: Crime, deviance and identity on the internet*. Devon: Willan Publishing.
- Johnson, R.B. and Onwuegbuzie, A.J. 2007. Mixed methods research: A research paradigm whose time has come. *Educational Researcher*, 33(7): 14-26.
- Karakasiliotis, A., Furnell, S.M. and Papadaki, M. 2006. *Assessing end-user awareness of social engineering and phishing*. Available at: <http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1011&context=isw> (retrieved: 6 February 2016).
- Kassin, S., Fein, S. and Markus, H.R. 2014. *Social psychology: International edition* (9th edition). Wadsworth: Cengage Learning.
- Kearney, W.D. and Kruger, H.A. 2014. Considering the influence of human trust in practical social engineering exercises. Available at:

- <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6950509> (retrieved: 2 October 2015).
- Keyworth, M. and Wall, M. 2016. The bogus boss email scam costing firms millions. 8 January. Available at: <http://www.bbc.com/news/business-35250678> (retrieved: 23 September 2016).
- Kirwan, G. and Power, A. 2013. *Cybercrime: The psychology of online offenders*. New York: Cambridge University Press.
- Kleupfel, H. 1989. *Foiling the wiley hacker: More than analysis and commitment*. Security Technology, International Carnahan Conference (1989): 15-21.
- Kosslyn, S.M. and Miller, G.W. 2014. *Left brain, right brain: Two sides, always working together*. Available at: <https://www.psychologytoday.com/blog/the-theory-cognitive-modes/201405/left-brain-right-brain-two-sides-always-working-together> (retrieved: 14 January 2016).
- Krombholz, K., Hobel, H., Huber, M. and Weippl, E. 2015. Advanced social engineering attacks. *Journal of information security and applications*, (22): 113-122.
- Kumar, R. 2005. *Research methodology: A step-by-step guide for beginners* (2nd edition). London: Sage.
- Labaree, R.V. 2013. *Organizing your social sciences research paper: Limitations of the study*. University of Southern California: UCS Libraries.
- Langer, E., Blank, A. and Chanowitz, B. 1978. The mindlessness of ostensibly thoughtful action: The role of "placebic" information in interpersonal interaction. *Journal of Personality and Social Psychology*, 36: 635-642.
- Lee, J.K., Moon, S.Y. and Park, J.H. 2016. CloudRPS: A cloud analysis based enhanced ransomware prevention system. *The Journal of Supercomputing*, (10): 1825 - 1830.
- Leedy, P.D. and Ormrod, J.E. 2005. *Practical research: Planning and design* (8th edition). Upper Saddle River, New Jersey: Merrill Prentice Hall.
- Lewis-Beck, M., Bryman, A. and Liao, T. 2004. *Encyclopaedia of social science research methods*. Thousand Oaks, CA: Sage.
- Liebenberg, J.C.R. 2008. *Truth and reconciliation process and civil-military relations: A qualitative exploration*. Unpublished PhD thesis, University of South Africa, Pretoria.
- Lord, N. 2016. *Social engineering attacks: Common techniques and how to prevent an attack*. 27 June. Available at: <https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack> (retrieved: 6 August 2016).
- Lotz, B. 2016. A hacker told us South Africans should be talking about online privacy more, and we agree. 26 February. Available at: <http://www.htxt.co.za/2016/02/26/91182/> (retrieved: 2 August 2016).
- Lucks, B.D. 2004. *Cyberstalking: Identifying and examining electronic crime in cyberspace*. Unpublished DPhil thesis. Alliant International University, California.

- Makosky, V.P. 1985. Teaching psychology in the information age. *Teaching of Psychology*, (12): 23-26.
- Mann, I. 2008. *Hacking the human: Social engineering techniques and security countermeasures*. Unpublished DPhil thesis, Gower Publishing Company, England.
- Manske, K. 2006. *An introduction to social engineering, information systems security*. 21 December. Available at: <http://www.tandfonline.com/doi/pdf/10.1201/1086/43312.9.5.20001112/31378.10> (retrieved: 10 October 2015).
- Mashiloane, N.P. 2014. *The use of intelligence led policing in crime prevention by the South African Police Service*. Unpublished PhD thesis, University of South Africa, Pretoria.
- Maslow, A. 1987. *Motivation and personality* (3rd edition). New York: Harper Collins.
- Maurushat, A.M. 2011. *Botnet badinage: Regulatory approaches to combating botnets*. Unpublished PhD thesis, University of South Wales, Mid Glamorgan.
- McCann, D. 2014. *Criminals posing as CFOs to commit wire fraud*. Available at: <http://ww2.cfo.com/fraud/2014/08/criminals-posing-cfos-commit-wire-fraud/> (retrieved: 14 January 2016).
- McLeod, S. 2014. *Maslow's hierarchy of needs*. Available at: <http://www.simplypsychology.org/maslow.html> (retrieved: 11 January 2016).
- Microsoft. 2016. BitLocker drive encryption overview. Available at: [https://technet.microsoft.com/en-us/library/cc732774\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc732774(v=ws.11).aspx) (retrieved: 2 August 2016).
- Milgram, S. 1963. Behavioral study of obedience. *The Journal of Abnormal and Social Psychology*, 67: 371-378.
- Milgram, S. and Sabini, J. 1978. On maintaining urban norms: A field experiment in the subway. In A. Baum, J.E. Singer and S. Valins. *Advances in Environmental Psychology: The urban environment* (1): 31-40. Hillsdale: Erlbaum.
- Minnaar, A. 2013. *Cybercrime, hackers, cyberattacks and problems of implementing organizational cybersecurity*. Paper presented to the 23rd Annual Meeting of the International Police Executive Symposium (IPES): *Global issues in contemporary policing*. International Law Enforcement Academy (ILEA), Budapest, Hungary. 4-9 August.
- Minnaar, A. 2014. "Crackers", cyberattacks and cybersecurity vulnerabilities: The difficulties in combatting the "new" cybercriminals. *Acta Criminologica: South African Journal of Criminology*, Special Edition No. 2: 127-144.
- Mitnick, K.D. and Simon, W.L. 2002. *The art of deception*. Indianapolis: Wiley Publishing.
- Mitnick, K.D. and Simon, W.L. 2011. *Ghost in the wires: My adventures as the world's most wanted hacker*. New York: Little, Brown & Company.

- Mokati, N. 2015. *Video shows dangers of sharing too much*. 5 September. Available at: <https://www.iol.co.za/news/south-africa/gauteng/video-shows-dangers-of-sharing-too-much-1911262> (retrieved: 20 February 2016).
- Mouton, J. 1998. *Understanding social research*. Pretoria, Hatfield: Van Schaik.
- Mouton, F., Leenen, L., Malan, M.M. and Venter, H. 2014a. *Towards an ontological model defining the social engineering domain*. Available at: https://www.researchgate.net/publication/263588276_Towards_an_Ontological_Model_Defining_the_Social_Engineering_Domain (retrieved: 14 January 2015).
- Mouton, F., Leenen, L. and Venter, H.S. 2016. Social engineering attack examples, templates and scenarios. *Computer & Security*, (59): 186-209.
- Mouton, F., Malan, M.M., Leenen, L. and Venter, H.S. 2014b. *Social engineering attack framework*. Available at: https://www.researchgate.net/publication/263588935_Social_Engineering_Attack_Framework (retrieved: 14 January 2015).
- Mouton, F., Malan, M.M., Kimppa, K.K. and Venter, H.S. 2015. Necessity for ethics in social engineering research. *Computers & Security*, (55): 114-127.
- Mouton, F., Malan, M.M. and Venter, H.S. 2013. Social engineering from a normative ethics perspective. Available at: <http://ieeexplore.ieee.org/document/6641064/> (retrieved: 20 September 2015).
- Mphidi, A.J. 2015. *An analysis of the rules and procedures of reporting fraud and corruption in the department of trade and industry*. Unpublished MTech dissertation, University of South Africa, Pretoria.
- Munyua, H.M. and Stilwell, C. 2012. The applicability of the major social science paradigms to the study of the agricultural knowledge and information systems of small-scale farmers. Available at: https://www.researchgate.net/profile/Christine_Stilwell/publication/268801252_The_applicability_of_the_major_social_science_paradigms_to_the_study_of_the_agricultural_knowledge_and_information_systems_of_small-scale_farmers/links/54d0abf40cf298d65667cc27.pdf (retrieved 15 March 2016).
- Myers, M.D. 2009. *Qualitative research in business and management*. London: Sage.
- National Institute of Standards and Technology. 2000. *PBX vulnerability analysis: Finding holes in your PBX before someone else does*. Available at: <http://csrc.nist.gov/publications/nistpubs/800-24/sp800-24pbx.pdf> (retrieved: 24 September 2015).
- Neuman, W.L. 2006. *Social research methods: Qualitative and quantitative approaches* (6th edition). Boston: Pearson Education.
- Newburn, T. 2007. *Criminology*. Devon: Willan Publishing.
- Nohlberg, M. 2008. *Securing information assets: Understanding, measuring and protecting against social engineering attacks*. Unpublished DPhil Thesis, Stockholm University, Sweden.

- Olavsrud, T. 2010. *Nine best defences against social engineering attacks*. 19 October. Available at: <http://www.esecurityplanet.com/views/article.php/3908881/9-Best-Defenses-Against-Social-Engineering-Attacks.htm> (retrieved: 30 August 2016).
- Opland, R. and Moodley, T. 2013. *What happens if we violate PoPI?* Available at: [http://www.ey.com/Publication/vwLUAssets/What_happens_if_we_violate_PoPI/\\$FILE/130522%20Privacy%20Thought%20Leadership%202.pdf](http://www.ey.com/Publication/vwLUAssets/What_happens_if_we_violate_PoPI/$FILE/130522%20Privacy%20Thought%20Leadership%202.pdf) (retrieved: 3 February 2016).
- Orgill, G.L., Romney, G.W., Bailey, M.G. and Orgill, P.M. 2004. *The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems*. Available at: <http://delivery.acm.org/> (retrieved: 14 January 2015).
- Ormston, R., Spencer, L., Barnard, M. and Snape, D. 2014. The foundations of qualitative research. In J. Ritchie, J. Lewis, C.M. Nicholls and R. Ormston. *Qualitative research practice: A guide for social science students and researchers* (2nd edition). London: Sage.
- Padayachee, K. 2013. A conceptual opportunity-based framework to mitigate the insider threat. Available at: <http://ieeexplore.ieee.org/document/6641060/> (retrieved 15 June 2014).
- Patel, A. 2013. *How spammers get your number*. 9 June. Available at: <http://www.news24.com/Archives/City-Press/How-spammers-get-your-number-20150429> (retrieved: 23 June 2016).
- Peltier, T.R. 2001. *Information security policies, procedures and standards*. Florida: Taylor & Francis Group.
- Perlman, M. 2014. *Eight tips to prevent social engineering attacks*. 21 December. Available at: <http://lightcyber.com/8-tips-to-prevent-social-engineering-attacks/> (retrieved: 30 August 2016).
- Persuad, N. 2010. Pilot study. In N.J. Salkind. *Encyclopaedia of research design*. Thousand Oaks, CA: SAGE. Available at: <http://knowledge.sagepub.com/view/researchdesign/n312.xml?rskey=z119MX&row=1> (retrieved: 4 March 2014).
- Petty, R.E. and Cacioppo, J.T. 1986. *Communication and persuasion: Central and peripheral routes to attitude change*. New York: Springer-Verlag.
- Pillay, L. 2016. *Get a head start on POPI with these 5 tips*. Available at: <http://www.itnewsafrika.com/2016/01/get-a-head-start-on-popi-with-these-5-tips/> (retrieved: 27 January 2016).
- Pinola, M. 2012. *How can I protect against social engineering hacks?* 8 September. Available at: <http://lifehacker.com/5933296/how-can-i-protect-against-hackers-who-use-sneaky-social-engineering-techniques-to-get-into-my-accounts> (retrieved: 30 August 2016).
- Polit, S.F. and Beck, C.T. 2010. Generalization in quantitative and qualitative research: Myths and strategies. *International Journal of Nursing Studies* (47): 1451-1458.

- Ponemon Institute. 2013. *2013 cost of data breach study: Global analysis*. Available at: <http://www.ponemon.org/local/upload/file/2013%20Report%20GLOBAL%20CO%20FINAL%205-2.pdf> (retrieved: 17 July 2015).
- Ponemon Institute. 2016. *2016 cost of data breach study: Global analysis*. Available at: <http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN> (retrieved: 3 September 2016).
- PoPI Compliance. 2016. Get informed. Available at: <https://www.popi-compliance.co.za/oecd-publishes-data-protection-guidelines/> (retrieved 20 May 2016).
- Pratt, T.C., Holtfreter, K. and Reisig, M.D. 2010. Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency*, 47(2): 67-96.
- PricewaterhouseCoopers (South Africa). 2015. Reported security breaches have increased by 66 per cent annually since 2009 (18th Annual Global CEO Survey, 2015).
- Prinsloo, J.H. 2008. Actuarial based offender assessment: An evaluation of the reliability of the Self-Appraisal Questionnaire (SAQ). *Acta Criminologica: South African Journal of Criminology*, (21): 1-10.
- Quann, J. and Belford, P. 1987. *The hack attack: Increasing computer system awareness of vulnerability threats*. Applying Technology to Systems: Aerospace Computer Security Conference, United States, American Institute of Aeronautics and Astronautics (1987): 155-157.
- Ratele, K. 2006. Postcolonial African methods and interpretation. In M. Terre Blanche (Ed.), K. Durkheim and D. Painter. *Research in practice: Applied methods for the social science*. Cape Town: University of Cape Town Press.
- Reczek, R.W., Summers, C.A. and Smith, R.W. 2016. *Online ads know who you are, but can they change you too?* 2 March. Available at: <https://theconversation.com/online-ads-know-who-you-are-but-can-they-change-you-too-54983> (retrieved: 22 March 2016).
- Republic of South Africa, Department of Justice. Constitution of the Republic of South Africa, Act 108 of 1996. Published in the Government Gazette. Pretoria: Government Printer.
- Republic of South Africa, Department of Justice. Promotion of Access to Information (PAIA) Act 2 of 2000. Published in the Government Gazette. Pretoria: Government Printer.
- Republic of South Africa. Department of Justice. Electronic Communications and Transactions Act 25 of 2002. Published in the *Government Gazette* (23708). Pretoria: Government Printer.
- Republic of South Africa. Department of Justice. National Credit Act 34 of 2005. Published in the Government Gazette. Pretoria: Government Printer.

- Republic of South Africa. Department of Justice. Consumer Protection Act 68 of 2008. Published in the *Government Gazette*. Pretoria: Government Printer
- Republic of South Africa. Department of Justice. Protection of Personal Information Act 4 of 2013. Published in the *Government Gazette* (37067). Cape Town: Government Printer.
- Republic of South Africa. Department of Justice. Cybercrime and Cybersecurity Bill. 2015. Published in the *Government Gazette*. Cape Town: Government Printer.
- Republic of South Africa. Department of Justice. Protection of Information Bill (B28-2008: 6]. Published in the *Government Gazette* (32999). Cape Town: Government Printer.
- Resnik, D.B. 2011. *What is ethics in research and why is it important?* 1 May. Available at: <http://www.veronaschools.org/cms/lib02/NJ01001379> (retrieved: 21 January 2016).
- Reyns, B.W. 2010. *Being pursued online: Extent and nature of cyberstalking victimisation from a lifestyle/routine activities perspective*. University of Cincinnati.
- Reyns, B.W. 2011. Online routines and identity theft victimisation: Further expanding Routine Activity Theory beyond direct-contact offences. *Journal of Research in Crime and Delinquency*, 50(2): 216-238.
- Richardson, R. 2010. *15th Annual 2010/2011 computer crime and security survey*. Computer Security Institute. Available at: <http://GoCSI.com> (retrieved: 13 October 2013).
- Ritter, J. 2015. *Contemporary digital information assets require new look at governance*. 5 April. Available at: <http://searchcompliance.techtarget.com/tip/Contemporary-digital-information-assets-require-new-look-at-governance> (retrieved: 13 October 2015).
- Robinson, R.M. 2015. *Social engineering attackers deploy fake social media profiles*. 6 November. Available at: <https://securityintelligence.com/social-engineering-attackers-deploy-fake-social-media-profiles/> (retrieved: 22 March 2016).
- Rogers, M., Seigfried, K. and Tidke, K. 2006. *Self-reported computer criminal behavior: A psychological analysis*. Available at: <http://www.dfrws.org/2006/proceedings/15-Rogers.pdf> (retrieved: 28 February 2016).
- Royse, D. 2008. *Research methods in social work* (5th edition). Belmont: Thomson Brooks/Cole.
- Rusch, J.J. 1999. *The "social engineering" of internet fraud*. Available at: http://www.isoc.org/isoc/conferences/inet/99/proceedings/3g/3g_2.htm (retrieved: 9 January 2016).
- Safa, N.S., Von Solms, R. and Fitcher, L. 2016. Human aspects of information security in organisations. *Computer Fraud & Security*, (2): 15-18.
- Saponaro, A. 2013. Theoretical approaches and perspectives in victimology. In R, Peacock. *Victimology in South Africa*. Pretoria: Van Schaik.



- SARS – see The South African Revenue Service.
- Schwandt, T.A. 2007. *The dictionary of qualitative research* (3rd edition). Thousand Oaks, CA: Sage.
- Shaw, R. 2013. *Social engineering: A hacking story*. InfoSec Institute. Available at: <http://resources.infosecinstitute.com/social-engineering-a-hacking-story> (retrieved: 27 June 2014).
- Schurink, W., Fouché, C.B. & De Vos, A.S. 2011. Qualitative data analysis and interpretation. In A.S. de Vos, H. Strydom, C.B. Fouché & C.S.L. Delport (Eds). *Research at grass roots: For the social sciences and human service professions* (4th edition). Pretoria: Van Schaik.
- Siegel, L.J. 2004. *Criminology: Theories, patterns and typologies* (8th edition). California: Thomson Learning.
- Siegel, L.J. 2011. *Criminology: The core* (4th edition). California: Cengage Learning.
- Siponen, M.T. 2005. An analysis of the traditional IS security approaches: Implications for research and practice. *European Journal of Information Systems*, (14): 303-315
- Sissing, S.K. 2013. *A criminological exploration of cyber stalking in South Africa*. Unpublished MA dissertation, University of South Africa, Pretoria.
- Slonka, K.J. 2014. *Awareness of malicious social engineering among Facebook users*. Unpublished PhD thesis, Robert Morris University, Pittsburgh.
- Spinapolice, M. 2011. *Mitigating the risk of social engineering attacks*. Unpublished MA dissertation, Rochester Institute of Technology, New York.
- Smith, E.R., Mackie, D.M. and Claypool, H.M. 2015. *Social psychology* (4th edition). New York: Psychology Press.
- Stock, P. and Burton, R.J.F. 2011. Defining terms for integrated (Multi-inter-transdisciplinary) sustainability research, *Sustainability*, (3): 1090-113.
- Stroebe, W., Hewstone, M. and Jonas, K. 2008. Introducing social psychology. In M. Hewstone, W. Stroebe and K. Jonas. *Introduction to social psychology: A European perspective* (4th edition). Oxford: Blackwell Publishing.
- Struwig, F.W. and Stead, G.B. 2001. *Planning, reporting and reporting research*. Cape Town: Pearson Education South Africa.
- Stuart, K. and Arthur, C. 2011. *PlayStation Network hack: Why it took Sony seven days to tell the world*. Available at: <http://www.theguardian.com/technology/gamesblog/2011/apr/27/playstation-network-hack-sony> (retrieved: 3 February 2016).
- Strydom, H. 2011. Sampling in the qualitative paradigm. In A.S. de Vos (Ed.), H. Strydom, C.B. Fouché and C.S.L. Delport. *Research at grass roots: For the social sciences and human service professions* (4th edition). Pretoria: Van Schaik.
- Strydom, H. and Delport, C.S.L. 2011. Sampling and pilot study in qualitative research. In A.S. de Vos (Ed.), H. Strydom, C.B. Fouché and C.S.L. Delport. *Research at*

- grass roots: For the social sciences and human service professions* (4th edition). Pretoria: Van Schaik.
- Sutherland, E.H. 1949. *White collar crime*. New York: Dryden.
- Sutherland, E.H. and Cressey, D.R. 1974. *Criminology* (9th edition). Philadelphia: J.B. Lippincott.
- Sykes, G.M. and Matza, D. 1957. Techniques of neutralization: A theory of delinquency. *American Sociological Review*, (22): 664–670.
- Teddlie, C. and Tashakkori, A. 2009. *Foundations of mixed methods research: Integrating quantitative and qualitative approaches in the social and behavioural sciences*. Thousand Oaks, CA: Sage.
- Terre Blanche, M., Durrheim, K. and Painter, D. 2006. *Research in practice: Applied methods for the social science*. Cape Town: University of Cape Town Press.
- The Verizon Risk Team. 2010. *2010 Data breach investigations report*. Verizon. Available at: http://www.wired.com/images_blogs/threatlevel/2010/07/2010-Verizon-Data-Breach-Investigations-Report.pdf (retrieved: 21 May 2015).
- The Verizon Risk Team. 2013. *2013 Data breach investigations report*. Verizon. Available at: http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf (retrieved: 13 October 2015).
- The Verizon Risk Team. 2015. *2015 Data breach investigations report*. Verizon. Available at: <http://www.verizonenterprise.com/DBIR/2015/> (retrieved: 13 October 2015).
- The South African Revenue Service. 2016. *Scams and phishing attacks*. Available at: <http://www.sars.gov.za/TargTaxCrime/Pages/Scams-and-Phishing.aspx?k> (retrieved: 10 March 2016).
- The Statistics Portal. 2016. Statistics and facts about social networks. Available at: <https://www.statista.com/topics/1164/social-networks/> (retrieved: 10 July 2016).
- Thomas, S. 2014. *16 graphs that shed new light on the South African smartphone space*. Available at: <http://memeburn.com/2014/08/16-graphs-that-shed-new-light-on-the-south-african-smartphone-space/> (retrieved: 24 May 2016).
- Thornburgh, T. 2004. *Social engineering: The “Dark Art”*. Available at: <http://dl.acm.org/citation.cfm?id=1059554> (retrieved: 15 June 2014).
- Thorne, S., Armstrong, E., Harris, S., Hislop, T., Kim-Sung, C. and Oglov, V. 2009. Patient real-time and 12-month retrospective perceptions of difficult communications in the cancer diagnostic period. *Qualitative Health Research*, 19: 1383-1394.
- Thulin, J. 2015. *Could PoPI help curb the rising tide of cybercrime in South Africa?* Available at: <http://memeburn.com/2015/03/could-popi-help-curb-the-rising-tide-of-cybercrime-in-south-africa/> (retrieved: 27 January 2016).
- Tibbetts, S.G. and Hemmens, C. 2010. *Criminological theory: A text/reader*. London: Sage.
- Tierney, J. 2006. *Criminology: Theory and context* (2nd edition). England: Pearson Education.

- Towle, A. 2016. *Security on the spot with internet solutions*. 17 May. Available at: http://www.itweb.co.za/index.php?option=com_content&view=article&id=152596 (retrieved: 20 May 2016).
- Trim, P. and Upton, D. 2013. *Cyber security culture: Counteracting cyber threats through organizational learning and training*. Surrey: Gower Publishing.
- Tubbs, B. 2015. *SA's 2015 smartphone scene*. Available at: http://www.itweb.co.za/index.php?option=com_content&view=article&id=140378 (retrieved: 24 May 2016).
- Tuli, F. 2010. The basis of distinction between qualitative and quantitative research in social science: Reflection on ontological, epistemological and methodological perspectives. *Ethiopian Journal of Education and Sciences*, 6(1): 97-108.
- Van der Westhuizen, M. 2011. *Criminological theories*. In C. Bezuidenhout. *A Southern African perspective on fundamental criminology*. Cape Town: Pearson Education South Africa.
- Van Jaarsveldt, L.C. 2010. *Information technology competence in undergraduate public administration curricula*. Unpublished MA Thesis, University of South Africa, Pretoria.
- Van Niekerk, J.F. and Von Solms, R. 2009. Information security culture: A management perspective. *Computers & Security*, 29: 476-486.
- Vermeulen, J. 2013. *How scammers hack your bank account*. 17 April. Available at: <http://mybroadband.co.za/news/security/75807-how-scammers-hack-your-bank-account.html> (retrieved: 10 March 2016).
- Vodacom, 2016. *SA internet use set to skyrocket by 2019*. Available at: <http://now.vodacom.co.za/article/2016/01/14/south-african-internet-use-set-to-skyrocket-by-2019> (retrieved: 14 August 2016).
- Von Solms, E. and Eloff, J.H.P. 2004. *Information security development trends*. Available at: <http://citeseerx.ist.psu.edu/viewdoc/download> (retrieved: 7 April 2016).
- Walters, G.D. 2012. *Crime in a psychological context: From career criminals to criminal careers*. London: Sage.
- Wang, Y. 2013. *More people have cell phones than toilets, U.N. study shows*. 25 March. Available at: <http://newsfeed.time.com/2013/03/25/more-people-have-cell-phones-than-toilets-u-n-study-shows/> (retrieved: 21 January 2016).
- Webber, C. 2010. *Psychology and crime: Key approaches to criminology*. London: Sage.
- Whitaker, A., Evans, K. and Voth, J.B. 2009. *Chained exploits*. Boston: Pearson Education.
- White, R. and Haines, F. 2004. *Crime and criminology: An introduction* (3rd edition). Oxford: Oxford University Press.
- Whitman, M.E. and Mattord, H.J. 2008. *Management of information security* (2nd edition). Boston: Course Technology Cengage Learning.

- Whitman, M.E. and Mattord, H.J. 2012. *Principles of information security* (4th edition). Boston: Course Technology Cengage Learning.
- Williams, F.P. and McShane, M.D. 2013. *Criminological theory* (6th edition). New Jersey: Prentice Hall.
- Woit, D. and Mason, D. 2003. Effectiveness of online assessment. Available at: <http://dl.acm.org/citation.cfm?id=611952> (retrieved: 30 September 2016).
- Wood, A.F. and Smith, M.J. 2014. *Online communication: Linking technology, identity and culture* (2nd edition). New York: Psychology Press.
- Wood, M. 2010. *Want my autograph? The use and abuse of digital signatures by malware*. Available at: https://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/digital_signature_abuse.pdf?la=en.pdf?dl=true (retrieved: 29 May 2016).
- Workman, J.E. 2011. Information security managers. Available at: <http://www.holisticpage.com.au/information-security-for-managers-workman/9780763793012> (retrieved: 20 September 2015).
- Yeh, Q.Y. and Chang, J.T. 2007. Threats and countermeasures for information systems security: A cross-industry study. *Information & Management*, 44: 480-491.
- Young, R. 2015. *Advanced cyber defence is essential*. 24 December. Available at: <http://www.itnewsafrika.com/2015/12/advanced-cyber-defence-is-essential/> (retrieved: 20 February 2016).

ANNEXURE A: Ethical clearance certificate

	
COLLEGE OF LAW RESEARCH ETHICS REVIEW COMMITTEE	
Date: 04-03-2016	
<div>Reference: P5 Applicant: SK Jansen van Rensburg</div>	
Dear SK Jansen van Rensburg	
DECISION: ETHICS APPROVAL	
Name	SK Jansen van Rensburg
Proposal	An evaluation of the human element in information security: an analysis of social engineering attacks
Qualification	PhD
Thank you for the application for research ethics clearance by the College of Law Research Ethics Review Committee for the above mentioned research. Final approval is granted.	
<i>The application was reviewed in compliance with the Unisa Policy on Research Ethics.</i>	
<i>The proposed research may now commence with the proviso that:</i>	
<ol style="list-style-type: none"><i>The researcher will ensure that the research project adheres to the values and principles expressed in the Unisa Policy on Research Ethics which can be found at the following website:</i> http://www.unisa.ac.za/cmsys/staff/contents/departments/res_policies/docs/Policy_Research%20Ethics_rev%20app%20Council_22.06.2012.pdf<i>Any adverse circumstances arising in the undertaking of the research project that is relevant to the ethicality of the study, as well as changes in the methodology, should be communicated in writing to the College of Law Ethical Review Committee.</i>	
<div> Open Rubric</div> <div>University of South Africa Preller Street, Muckleneuk Ridge, City of Tshwane PO Box 392, Unisa, 0003, South Africa www.unisa.ac.za/laure</div>	

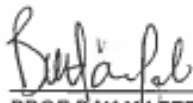
An amended application could be requested if there are substantial changes from the existing proposal, especially if those changes affect any of the study-related risks for the research participants

3. *The researcher will ensure that the research project adheres to any applicable national legislation, professional codes of conduct, institutional guidelines and scientific standards relevant to the specific field of study.*

Note:

The reference number (top right corner of this communique) should be clearly indicated on all forms of communication (e.g. Webmail, E-mail messages, letters) with the intended research participants, as well as with the URERC.

Kind regards



PROF B W HAEFELE
CHAIR PERSON: RESEARCH ETHICS
REVIEW COMMITTEE
COLLEGE OF LAW



PROF R SONGCA
EXECUTIVE DEAN:
COLLEGE OF LAW

ANNEXURE B: Informed consent form (subject matter experts)



INFORMED CONSENT FORM: SUBJECT MATTER EXPERTS

Researcher: Shandré Kim Jansen van Rensburg
Department of Criminology and Security Sciences
(contact details omitted)

Supervisor: Professor Johan Prinsloo
Department of Criminology and Security Sciences
(contact details omitted)

Dear Research Respondent,

The human element in information security: An analysis of social engineering attacks in the greater Tshwane area of Gauteng, South Africa

Thank you for your involvement in this research study. Please enquire about the research proposal for more information regarding the study. You were chosen to take part in this study because of your identified knowledge and insight on the topic at hand. It is deemed ethical practice to obtain informed consent from a research respondent prior to the commencement of a research initiative.

Informed consent involves the following:

1. **Purpose of the study.** The present study is being undertaken for the fulfillment of a PhD Degree in Criminology at the University of South Africa. To explore, describe, explain and analyse social engineering attacks through a Multi-Inter-Trans-disciplinary approach in order to better understand and measure such attacks as a means to formulate a proactive strategy.
2. **Procedures.** A semi-structured interview will be used in order to gain valuable information from the participants. The interview will serve as a means to gain insight



University of South Africa
Pretorius Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

last longer the 60 minutes and will be held according to the participant's convenience. The interviewer will be recorded and notes will be written during the interview.

3. **Risks and discomfort.** There are no predetermined risks accompanying this study. The research participant is merely providing the researcher with knowledge about the subject matter.
4. **Benefits.** There are no perceptible benefits or incentives available for the respondents of this study. However, it can be proposed that the research participant will benefit in some way through the process of knowledge production. If the researcher receives permission from the respondent, the researcher will publish their names in the final dissertation. The study will benefit the local community and society at large through the awareness of information security guidelines.
5. **Respondent's rights.** Respondents are of liberty to withdraw from the study at any stage of the research provided a courtesy notification of withdrawal is sent to the researcher. No negative repercussions will be enacted on the respondent, as participation is voluntary, and all data received from the respondent will be assumed void.
6. **Confidentiality.** All information will be regarded as private and confidential. The researcher will not disclose respondents' names or contact details unless permission is obtained.
7. **Data storage and dissemination of findings.** The information received will be stored (password protected and in a locked cabinet) by the researcher for five years before being destroyed electronically (deleting of the files) and physically (shredding of the collected data). The findings of the research will be documented in the form of an academic dissertation.
8. **Ethical considerations.** The study was ethically constructed and approved by UNISA's Ethical Committee.
9. **Questions and concerns.** The researcher welcomes any questions or concerns regarding the research study.



Please provide your initials and surname below:

I understand my rights as a research respondent and voluntarily give my consent to participate.	
Research respondent:	Date:
Researcher: S.K Jansen van Rensburg	Date:



University of South Africa
Pretorius Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

ANNEXURE C: Semi-structured interview schedule (subject matter experts)



SEMI-STRUCTURED INTERVIEW SCHEDULE – SUBJECT MATTER EXPERTS

I, Shandre Jansen van Rensburg, am a PhD candidate, currently enrolled at the University of South Africa (UNISA). In order to meet the degree's requirements, empirical research needs to be undertaken. Therefore, any information obtained from the interview will be for research and academic purposes only.

The study's objective is to explore, describe, explain and analyse social engineering attacks through a Multi-Inter-Trans-disciplinary approach in order to better understand, measure and explain such attacks as a means to formulate a proactive strategy. Thus, the aim of this interview is to gather vital information pertaining to the study at hand in an effort to meet the study's objective.

Please refer to the informed consent form for more information regarding the purpose of the study, the procedures involved, risks and discomfort, benefits, respondent's rights, confidentiality, data storage and dissemination of findings, ethical considerations and any questions and concerns.

FOR OFFICIAL USE	
Date:	
Consent form signed:	
Interview number:	



University of South Africa
Profler Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

SECTION A: BIOGRAPHICAL DATA
1. What is your educational background?
2. What is your highest qualification?
3. Briefly indicate your work experience.
4. Which position do you hold at your employed institution?
5. What does your current position entail on a daily basis?
SECTION B SEMI-STRUCTURED INTERVIEW The following questions are based on your knowledge and experience regarding Information Security and social engineering.
6. What is meant by the term "social engineering"?
7. According to your knowledge, how prominent is social engineering in South Africa?
8. Who are vulnerable to social engineering attacks?
9. According to your knowledge, who is the typical social engineer?
10. How does social engineering impact on your current employment or research?
11. According to your knowledge, what types of social engineering attacks are most prevalent?
12. In your opinion, how does social engineering affect business institutions?
13. In your opinion, how does social engineering affect the public?
14. How can businesses safeguard themselves against social engineering attacks?
15. How can the public safeguard themselves against social engineering attacks?
16. To what extent does human vulnerability affect Information Security?
17. Are you familiar with legislation regarding Information Security? If so, how does it affect the operational functioning of businesses?
18. Is there anything else you would like to mention?



ANNEXURE D: Letter of motivation



LETTER OF MOTIVATION

Professor JH Prinsloo
Department of Criminology and Security Science
School of Criminal Justice
College of Law
March 2016

TO WHOM IT MAY CONCERN,

Dear Sir/Madam

RESEARCH STUDY: THE HUMAN ELEMENT IN INFORMATION SECURITY: AN ANALYSIS OF SOCIAL ENGINEERING ATTACKS IN THE GREATER TSHWANE AREA OF GAUTENG, SOUTH AFRICA

Shandré Jansen van Rensburg is a lecturer at the University of South Africa (UNISA) in the Department of Criminology and Security Science. She is currently enrolled for a PhD in the subject of Criminology. The title of her research study is *"The human element in information security: An analysis of social engineering attacks in the greater Tshwane Area of Gauteng, South Africa"*. Ms Jansen van Rensburg successfully completed her Master's degree (MA) in Criminology in 2013 where she obtained her degree *cum laude*.

During the course of history, human beings have sought to protect and secure themselves against all types of threats to their well-being and their property. In light of technological advances, the concept of property has evolved to include not only tangible assets such as land or possessions but also intangible belongings such as ideas, artistic works or information. Social engineering involves the targeting of people through deception and manipulation with the purpose of two main outcomes – direct loss of



University of South Africa
Proffer Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

critical information and the achievement of some action intended by the attacker. As a countermeasure, it can be assumed that stricter technical controls should be a viable solution to social engineering. However, stricter technical controls cannot effectively deal with the issues surrounding human beings, their inherent nature and security. The impact of social engineering attacks vary widely according to the nature of the attack. Big corporations, private industries, businesses, government agencies as well as individuals are at risk to information security breaches. Furthermore, many of these attacks, data breaches and stolen information are carried out for criminal purpose.

The purpose of the current research study entails the following:

- To explore and describe the occurrence and nature of social engineering attacks.
- To explore and describe the awareness of social engineering attacks and Information Security.
- To analyse and explain the contextual role of social engineering attacks within the various disciplines through a Multi-Inter-Trans-disciplinary research.
- To integrate and evaluate the research results to design and apply an integrative Multi-Inter-Trans-disciplinary social engineering model.

Research plays a vital role in informing the decision making processes regarding security related issues. Ms. Jansen van Rensburg proposes to come to your institution to make a presentation based on her studies regarding the dangers of social engineering, the potential impact it has on business and how the related South African legislation impacts your institution. She will then request the personnel who attend the presentation to complete a short questionnaire regarding Information Security and social engineering. All information will be regarded as personal and confidential. The questionnaire does not require the research respondent to provide his or her name and no names or contact details of the respondents or their affiliated institution will be disclosed for any reasons. The study has obtained Unisa's ethical clearance to ensure the institution's integrity and confidentiality. The presentation and completion of the group-administered questionnaires will take no longer than 60 minutes. A possible date and time of this information session will be requested at your earliest convenience. This vital information security awareness session will be offered free of charge as it is purely for research purposes.



University of South Africa
Pretorius Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

Your participation and cooperation in this regard would be much appreciated.

Please feel free to contact Ms. Jansen van Rensburg's research supervisor, **Prof Johan Prinsloo** (Department of Criminology and Security Science, School of Criminal Justice, College of Law, UNISA) (contact details omitted) for any further queries or verification.

For more information or for arrangement purposes, please contact **Ms. Jansen van Rensburg**, her details are as follows (contact details omitted).

Yours sincerely,



Prof JH Prinsloo
Research Professor
Department of Criminology and Security Science



University of South Africa
Pretorius Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

ANNEXURE E: Informed consent form (group-administered questionnaire)



INFORMED CONSENT FORM: GROUP-ADMINISTERED QUESTIONNAIRE

Researcher: Shandre Kim Jansen van Rensburg
Department of Criminology and Security Sciences
(contact details omitted)

Supervisor: Professor Johan Prinsloo
Department of Criminology and Security Sciences
(contact details omitted)

Dear Research Respondent,

The human element in information security: An analysis of social engineering attacks in the greater Tshwane area of Gauteng, South Africa

Thank you for your involvement in this research study. Please enquire about the research proposal for more information regarding the study. It is deemed ethical practice to obtain informed consent from a research respondent prior to the commencement of a research initiative. Informed consent involves the following:

1. **Purpose of the study.** The present study is being undertaken for the fulfillment of a PhD Degree in Criminology at the University of South Africa. The purpose of this study is to explore, describe, explain and analyse social engineering attacks through a Multi-Inter-Trans-disciplinary approach in order to better understand and measure such attacks as a means to formulate a proactive strategy.
2. **Procedures.** The researcher will hand out a questionnaire to the research respondent. The questionnaire should not take more than 20 minutes to complete. Thereafter, a presentation on the topic at hand will be conducted.
3. **Risks and discomfort.** There are no predetermined risks accompanying this study. The research participant is merely providing the researcher with insight and personal experience about the subject matter.



University of South Africa
Pretorius Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

experience about the subject matter.

4. **Benefits.** There are no perceptible benefits or incentives available for the respondents of this study. However, it can be proposed that the research participant will benefit by becoming more information security conscious when completing the questionnaire. The study will benefit the local community and society at large through the awareness of information security guidelines.
5. **Respondent's rights.** Respondents are of liberty to withdraw from the study at any stage of the research provided a courtesy notification of withdrawal is expressed to the researcher. No negative repercussions will be enacted on the respondent, as participation is voluntary.
6. **Confidentiality.** All information will be regarded as personal and confidential. The questionnaire does not require the research respondent to provide his or her name and no names or contact details of the respondents will be disclosed for any reasons.
7. **Data storage and dissemination of findings.** The information received will be stored (password protected and in a locked cabinet) by the researcher for five years before being destroyed electronically (deleting of the files) and physically (shredding of the collected data). The findings of the research will be documented in the form of an academic dissertation.
8. **Ethical considerations.** The study was ethically constructed and approved by UNISA's Ethical Committee.
9. **Questions and concerns.** The researcher welcomes any questions or concerns regarding the research study.

I understand my rights as a research respondent and voluntarily give my consent to participate.	
Research respondent:	Date:
Researcher: S.K Jansen van Rensburg	Date:



ANNEXURE F: Group administered questionnaire



GROUP-ADMINISTERED QUESTIONNAIRE

I, Shandr  Jansen van Rensburg, am a PhD candidate, currently enrolled at the University of South Africa (UNISA). In order to meet the degree's requirements, empirical research needs to be undertaken. Therefore, any information obtained from this questionnaire will be for research and academic purposes only.

The study's objective is to explore, describe, explain and analyse social engineering attacks through a Multi-Inter-Trans-disciplinary approach in order to better understand, measure and explain such attacks as a means to formulate a proactive strategy. Thus, the aim of this questionnaire is to gather vital information pertaining to the study at hand in an effort to meet the study's objective.

Please see the informed consent form for more information regarding the purpose of the study, the procedures involved, risks and discomfort, benefits, respondent's rights, confidentiality, data storage and dissemination of findings, ethical considerations and any questions and concerns.

FOR OFFICIAL USE	
Date:	
Consent form signed:	
Questionnaire number:	



University of South Africa
Pretorius Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA, 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

INSTRUCTIONS: Please circle the relevant option. In some cases, more than one option can be circled if relevant. Please feel free to request clarity if you do not understand any question. The questionnaire is eight pages (back-to-back) long and consists of 43 questions. Please ensure that all the questions are answered. The questionnaire will take approximately 20 minutes to answer.

SECTION A: BIOGRAPHICAL DETAILS

1. Gender

Male	1
Female	2

2. Race

Black	1	White	2	Coloured	3
Indian	4	Other	5		

2.1 If other, please specify _____

3. How old are you?

4. Marital Status

Single	1	Married	2
Divorced	3	Widow(er)	4

SECTION B: EMPLOYMENT DETAILS

5. What is your occupation?

6. How long have you been employed by your current employer?



SECTION C: GENERAL USE OF COMMUNICATION THROUGH TECHNOLOGY

7. Which technological devices do you access the Internet from?

Computer	1	Laptop	2
Tablet	3	Mobile phone	4
Other	5		

7.1 If other, please specify:

8. How many hours a day, do you use the Internet?

9. On a daily basis, what do you use the Internet for?

Browsing	1	E-mails	2
Work-purposes	3	Social networking	4
Internet banking	5	Other	6

9.1 If other, please specify

10. To what extent would you agree or disagree with the view that your personal information might be accessible to the general public?

Totally agree	1	Agree	2
Uncertain	3	Disagree	4
Totally disagree	5		

10.1 Please provide a reason(s) for your answer:



11. To what extent do you consider your telephone number to be accessible to the general public?

Very accessible	1	Accessible	2
Uncertain	3	Somewhat accessible	4
Not at all accessible	5		

11.1 Please provide a reason(s) for your answer:

12. To what extent do you consider your e-mail address to be accessible to the general public?

Very accessible	1	Accessible	2
Uncertain	3	Somewhat accessible	4
Not at all accessible	5		

12.1 Please provide a reason(s) for your answer:

SECTION D: ACCESS TO AND VERIFICATION OF PERSONAL INFORMATION

13. Does your Institution's access control procedure address access to sensitive and personal information?

Yes	1
No	2
Unsure	3

13.1 If yes, indicate how:



14. Is a password management process compulsory in your institution?

Yes	1
No	2
Unsure	3

14.1 If yes, please indicate which of the following statements are true in relation to your institution. Tick the true statements:

Unique username and password for user authentication is mandatory.	
Passwords must be complex and alphanumeric.	
Users are technologically required to change passwords on a regular basis.	
The same password cannot be reused.	
Technology is configured to allow authorised users to change passwords when the need arises.	
Unsure of the process.	

15. Are the connections from laptops, mobile phones, tablets and remote users (users who access connections from a distance) into the company's network secured?

Yes	1
No	2
Unsure	3

16. Are passwords used to protect sensitive information?

Always	1	Often	2
Seldom	3	Never	4
Unsure	5		

17. How often do you come into contact with the following personal information which does not belong to you on a daily basis? Please tick the relevant option.

	Very often	Often	Seldom	Not at all
Biographical information				
Information relating to the education or the medical, financial, criminal or employment history				
Any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment				
Personal opinions, views or preferences				
Correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence				
Other				



17.1 If other, please specify:

18. To what extent do you believe the following information can be used in an attack against your institution? Please tick the relevant option.

	Highly possible	Possible	Fairly possible	Impossible
Biographical information				
Information relating to the education or the medical, financial, criminal or employment history				
Any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment				
Personal opinions, views or preferences				
Correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence				
Other				

18.1 If other, please specify:

19. To what extent do you consider it safe to provide your identification (i.e. username) via telephone?

Very safe	1	Safe	2
Uncertain	3	Fairly safe	4
Not safe at all	5		

20. To what extent do you consider it safe to provide authentication (i.e. password) via telephone?

Very safe	1	Safe	2
Uncertain	3	Fairly safe	4
Not safe at all	5		

21. To what extent do you consider it safe to provide your identification (i.e. username) via e-mail?

Very safe	1	Safe	2
Uncertain	3	Fairly safe	4
Not safe at all	5		



22. To what extent do you consider it safe to provide authentication (i.e. password) via e-mail?

Very safe	1	Safe	2
Uncertain	3	Fairly safe	4
Not safe at all	5		

23. To what extent do you consider it safe to physically provide your Identification (i.e. username) when dealing with a person unknown to you?

Very safe	1	Safe	2
Uncertain	3	Fairly safe	4
Not safe at all	5		

24. To what extent do you consider it safe to physically provide authentication (i.e. password) when dealing with a person unknown to you?

Very safe	1	Safe	2
Uncertain	3	Fairly safe	4
Not safe at all	5		

25. Do you make use of an e-mail signature?

Yes	1
No	2
Unsure	3

26. How do you get rid of personal and sensitive Information, physically?

27. How do you get rid of personal and sensitive Information, electronically?



SECTION E: ACCESS CONTROL

28. Indicate which technological devices you use are protected by passwords?

Mobile phone	1	Tablet	2
Computer	3	Laptop	4

29. To what extent are your passwords the same?

All of my passwords are the same	1	Most of my passwords are the same	2
My passwords differ somewhat	3	All of my passwords differ	4

30. How often do you change your password?

Only when prompted	1	Often	2
Not often	3	Never	4

31. How often do you keep your social networking applications logged in?

All the time	1	Most times	2
Seldom	3	Never, I always log out	4
Not applicable	5		

32. Where do you store your passwords?

33. Does any other person have access to your passwords?

Yes	1
No	2



33.1 If yes, who has access to your passwords?

34. When is user access revoked from ex-employees?

Immediately	1	Days after termination	2
Months after termination	3	Never	4
Unsure	5		

SECTION F: SOCIAL ENGINEERING

35. Do you know what social engineering is?

Yes	1
No	2

35.1 If yes, please explain what it is.

36. How aware are you of social engineering threats?

Very aware	1	Somewhat aware	2
Somewhat unaware	3	Not aware at all	4



37. The following questions are based on hypothetical scenarios. In as much detail as possible, indicate how you would respond to the following hypothetical scenarios.

37.1 *The Chief Financial Officer (CFO), of your company, whom you have never met before, is located in another province. The CFO is known, by those who have had an encounter with him, for his high-pitched voice. One morning a man speaking in a high-pitched voice phones you, identifying himself as the CFO, and requests confidential financial information from you.*

37.2 *An authoritative figure, unknown to you, informs you that he has permission from an authorised person, known to you, to use confidential information. The known colleague is away on maternity leave and has requested not to be disturbed. The authoritative figure identifies your colleague and confirms her current whereabouts and subsequently requests confidential information from you.*

37.3 *You have been experiencing problems with your laptop and require urgent assistance. As such you receive a phone call from a technician at desktop support who, in an effort to solve your problem, requests for your login credentials.*



37.4 A person unknown to you stands closely behind you as you key in personal identification and authentication credentials on your mobile phone, laptop or automated teller machine (ATM).

37.5 A person you do not know asks you to kindly hold the door for him/her while accessing the building (where your offices are located).

37.6 You receive what appears to be a legitimate invitation to a job interview which you have recently applied for. As the job is in another country; the employer offers to pay for your travel arrangements. The invitation requests you to follow a link and subsequently requires you to enter your banking details so that payment can be made.



37.7 Your company credit card is almost about to expire and you have applied to renew it. You receive a phone call from a representative from your bank requesting that you confirm the following personal details: Identity Number, telephone number, physical address, work address and all the information pertaining to your previous credit card.

37.8 You receive an e-mail from what appears to be a legitimate sender informing you that there is a virus circulating through the Internet and that specific files should be deleted and security settings should be changed.

37.9 You find a USB flash drive with a company logo labeled "Executive Salary Summary" left in the bathroom cubicle.



37.10 You receive a pop-up window, while working on your company laptop, which advertises a special to a travel location that you have been researching. The pop-up screen conveys that this special is only valid for a limited time period.

37.11. You, in your work e-mail, receive an influx of e-mails which appear to be spam.

38. In your opinion, what do you think the main motive(s) behind the above threats are?

39. In your opinion, who is most at risk to the risks illustrated in the hypothetical scenarios?

New employees	1	Contract workers	2
Executive assistants	3	IT personnel	4
Human resources	5	Executive personnel	6
Other	7		



University of South Africa
 Pretorius Street, Muckleneuk Ridge, City of Tshwane
 PO Box 392 UNISA 0003 South Africa
 Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

39.1 If other, please specify:

40. In your opinion, does your Institution maintain a healthy Information Security culture?

Yes	1
No	2
Unsure	3

40.1 Please provide reasons for your answer.

SECTION G: LEGISLATION RELATED TO INFORMATION SECURITY

41. Do you know of any South African legislation relating to Information Security and social engineering?

Yes	1
No	2
Uncertain	3

If yes, please answer questions 41.1 to 41.3.



41.1 How does the Protection of Personal Information Act 4 of 2013 Impact on Information Security?

41.2 How does the Electronic Communications and Transactions Act 25 of 2002 Impact on Information Security?

41.3 How could the Cybercrime and Cybersecurity Bill Impact on Information Security?

42. How has completing this questionnaire Impacted on your own Information Security in the workplace?



43. Is there anything else you would like to mention?

END OF QUESTIONNAIRE
Thank you for your participation!

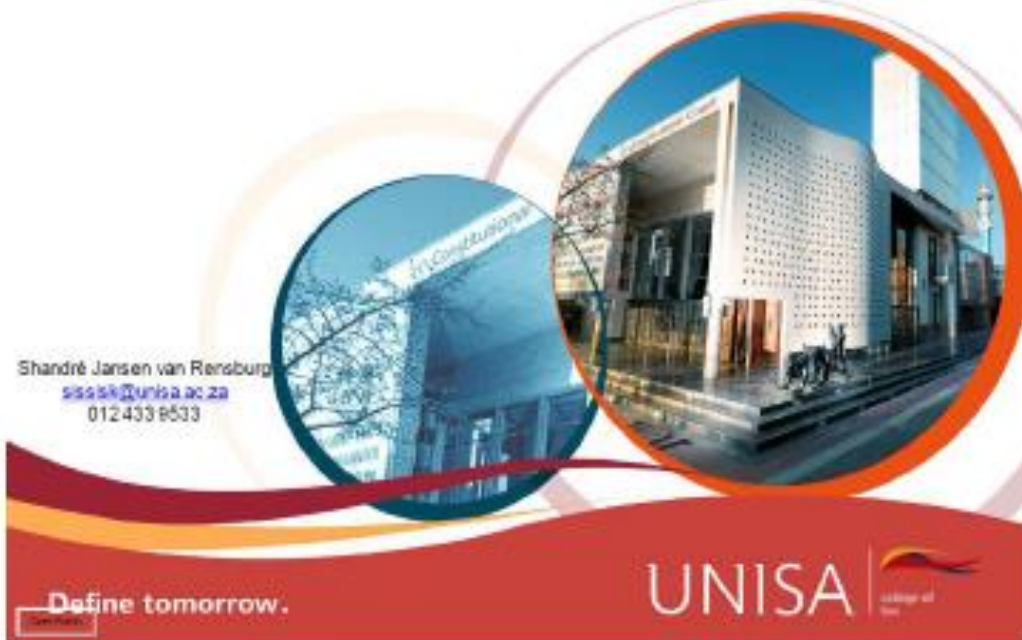


University of South Africa
Pretorius Street, Muckleneuk Ridge, City of Tshwane
PO Box 393, UNISA, 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

ANNEXURE G: Business presentation

SOCIAL ENGINEERING AND THE HUMAN ELEMENT IN INFORMATION SECURITY

Shandré Jansen van Rensburg
sjs@unisa.ac.za
012 433 9533



INTRODUCTION & OVERVIEW

- Social engineering has roots in various disciplines - Computer Science, Psychology, Law, Criminology & Security Science
- Presentation Focus:
 - The problem of social engineering
 - Social engineering threats and attacks
 - Human aspects in Information Security
 - South African legislation

THE PROBLEM OF SOCIAL ENGINEERING

- The perpetrator induces the victim to release information or perform unauthorised actions
- Two main outcomes:
 1. Direct loss of critical information
 2. Achievement of some action intended by the attacker

THE SOCIAL ENGINEERING ATTACK CYCLE



(Source: Authors' own elaboration as adapted from Mitnick and Simon (2009))

SUCCESSFUL SOCIAL ENGINEERING ATTACKS

- **Method.** He or she must have the skills and tools and other necessary resources to perpetrate an attack.
- **Opportunity.** A perpetrator must have the time and the access to perform and succeed with an attack.
- **Motive.** There must be a reason for a perpetrator to perform an attack on the system.

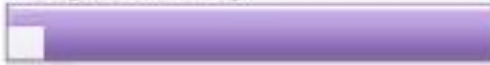
THE INSIDER THREAT

- Data breaches – intentional or unintentional
- Motivations – financial, malicious
- Methods – selling or destroying



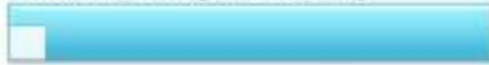
MODUS OPERANDI

Human based social engineering



- ☐ Impersonation
- ☐ Authoritative figure
- ☐ Shoulder surfing
- ☐ Dumpster diving

Technological based social engineering



- ☐ Phishing (vishing, spear-phishing, whaling, pharming)
- ☐ Hoaxing
- ☐ Baiting
- ☐ Online scams

HUMANS AS THE WEAKEST LINK

Case Study: Etna Industrial



SOUTH AFRICAN LEGISLATION

- The Electronic Communications and Transactions Act
- The Protection of Personal Information Act
- The Cybercrime and Cybersecurity Bill



CONCLUDING REMARKS

- Security is often an illusion - fueled by gullibility, naïveté and/ or ignorance.
- Social engineering practices are successful when people are unaware of good security practices.
- In this way, it can be maintained that security is not a product but rather a process.

Thank you

For more information please contact:
Mrs. Shandré Jansen van Rensburg



Learn without limits.

UNISA  College of
the South

ANNEXURE H: Informed consent form (self-administered questionnaire)



INFORMED CONSENT FORM: SELF-ADMINISTERED QUESTIONNAIRE

Researcher: Shandre Kim Jansen van Rensburg
Department of Criminology and Security Sciences
(contact details omitted)

Supervisor: Professor Johan Prinsloo
Department of Criminology and Security Sciences
(contact details omitted)

Dear Research Respondent,

The human element in information security: An analysis of social engineering attacks in the greater Tshwane Area of Gauteng, South Africa

Thank you for your involvement in this research study. Please enquire about the research proposal for more information regarding the study. You were chosen to take part in this study due to your willingness to take part in the information security awareness presentation. It is deemed ethical practice to obtain informed consent from a research respondent prior to the commencement of a research initiative.

Informed consent involves the following:

1. **Purpose of the study.** The present study is being undertaken for the fulfillment of a PhD Degree in Criminology at the University of South Africa. The purpose of this study is to explore, describe, explain and analyse social engineering attacks through a Multi-Inter-Trans-disciplinary approach in order to better understand and measure such attacks as a means to formulate a proactive strategy.
2. **Procedures.** The researcher will hand out a questionnaire to the research respondent. The questionnaire should not take more than 20 minutes to complete.
3. **Risks and discomfort.** There are no predetermined risks accompanying this study.



University of South Africa
Pretorius Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

The research participant is merely providing the researcher with insight and personal experience about the subject matter.

4. **Benefits.** There are no perceptible benefits or incentives available for the respondents of this study. However, it can be proposed that the research participant will benefit by gaining valuable awareness training regarding social engineering and information security. The study will benefit the local community and society at large through the awareness of information security guidelines.
5. **Respondent's rights.** Respondents are of liberty to withdraw from the study at any stage of the research provided a courtesy notification of withdrawal is expressed to the researcher. No negative repercussions will be enacted on the respondent, as participation is voluntary.
6. **Confidentiality.** All information will be regarded as personal and confidential. The questionnaire does not require the research respondent to provide his or her name and no names or contact details of the respondents will be disclosed for any reasons.
7. **Data storage and dissemination of findings.** The information received will be stored (password protected and in a locked cabinet) by the researcher for five years before being destroyed electronically (deleting of the files) and physically (shredding of the collected data). The findings of the research will be documented in the form of an academic dissertation.
8. **Ethical considerations.** The study was ethically constructed and approved by UNISA's Ethical Committee.
9. **Questions and concerns.** The researcher welcomes any questions or concerns regarding the research study.

I understand my rights as a research respondent and voluntarily give my consent to participate.	
Research respondent:	Date:
Researcher: S.K Jansen van Rensburg	Date:



ANNEXURE I : Self-administered questionnaire



SELF-ADMINISTERED QUESTIONNAIRE

I, Shandré Jansen van Rensburg, am a PhD candidate, currently enrolled at the University of South Africa (UNISA). In order to meet the degree's requirements, empirical research needs to be undertaken. Therefore, any information obtained from this questionnaire will be for research and academic purposes only.

The study's objective is to explore, describe, explain and analyse social engineering attacks through a Multi-Inter-Trans-disciplinary approach in order to better understand, measure and explain such attacks as a means to formulate a proactive strategy. Thus, the aim of this questionnaire is to gather vital information pertaining to the study at hand in an effort to meet the study's objective.

Please see the informed consent form for more information regarding the purpose of the study, the procedures involved, risks and discomfort, benefits, respondent's rights, confidentiality, data storage and dissemination of findings, ethical considerations and any questions and concerns.

FOR OFFICIAL USE	
Date:	
Consent form signed:	
Questionnaire number:	



University of South Africa
Pretorius Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

INSTRUCTIONS: Please circle the relevant option. In some cases, more than one option can be circled if relevant. Please feel free to request clarity if you do not understand any question. The questionnaire is seven pages long (back-to-back) and consists of 38 questions. Please ensure that all the questions are answered. The questionnaire will take approximately 15 minutes to answer.

SECTION A: BIOGRAPHICAL DETAILS

1. Gender

Male	1
Female	2

2. Race

Black	1	White	2	Coloured	3
Indian	4	Other	5		

2.1 If other, please specify _____

3. How old are you?

4. Marital Status

Single	1	Married	2
Divorced	3	Widow(er)	4

SECTION B: EMPLOYMENT DETAILS

5. What is your occupation?

6. Provide a brief job description of what your job entails.



7. How long have you been employed by your current employer?

SECTION C: GENERAL USE OF COMMUNICATION THROUGH TECHNOLOGY

8. Which technological devices do you access the Internet from?

Personal Computer	1	Laptop	2
Tablet	3	Mobile phone	4
Other	5		

8.1 If other, please specify:

9. How many hours a day, do you use the Internet?

10. On a daily basis, what do you use the Internet for?

Browsing	1	E-mails	2
Work purposes	3	Social networking	4
Internet banking	5	Other	6

10.1 If other, please specify

11. To what extent would you agree or disagree with the view that your personal information might be accessible to the general public?

Totally agree	1	Agree	2
Uncertain	3	Disagree	4
Totally disagree	5		

11.1 Please provide a reason(s) for your answer:



12. To what extent do you consider your telephone number to be accessible to the general public?

Very accessible	1	Accessible	2
Uncertain	3	Somewhat accessible	4
Not at all accessible	5		

12.1 Please provide a reason(s) for your answer:

13. To what extent do you consider your e-mail address to be accessible to the general public?

Very accessible	1	Accessible	2
Uncertain	3	Somewhat accessible	4
Not at all accessible	5		

13.1 Please provide a reason(s) for your answer:

SECTION D: IDENTIFICATION AND AUTHENTICATION

14. How often do you come into contact with the following personal information which does not belong to you on a daily basis? Please tick the relevant option.

	Very often	Often	Seldom	Not at all
Biographical information				
Information relating to the education or the medical, financial, criminal or employment history				
Any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment				
Personal opinions, views or preferences				
Correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence				
Other				



14.1 If other, please specify:

15. To what extent do you believe the following information can be used in an attack against you. Please tick the relevant option.

	Highly possible	Possible	Fairly possible	Impossible
Biographical information				
Information relating to the education or the medical, financial, criminal or employment history				
Any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment				
Personal opinions, views or preferences				
Correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence				
Other				

15.1 If other, please specify:

16. To what extent do you consider it safe to provide your identification (i.e. username) and authentication (i.e. password) via telephone?

Very safe	1	Safe	2
Uncertain	3	Fairly safe	4
Not safe at all	5		



17. To what extent do you consider it safe to provide your identification (i.e. username) and authentication (i.e. password) via e-mail?

Very safe	1	Safe	2
Uncertain	3	Fairly safe	4
Not safe at all	5		

18. To what extent do you consider it safe to provide your identification (i.e. username) and authentication (i.e. password) when dealing with a person unknown to you?

Very safe	1	Safe	2
Uncertain	3	Fairly safe	4
Not safe at all	5		

19. Do you make use of an e-mail signature?

Yes	1
No	2
Unsure	3

20. How do you get rid of personal and sensitive information, physically and electronically?

SECTION E: ACCESS CONTROL

21. Indicate which technological devices you use are protected by passwords?

Mobile phone	1	Tablet	2
Personal computer	3	Laptop	4

22. To what extent are your passwords the same?

All of my passwords are the same	1	Most of my passwords are the same	2
My passwords differ somewhat	3	All of my passwords differ	4



23. How often do you change your password?

Only when prompted	1	Often	2
Not often	3	Never	4

24. How often do you allow websites to remember your username and password?

Only when prompted	1	Often	2
Not often	3	Never	4

25. How often do you keep your social networking applications logged in?

All the time	1	Most times	2
Seldom	3	Never, I always log out	4
Not applicable	5		

26. Where do you store your passwords?

27. Does anyone else have access to your passwords?

Yes	1
No	2

27.1 If yes, who has access to your passwords?

SECTION F: SOCIAL ENGINEERING

28. Do you know what social engineering is?



Yes	1
No	2

28.1 If yes, please explain what it is.

29. How aware are you of social engineering threats?

Very aware	1	Somewhat aware	2
Somewhat unaware	3	Not aware at all	4

30. Have you ever been exposed to a social engineering attack?

Yes	1
No	2
Unsure	3

If yes, please answer questions 31 - 35. If no, please review questions 31-35 and if it is still not applicable skip to question 36.



31. Please indicate if you have been exposed to any of the below statements. Please circle the relevant option(s).

I have received a fake email, chat, SMS or website link designed to impersonate real systems with the goal of capturing my personal information.	1
I have received a false warning in the form of an e-mail, chat, SMS or website link claiming to come from a legitimate source.	2
My computer system has been infected by malicious software through the input of an infected device which did not belong to me.	3
I have received an e-mail which had attachments that include malicious code (viruses, trojans, or worms) inside of the attachment.	4
I have clicked on pop-up windows that advertise special offers which installed malicious software onto my computer.	5
I have received spam communication which I am unable to stop from receiving.	6
Other	7

31.1 If other, please specify:

31.2 If any of the above statements are applicable to you, please explain the incident(s) in detail:



This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and extend across the width of the page. There are no margins, text, or other markings on the paper.

Financial gain	1	Access to sensitive information	2
Competitive advantage	3	Revenge	4
Entertainment	5	Unsure	6
Other	7		

Less than 5 times	1	Less than 10 times	2
Less than 20 times	3	More than 20 times	4



35. Have you ever reported a social engineering attack?

Yes	1
No	2

35.1 If yes, please provide details:

35.2 If no, why not?

36. How important is information security to your personal well-being?

Very important	1	Important	2
Not important	3	Not at all important	4
Unsure	5		

SECTION G: LEGISLATION RELATED TO INFORMATION SECURITY

37. Do you know of any South African legislation relating to Information Security and social engineering?

Yes	1
No	2
Uncertain	3

If yes, please answer questions 37.1 to 37.3. If no, skip to question 38.



37.1 To what extent are you familiar with the Protection of Personal Information Act 4 of 2013?

Very familiar	1	Familiar	2
Somewhat familiar	3	Not familiar at all	4

37.2 To what extent are you familiar with the Electronic Communications and Transactions Act 25 of 2002?

Very familiar	1	Familiar	2
Somewhat familiar	3	Not familiar at all	4

37.3 To what extent are you familiar with the Cybercrime and Cybersecurity Bill?

Very familiar	1	Familiar	2
Somewhat familiar	3	Not familiar at all	4

38. How did answering this questionnaire impact on your own information security awareness?

END OF QUESTIONNAIRE - THANK YOU FOR YOUR PARTICIPATION



University of South Africa
 Pretorius Street, Muckleneuk Ridge, City of Tshwane
 PO Box 392 UNISA 0003 South Africa
 Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

ANNEXURE J: Certificate of editing

Declaration of editing

Lanie van Kradenburg

BA(HED) Dip Translation Studies (Unisa)

lanievk@hotmail.com

0825591307

<http://lanievk.wix.com/lanievankradenburg>

Title of edited text:

The human element in information security: An analysis of social engineering attacks in the greater Tshwane area of Gauteng, South Africa

Date of editing: 13 October 2016

My editing service includes language editing and proofreading of the entire text, control of the table of contents, uniformity of layout, numbering and font, control of cross references and a comprehensive auditing of text references and bibliographic detail. I also bring to your attention any aspects of the language, academic style, content, contradictions or sentence construction that I wish to inquire about.

Notes to the author:

- Changes and recommendations have been inserted by means of track changes.
- For dissertations and theses please also refer to my editing report.
- It is the responsibility of the author to ensure that all my recommendations are considered and either accepted or rejected to clear the track changes.
- If you wish to resubmit to me for editing after the corrections have been done, there will be an extra charge of R300/hour.
- Please ensure that the page numbers line up with the table of contents on the final draft before submitting.

My best wishes for the successful completion of your project.

Lanie van Kradenburg