INVESTIGATION TOWARDS THE PREVENTION OF CABLE THEFT FROM ESKOM

REMONE GOVENDER

2017

INVESTIGATION TOWARDS THE PREVENTION OF CABLE THEFT FROM ESKOM

BY

REMONE GOVENDER

A thesis submitted for the degree of Doctor of Philosophy (DPhil)

in Criminology in the Department of Criminal Justice

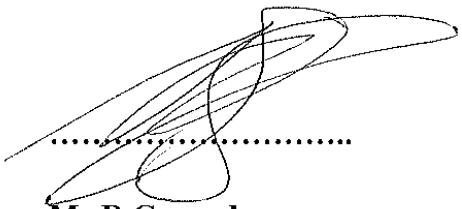
at the University of Zululand

SUPERVISOR / PROMOTER: PROF. DR. JOHANNES MARTHINUS RAS

2017

DECLARATION

I declare that the thesis: "Investigation towards prevention of cable theft from Eskom" is my own work, both in conception and in execution. As far as possible and where applicable, I have acknowledged all my sources by means of complete references.



Mr R Govender

ACKNOWLEDGEMENTS

This study is dedicated to:

My wife, Amanda, daughter, Simone, and sons, Ryan and Ethan, for their never-ending love, support, patience, and for them always being there for me during difficult times.

My sincere thanks and appreciation go to the following:

- God almighty for guiding me along his planned path (John 15:5 – "I am the vine, you are the branches: He that abides in me and I in him, the same brings forth much fruit: For without me you can do nothing".)
- My promoter, Prof. Johan Ras, for his devoted guidance and support in this study. His experience, knowledge and insight into this topic made it possible for me to complete this thesis.
- Eskom, for funding this project and affording me the opportunity to develop in knowledge and experience through this research.
- A special word of thanks go to my friends, Mr Devan (Speedy) Moodley, Mr Colin Meek and Mr Imraan (Immo), for the constant motivation, assistance and support throughout the study. It is truly appreciated.
- To all other persons – too many to name individually – I would like to express my thanks to each and every one of you for your assistance and support throughout the research process.

Abstract

Cable theft could be currently considered as a significant problem, globally. The Eskom statistical figures indicate that cable theft creates a massive problem for service delivery and places a vast amount of pressure on its financial resources. Cable theft is highlighted on various different platforms within Eskom's business operating units and while efforts for increased security and protection measures are in place, these measures appear to be inadequate to prevent it.

This study investigated the extent of cable theft at Eskom and examined what actions Eskom and private security personnel should undertake to prevent it. This study further determined what action steps need be taken by Eskom's internal security management team, and those responsible for the capturing of all relevant information related to it, in order to prevent any form of cable theft.

This research has made four key contributions to the subject: (i) A new Eskom security structure was proposed, (ii) a newly designed Eskom training curriculum framework was designed for all private security personnel working at Eskom facilities, (iii) proposed changes to Eskom's CURA system were made, and (iv) proposed changes were suggested for Eskom's internal ENECC cable theft reporting system.

LIST OF ABBREVIATIONS

BAC – Business Against Crime

CPED – Crime Prevention Through Environmental Design

DX – Eskom Distribution

EAL - Eskom Academy of Learning

ENECC – Eskom Network Equipment Crime Committee

GX – Eskom Generation

HOS – Head of Security

HV – High Voltage

NEC - New Engineering Contract

NKP – National Key Point

NPA – National Prosecuting Authority

PSIRA – Private Security Industry Regulatory Authority

PPE – Personal Protective Equipment

SADC - Southern African Development Community

SANDF – South African National Defence Force

SAPS – South African Police Service

TSC – Term Service Contract

TX – Eskom Transmission

Table of Contents

DECLARATION **2-ii**

ACKNOWLEDGEMENTS **2-iii**

Abstract **2-iv**

Table of Contents **2-vi**

Table of Contents of Annexures **2-xix**

List of Figures **2-xxiii**

List of Tables **2-xxiv**

CHAPTER ONE GENERAL ORIENTATION **1**

1.1 INTRODUCTION 1

1.2 BACKGROUND REMARKS ON ESKOM 2

1.3 THE DANGERS OF CABLE THEFT 3

1.4 THE ROLE OF SECURITY IN ESKOM 4

1.5 SOME PROBLEMS OF CABLE THEFT OCCURRING AT ESKOM 5

1.6 RATIONALE/REASON FOR THIS STUDY 10

1.7 RESEARCH HYPOTHESES 11

1.7.1 First Hypothesis 11

1.7.2 Second Hypothesis 11

1.8 RESEARCH AIMS 11

1.9 RESEARCH OBJECTIVES 12

1.10 BASIC RESEARCH APPROACH 12

1.11 RESEARCH METHODS AND TECHNIQUES 13

1.12 BRIEF REMARKS ON CABLE THEFT IN VARIOUS COUNTRIES 14

1.12.1 The Extent of Cable Theft in Africa 15

1.12.2 The Extent of Cable Theft in South Africa 18
1.12.3 The Extent of Cable Theft in Asia 22
1.12.4 The Extent of Cable Theft in Europe 25
1.12.5 The Extent of Cable Theft in the Americas 31
1.12.6 The Extent of Cable Theft in Australasia 33
1.13 FACTORS CONTRIBUTING TO CABLE THEFT 35
1.14 DEFINITIONS 37
1.15 STRUCTURE OF THE THESIS 40
1.16 SUMMARY 41
CHAPTER TWO RESEARCH METHODOLOGY 42
2.1 INTRODUCTION 42
2.2 THE REASON FOR THE PRESENT RESEARCH 42
2.3 RESEARCH APPROACH THAT IS USED IN THIS STUDY 43
2.3.1 Action Research 43
2.4 THE REASONS FOR USING QUALITATIVE APPROACH IN THIS STUDY 45
2.5 THE PRAGMATIC RESEARCH APPROACH 45
2.6 RESEARCH DESIGN 47
2.7 DATA COLLECTION TECHNIQUES 47
2.7.1 Personal interviews 48
2.7.2 Personal Conversations 49
2.7.3 Telephone interviews 50
2.7.4 Group interviews 51
2.7.5 Document analysis 51
2.7.5.1 Literature review 54
2.7.5.2 Photographs 54
2.7.5.3 Field visits to Eskom facilities 55

2.7.6 Observations 55
2.7.7 The use of tropes 56
2.8 POPULATION AND SAMPLING 57
2.8.1 Participants of the Study 58
2.8.3 Gaining access to the participants 59
2.8.4 Sampling Method 59
2.9 DATA ANALYSIS AND PRESENTATION 60
2.9.1 Coding and categorising the data for the interviews 60
2.9.2 Identifying themes and emerging explanations 61
2.9.3 Presenting the data 61
2.9.4 Observations, documents and personal conversations 62
2.11 THE DANGER OF BECOMING A 'FIELD WORK JUNKIE' 62
2.12 PERSONAL INVOLVEMENT IN THE RESEARCH 62
2.13 RESEARCH DELIMITATION 66
2.14 VALUE OF THE RESEARCH 67
2.15 VALIDITY 67
2.15.1 Content validity 68
2.15.2 Face validity 68
2.15.3 Construct validity 68
2.16 RELIABILITY 68
2.17 ETHICAL CONSIDERATIONS 69
2.18 SUMMARY 70
CHAPTER THREE THE EXTENT OF CABLE THEFT AT ESKOM 71
3.1 INTRODUCTION 71
3.2 WHY IS ESKOM COPPER CABLES PREFERRED TO ALUMINIUM CABLES? 72

3.3 SOME OF THE REASONS WHY CABLE THEFT HAS INCREASED AT ESKOM? 73
3.3.1 High price of copper 73
3.3.2 Eskom's unsecured asset on its open network 74
3.3.3 The difficulty to identify Eskom copper cables after it has been stolen 75
3.3.4 Lack of commitment and dedication by private security officers deployed to Eskom premises 76
3.3.5 Lack of adequate security measures at Eskom facilities 76
3.3.6 Poor control for stock (cable) movements and unused materials on construction / project sites 77
3.3.7 Socio-Economic Factors (Unemployment and Poverty) 78
3.3.8 Criminals are brazen in their attacks on Eskom 79
3.3.9 The involvement of the private security industry and law enforcement personnel in cable theft 80
3.4 ESKOM'S FINANCIAL LOSSES EXPERIENCED DUE TO CABLE THEFT ..81
3.5 THE ECONOMIC SABOTAGE CAUSED BY CABLE THEFT 83
3.6 THE HIDDEN COSTS OF CABLE THEFT 85
3.6.1 The hidden costs of cable theft to Eskom 85
3.6.2 The hidden costs of cable theft to the cities of Durban, Cape Town and Transnet 86
3.7 THE ROLE SCRAP DEALERS PLAY IN PROMOTING CABLE THEFT 87
3.8 ESKOM'S PARTNERSHIPS IN THE PREVENTION OF CABLE THEFT 88
3.9 SPECIFIC RESPONSES BY ESKOM TO REDUCE COPPER THEFT 90
3.10 SUMMARY 91
CHAPTER FOUR ESKOM'S IN HOUSE SECURITY AND CABLE THEFT 93
4.1 INTRODUCTION 93
4.2 THE MEANING OF THE TERM 'IN-HOUSE SECURITY' AT ESKOM 93

4.3 ESKOM'S MINIMUM PSIRA AND LEGAL REQUIREMENTS FOR THEIR IN-HOUSE SECURITY OFFICERS 94
4.4 THE ORIGIN OF ESKOM'S IN-HOUSE SECURITY 95
4.4.1 Eskom security dogs 95
4.4.2 Eskom security training 96
4.4.3 Integration of the National Key Points Act and training into Eskom 96
4.4.4 Eskom's first incident of sabotage 97
4.5 WHERE DOES ESKOM HAVE ITS IN-HOUSE SECURITY DEPLOYED? 97
4.5.1 Generation division: Eskom power stations 98
4.5.2 Generation Division: Eskom peaking stations 100
4.5.3 Generation Division: Eskom Koeberg Nuclear Station 100
4.5.4 Generation Division: Komati water facility 100
4.5.5 Transmission Division: 101
4.5.6 Distribution Division: 101
4.6 WHAT IS THE DIFFERENCE BETWEEN ESKOM'S IN-HOUSE SECURITY AND PRIVATE SECURITY INDUSTRY GUARDS? 101
4.6.1 Appointment processes to employ new security officers for its in-house division 101
4.6.2 Salary and benefits offered to newly appointed in-house security officers 102
4.6.3 Alternate job opportunities for security personnel 102
4.7 ESKOM'S IN-HOUSE SECURITY RESOURCES 103
4.7.1 Eskom security manager 103
4.7.2 Eskom supervisory staff 103
4.7.3 Vehicles 103
4.7.4 Firearms 104
4.7.5 Personal Protective Equipment (PPE) 104

4.8 HOW EFFECTIVE IS ESKOM IN-HOUSE SECURITY IN PREVENTING CABLE THEFT? 104

4.9 ESKOM'S NEW PROJECTS AND ITS IMPACT ON IN-HOUSE SECURITY DEPLOYMENT 105

4.9.1 Medupi Power Plant and its current security challenges 105

4.9.2 Kusile Power Station 106

4.9.3 Ingula Pump Storage 106

4.10 EQUESTRIAN ASSESSMENT 107

4.11 SUMMARY 107

CHAPTER FIVE PRIVATE SECURITY IN ESKOM AND CABLE THEFT 109

5.1 INTRODUCTION 109

5.2 THE MEANING OF THE TERM 'PRIVATE SECURITY' IN ESKOM 109

5.3 BRIEF REMARKS ABOUT THE PRIVATE SECURITY INDUSTRY IN SOUTH AFRICA 110

5.4 ORGANOGRAM OF ESKOM'S REGIONAL SECURITY STRUCTURES FOR TRANSMISSION (TX) AND DISTRIBUTION (DX) 111

5.5 ORGANOGRAM OF ESKOM SECURITY STRUCTURES FOR GENERATION (GX) 113

5.6 ROLE PLAYERS AND THEIR DUTIES TO REPORT CABLE THEFT 113

5.6.1 Role players duties when cable theft incidents occur 115

5.7 THE BASIC REQUIREMENTS FOR SECURITY COMPANIES THAT WISH TO RENDER A SERVICE TO ESKOM 115

5.8 WHY DO THE PRIVATE SECURITY GUARDS (PSG) NOT PREVENT CABLE THEFT AT ESKOM? 116

5.8.1 Security guards are not adequately trained to protect Eskom facilities and identify Eskom's cables 117

5.8.2 Lack of proper observation and reporting skills 119

5.8.3 Security officers are distracted by their mobile phones while on duty 121

5.8.4 Security officers sleep on duty (from 23h00 to 03h00) 122
5.8.5 Effective and dependable security patrols are not conducted consistently during the shifts (mostly at night) 123
5.8.6 Inadequate protection for security officers causes them to feel unsafe and not committed to their jobs 125
5.8.7 Vetting is not done consistently before deployment to Eskom 126
5.9 PSG PIE SUMMARY CHART 127
5.9.1 Explanation of the pie chart 128
5.10 WHY DO THE SUPERVISORS NOT PREVENT CABLE THEFT AT ESKOM? 129
5.10.1 The contract supervisors are ineffective, unprofessional and unreliable 129
5.10.2 Relationship problems between supervisors and security guards 130
5.10.3 Vetting is not done consistently before supervisors are deployed to supervise Eskom contracts 131
5.10.4 Supervisors should do first line investigations only 132
5.10.5 Insufficient support structures for supervisors to remain committed to their jobs. 133
5.10.6 Supervisors lack the ability to create significant impact on the security officers 134
5.11 PSS PIE CHART SUMMARY 135
5.11.1 Explanation of the pie chart 136
5.12 WHY DO THE PRIVATE SECURITY MANAGERS (PSM) AND COMPANY DIRECTORS/OWNERS NOT PREVENT CABLE THEFT AT ESKOM? 137
5.12.1 The contractual commitment by security managers and company directors/owners of security companies is not shown consistently throughout the contract period 137
5.12.2 All security managers and company owners/directors should be vetted before contracting to Eskom 138

5.12.3 Security managers are not adequately supported by company owners/directors ... 139

5.12.4 Security managers fail to provide clear, honest and definitive leadership roles in their positions ... 140

5.12.5 Security managers are not innovative enough ... 141

5.12.6 Security managers wear many hats during the contractual period ... 142

5.13 PSM AND COMPANY DIRECTORS/OWNERS PIE CHART SUMMARY ... 142

5.13.1 Explanation of the pie chart ... 144

5.14 WHAT ARE THE REAL REASONS WHY SECURITY CONTRACTED TO ESKOM CANNOT PREVENT CABLE THEFT? ... 144

5.14.1 The high turnover of security guards at Eskom facilities ... 144

5.14.2 Eskom lacks a standard training entry requirement for contracted private security employees to work at its facilities ... 145

5.14.3 Eskom's private security contractors should use security patrol dogs at all its high crime facilities ... 147

5.14.4 Eskom's private security contractors must use patrol vehicles at all its high crime facilities ... 148

5.14.5 Eskom's private security managers must manage in line with the security contract agreement ... 148

5.14.6 Improper utilization of security manpower ... 149

5.15 REAL REASONS PIE CHART SUMMARY ... 150

5.15.1 Explanation of the pie graph ... 151

5.16 OTHER GENERAL REMARKS MADE BY THE PARTICIPANTS FOR REDUCING CABLE THEFT ... 152

5.16.1 Security companies must deploy armed response to all facilities and improve its response times to panic alarms ... 153

5.16.2 Private security must reduce the opportunities for criminals to commit crime at Eskom facilities ... 154

5.16.3 Private security companies must target the underlying causes of crime against Eskom 155

5.16.4 Eskom management must improve its housekeeping procedures and lock up unused material 155

5.16.5 Eskom security management must create early warning crime prevention programmes 157

5.17 OTHER GENERAL REMARKS PIE CHART SUMMARIES 157

5.17.1 Explanation of the pie chart 158

5.18 SUMMARY 159

CHAPTER SIX ESKOM'S INTERNAL SECURITY MANAGEMENT TEAM AND THOSE RESPONSIBLE FOR THE CAPTURING OF ALL RELEVANT INFORMATION RELATED TO CABLE THEFT 160

6.1 INTRODUCTION 160

6.2 GROUP SECURITY'S ROLE WITHIN ESKOM'S SUSTAINABILITY DIVISION 160

6.3 ORGANOGRAM OF GROUP SECURITY WITHIN ESKOM'S SUSTAINABILITY SYSTEMS DIVISION 161

6.3.1 Discussion on the Organogram of Group Security within Eskom's Sustainability Systems Division 162

6.4 WHY CAN THE INTERNAL SECURITY MANAGEMENT TEAM NOT STOP CABLE THEFT AT ESKOM? 163

6.4.1 Eskom's security structures are not properly aligned 163

6.4.2 Succession planning policies are not applied consistently in Eskom security divisions 165

6.4.3 Eskom Security managers fail to consider recommendations made by private security companies to improve security measures to reduce losses 167

6.4.4 Disjointed relationships between security managers and in-house security officials (Area officers, sections officers, security officers working for Eskom) 168

6.4.5 Security contracts and oversight ownership are not structured evenly at Eskom 169

6.4.6 Criminals are adequately equipped and more determined 171

6.5 SUMMARY OF ESKOM INTERNAL SECURITY MANAGEMENT (EISM) PIE CHART 172

6.5.1 Explanation of the pie chart 173

6.6 WHAT ARE THE EXACT PROBLEMS WHY THE INTERNAL SECURITY MANAGEMENT TEAM STRUGGLE TO PREVENT CABLE THEFT AT ESKOM? 174

6.6.1 The absence of an accurate crime reporting culture relating to cable theft at Eskom 174

6.6.2 Eskom appoints security companies that fail to establish strategic partnerships and develop crime prevention programmes to prevent cable theft during their contract term 176

6.6.3 Security assessments in Eskom are not conducted meticulously and accurately to prevent repeated crimes 178

6.6.4 The need for Eskom investigators to forge closer relationships with the police investigators and justice department 180

6.6.5 Eskom security officials cannot identify the cable after it is stolen, which increases the problem of cable theft 182

6.6.6 Eskom security must support the use of intelligent security systems to manage private security guards and supervisors 183

6.6.7 Eskom in-house security officials need to work shifts to provide proper oversight management for security providers 184

6.7 PIE CHART SUMMARY OF WHY THE INTERNAL SECURITY MANAGEMENT STUGGLE TO PREVENT CABLE THEFT 185

6.7.1 Explanation of the pie chart 187

6.8 ESKOM'S CURA SYSTEM AND CABLE THEFT 187

6.9 ESKOM'S NETWORK EQUIPMENT CRIME COMMITTEE (ENECC) REPORT: DOES IT PREVENT OR EXACERBATE CABLE THEFT? 189

6.10 WHAT DID SOME OF THE PARTICIPANTS SAY WHEN ASKED THE FOLLOWING RESEARCH QUESTION: *IF THE PRESIDENT OF SOUTH AFRICA INSTRUCTS YOU TO IMMEDIATELY STOP CABLE THEFT AT ESKOM, WHAT WILL YOU DO WITHIN ONE MONTH*? 191

6.11 FURTHER INFORMATION SUPPLIED BY THE PARTICIPANTS RELATED TO CABLE THEFT 192

6.12 SUMMARY 193

CHAPTER SEVEN ACTION STEPS TOWARDS THE PREVENTION OF CABLE THEFT FROM ESKOM 195

7.1 INTRODUCTION 195

7.2 INFLUENCING THE JUDICIAL PROCESS 196

7.3 INFLUENCING LAW ENFORCEMENT AGENCIES 197

7.4 WHAT MUST ESKOM'S INTERNAL SECURITY MANAGEMENT TEAM AND THOSE RESPONSIBLE FOR THE CAPTURING OFF ALL RELEVANT INFORMATION RELATED TO CABLE THEFT DO TO PREVENT IT? 198

7.4.1 Improve relationships between security managers and in-house security officials 198

7.4.2 Eskom's security management must realign its security contracts, form strategic partnerships with private security companies, and develop effective crime prevention programmes to prevent cable theft 199

7.4.3 Security assessments for Eskom facilities must be improved through further training, education, monitoring and accountability 200

7.4.4 Management needs to improve its awareness culture among employees on the issue of cable theft 200

7.4.5 Eskom security personnel must report crime incidents accurately and diligently on the CURA system 201

7.4.6 Cable theft experts are needed to testify in court if criminals are to receive lengthy jail terms 202

7.5 WHAT MUST ESKOM'S INTERNAL SECURITY MANAGEMENT TEAM DEMAND FROM ITS IN-HOUSE SECURITY OFFICIALS 203

7.5.1 Proposed security management structured plan for supervising and managing private security contracts 204

7.5.2 Private security companies must deploy competent and reliable personnel to Eskom facilities 205

7.5.3 In-house security officials must encourage line management to report non-performance issues of private security companies and employees 205

7.6 WHAT MUST ESKOM'S IN-HOUSE SECURITY OFFICIALS DEMAND FROM PRIVATE SECURITY COMPANIES TO PREVENT CABLE THEFT FROM ESKOM 206

7.7 PROPOSED: ESKOM SECURITY STRUCTURE 209

7.8 EXPLANATION OF THE PROPOSED SECURITY STRUCTURE MODEL .. 212

7.8.1 Implementation of the proposed security structure 214

7.9 NEWLY DESIGNED ESKOM TRAINING CURRICULUM FOR ALL PRIVATE SECURITY CONTRACTS AT THE ESKOM FACILITIES 215

7.9.1 Course Content for the Standard Entry Training Curriculum to Qualify and Approve Security Personal Working to Work at the Eskom Facility 217

7.10 IMPROVEMENTS FOR THE CURA SYSTEM 220

7.10.1 NEW INFORMATION TEXT BOXES FOR CURA 222

7.11 IMPROVEMENTS TO THE ENECC REPORT 223

7.12 SUMMARY 224

CHAPTER EIGHT FINDINGS, CONCLUSIONS AND RECOMMENDATIONS ... 225

8.1 INTRODUCTION 225

8.2 GENERAL REMARKS 225

8.3 LIMITATIONS OF THE PRESENT STUDY 225

8.4 FINDINGS 226
8.4.1 Feedback on first hypothesis 226
8.4.2 Feedback on second hypothesis 227
8.5 SUMMARY OF THE FINDINGS 228
8.5.1 Why do the private security guards not prevent cable theft at Eskom? 228
8.5.2 Why the supervisors of the private security guards cannot prevent cable theft at Eskom? 228
8.5.3 Why do the managers and company owners/directors not prevent cable theft at Eskom? 229
8.5.4 The real problems why security contracted out to Eskom cannot prevent cable theft 229
8.5.5 General remarks made by the participants on reducing cable theft 230
8.5.6 Why does the internal security management team not stop theft at Eskom? ... 230
8.5.7 The exact problems why the internal security management team struggle to prevent cable theft 231
8.6 CRITICAL CONCLUSIONS ON SPECIFIC FINDINGS 231
8.7 RECOMMENDATIONS FOR THE STUDY 233
8.8 AREAS FOR FURTHER RESEARCH 235
8.9 SUMMARY 235
8.10 FINAL REMARKS 235

LIST OF REFERENCES 237

Table of Contents of Annexures

ANNEXURE A 263
Annexure A1 263
Annexure A2 263
Annexure A3 264
Annexure A4 264
Annexure A5 265
Annexure A6 266
Annexure A7 267
Annexure A8 268
Annexure A9 268
Annexure A10 269
Annexure A11 269
Annexure A12 270
Annexure A13 270
Annexures A14/A15/A16/A17/A18: EXAMPLES OF POOR HOUSEKEEPING 271
Annexure A15 271
Annexure A16 272
Annexure A17 272
Annexure A18 273
Annexure 19 273
Annexure A20 274
Annexure A21 274
Annexure A22 275
Annexure A23 276
Annexure A24 276

Annexure A25 277
Annexure A26 277
Annexure A27 278
Annexure A28 278
Annexure A29 279
Annexure A30 279
Annexure A31 280
ANNEXURE B FREQUENTLY STOLEN ESKOM MATERIAL 281
TRANSFORMERS 281
Figure A4.1: 11 kV Transformer 281
Figure A4.2: 315 kVA 282
Figure A4.3: Inside of a transformer 283
Figure A4.4: Inside of a transformer 283
OVER HEAD CABLE LINES 284
Figure A4.5: Overhead power lines 284
OVERHEAD LINES / PYLONS 285
Figure A4.6: Collapsed Pylons 286
COPPER AND COVERED CONDUCTOR 287
Figure A4.7: Covered aluminium conductor. 287
Figure A4.8: Copper conductors are used on overhead power lines. 287
REINFORCED CONDUCTOR 288
Figure A4.9: The composition of reinforced aluminium conductor – it is strengthened with strands of steel wire. 288
SUBSTATIONS 289
Figure A4.10: A substation transformer that was vandalised and the copper coils inside stolen. 290
Figure A4.11: Vandalised substation (1) 290

Figure A4.12: Vandalised substation (2) 291
ESKOM SUBSTATION STRUCTURES 291
Figure A4.13: VT (on the left) and CT (on the right) 292
Figure A4.14: Kiosk (on the left) and Voltage Regulator (on the right) 292
Figure A4.15: Mini Sub 293
Figure A4.16: NEC Transformer 293
Figure A4.17: Recloser 294
Figure A4.18: Breaker 294
COPPER EARTHING 295
Figure A4.19: Round Earthing 295
Figure A4.20: Flat earthing 296
AIRDAC AND BUNDLE THEFT 297
Figure A4.21: Various houses being electrified by means of airdac 297
Figure A4.22: Airdac cable (1) 297
Figure A4.23: Airdac cable (2) 297
Figure A4.24: Airdac cable (3) 298
AERIAL BUNDLE 298
Figure A4.25: Aerial bundle (1) 298
Figure A4.26: Aerial bundle (2) 298
Figure A4.27: Aerial bundle (3) 299
TYPES OF CABLE STOLEN 299
6.6kV – 33kV cable single / 3-core 301
Figure A4.28: Single-core copper cable. 302
3-CORE CABLE 302
Figure A4.29: 3-core copper cable 302
4-CORE CABLE 303

Figure A4.30: 4-core copper cable 303
Figure A4.31: 4-core copper cable 303
MULTI-CORE CABLE 304
Figure A4.32: Multi-core copper cable (1) 304
Figure A4.33: Multi-core copper cable (2) 304
EQUIPMENT USED TO STEAL CABLE 305
ANNEXURE C: MAPS 306
Annexure C1: ESKOM network in South Africa 306
Annexure C2: Map of Africa (cf. section 1.10.1) 307
Annexure C3: Map of South Africa (cf. section 1.10.2) 308
Annexure C4: Map of Asia (cf. section 1.10.3) 309
Annexure C5: Map of Europe (cf. section 1.10.4) 310
Annexure C6: Map of the United States of America (USA) (cf. section 1.10.5) 311
Annexure C7: Map of Australasia and New Zealand (cf. section 1.10.6) 312
ANNEXURE D: PSIRA CERTIFICATION 313
ANNEXURE E: NAME IN LIGHTS CERTIFICATE 314
ANNEXURE F: MTECH DEGREE SECURITY MANAGEMENT 315
ANNEXURE G: BTECH DEGREE FORENSIC INVESTIGATION 316
ANNEXURE H: ADVANCED SECURITY MANAGEMENT PROGRAM 317
ANNEXURE I: SAPS SWAT COURSE TRAINING CERTIFICATE 318

ANNEXURE J: INTERVIEW SCHEDULE 319
ANNEXURE K: PERMISSION LETTER 322
ANNEXURE L: CONSENT FORM 323
ANNEXURE M: CONSENT FORM FOCUS GROUP INTERVIEWS 325
ANNEXURE N: OBSERVATION GUIDE 327

List of Figures

Figure 4.1: The map of Eskom power stations in South Africa.....99

Figure 5.1: An organogram of the security structure for the Eskom Transmission and Distribution business units in the various regions 112

Figure 5.2: shows the organogram of the security structure for the Generation (GX) business unit 113

Figure 5.3: Pie Chart indicating the percentage of participants (55) that agree with the reasons for why the private security guards cannot prevent cable theft at Eskom 128

Figure 5.4: Pie Chart indicating the percentage of participants (55) that agree with the reasons for why the supervisors cannot prevent cable theft at Eskom.....136

Figure 5.5: Pie Chart indicating the percentage of participants (55) that the reasons why the Private Security Managers (PSM) and security company directors/owners do not prevent cable theft at Eskom.....143

Figure 5.6: Pie Chart indicating the percentage of participants (55) that agree with the real problems why private security contracted to Eskom cannot prevent cable theft 151

Figure 5.7: Pie Chart indicating the general remarks made by participants (55) on reducing cable theft.....158

Figure 6.1: Organogram of Group Security within Eskom's Sustainability Systems Division 162

Figure 6.2: security managers reporting structure for Eskom's business units 164

Figure 6.3: Pie Chart indicating the percentage of participants (55) that agreed with the reasons why Eskom internal security management team seemingly cannot stop cable theft.....173

Figure 6.4: Pie Chart indicating the percentage of participants (55) that agreed with what the exact problems are as to why the internal security management team struggle to prevent cable theft at Eskom.....186

Figure 7.1: Proposed security structure model 212

List of Tables

Table 2-1: Participants in the study 58

Table 4-1: Eskom Power Stations.....97

Table 4-2: Eskom peaking stations 100

Table 5-1: Route map for reporting cable theft at Eskom 115

Table 5-2: Security guards are not adequately skilled and trained to protect Eskom facilities and identify Eskom's cables 119

Table 5-3: Lack of proper observation and reporting skills.....120

Table 5-5: Security officers are distracted by their mobile phones while on duty 122

Table 5-6: Security officers sleep on duty (from 23:30 to 04:00) 123

Table 5-7: Effective and dependable security patrols are not conducted consistently during the shifts (mainly at night) 125

Table 5-8: Inadequate protection for security officers to feel safe and committed to their jobs 126

Table 5-9: Vetting is not done consistently before deployment to Eskom 127

Table 5-10: The contract supervisors are ineffective, unprofessional and unreliable 130

Table 5-11: Relationship problems between supervisors and security guards 131

Table 5-12: Vetting is not done consistently before supervisors are deployed to supervise Eskom contracts 132

Table 5-13: Supervisors should do first line investigations only.....133

Table 5-14: Inadequate support structures for supervisors to remain committed to their jobs 134

Table 5-15: Supervisors lack the ability to make a significant impact on the security officers 135

Table 5-16: The contractual commitment by security managers and company directors/owners is not shown consistently throughout the contract period 138

Table 5-17: All security managers and company owners/directors should be vetted before contracting to Eskom 139

Table 5-18: Security managers are not well supported by company owners/directors 140

Table 5-19: Security managers fail to provide clear, honest and definitive leadership roles in their positions 141

Table 5-20: Security managers are not innovative enough 141

Table 5-21: Security managers wear many hats during the contractual period 142

Table 5-22: The high turnover rate of security guards at Eskom facilities is a problem 145

Table 5-23: Eskom lacks a standard training entry requirement for private security employees to work at its facilities 146

Table 5-24: Eskom's private security contractors should use security patrol dogs at all its high crime facilities 147

Table 5-25: Eskom's private security contractors must use patrol vehicles at all its high crime facilities 148

Table 5-26: Eskom's private security managers must manage in line with the security contract agreement 149

Table 5-27: Improper utilisation of security manpower 150

Table 5-28: Security companies must deploy armed response to all facilities and improve its response times to panic alarms 153

Table 5-29: Private security must reduce the opportunities for criminals to commit crime at Eskom facilities 154

Table 5-30: Private security companies must target the underlying causes of crime from Eskom 155

Table 5-31: Eskom management must improve its housekeeping procedures and lock up unused material 156

Table 5-32: Eskom security management must create early crime prevention programmes 157

Table 6-1: Eskom's security structures are not properly aligned 165

Table 6-2: Succession planning policies are not applied consistently in Eskom security divisions 166

Table 6-3: Eskom Security managers fail to consider recommendations made by private security companies to improve security measures to reduce losses 167

Table 6-4: Disjointed relationships between security managers and in-house security officials 169

Table 6-5: Security contracts and oversight ownership are not structured evenly at Eskom 170

Table 6-6: Criminals are adequately equipped and more determined 171

Table 6-7: The absence of an accurate crime reporting culture relating to cable theft at Eskom 176

Table 6-8: Eskom appoints security companies that fail to establish strategic partnerships and develop crime prevention programmes to prevent cable theft 177

Table 6-9: Security assessments in Eskom are not conducted meticulously and accurately so as to prevent repeated crimes 179

Table 6-10: The need for Eskom investigators to forge closer relationships with the police investigators and justice department 181

Table 6-11: Eskom security officials cannot identify the cable after it is stolen, which increases the problem of cable theft.....182

Table 6-12: Eskom security must support the use of intelligent security systems to manage private security guards and supervisors 183

Table 6-13: Eskom in-house security officials need to work shifts to provide proper oversight management for security contractors 184

Table 7-1: Improvements required from the private security companies for security guards 207

Table 7-2: Improvements required from the private security companies for supervisors 207

Table 7-3: Improvements required from the private security companies for managers and the overall private security management team.....208

CHAPTER ONE
GENERAL ORIENTATION

1.1 INTRODUCTION

This study is based on an investigation of ways in which cable theft can be prevented from Eskom. This entailed the researcher examining the present state of affairs relating to cable theft at Eskom and what could be done to prevent it; more specifically, he examined the question of why contracted private security officials (Cf. 5.8 – 5.14) and Eskom security personnel (Cf. 6.4 – 6.6) are seemingly unable to prevent cable theft at Eskom. In other words, it was a systematic study of "*investigation*[1]" to ascertain why private security officers are struggling to prevent the theft, and more importantly, to see what can be done in a practical manner to prevent it. The investigation was also not dealing with the evaluation of the present security measures at Eskom. Criminology represents a social science study about crime, and while this research moved within the field of criminology, it primarily surveyed the cable theft issue at Eskom from a private security point of view (Berk, Campbell, Klap, & Western, 1992; Cullen, 2011; McNeeley & Warner, 2015). McNeeley and Warner (2015:582) say that criminology-based research is meant to test general theories or evaluate interventions and initiatives. The present research was not concerned with philosophical issues in science and research, or about the theories and various kinds of reasoning about research methods or statistical empiricism, but it rather took a practical, pragmatic approach to security (Ras, 2006; Ras 2010; Ras 2012a, 2012b). Russel (2013:1) says that one of the reasons for the slow and uncertain translation of research into practice is that emphasis in science is placed on explanatory models and efficacy designs, rather than on more pragmatic approaches.

Jabareen (2009: 58) says that conceptual framework analysis has its limitations, such as the fact that different researchers may have different conceptions of the same phenomenon and may create different "planes" and conceptual frameworks, and possible difficulties finding

1 The word "investigate" comes from the Latin term "*Investigare"*. The word *"Investigare"* means to track. The Concise Oxford Dictionary (1991:624) explains the word investigate *"as inquire into examine, or to study carefully*". It also says to make a systematic enquiry or search.

suitable texts and data. However, it does offer some important advantages which include *Flexibility*, meaning that it is based on flexible conceptual terms rather than rigid theoretical variables and causal relations; *Capacity for modification*, meaning that conceptual frameworks can be reconceptualised and modified according to the evolution of the phenomenon in question, or as a result of new data and texts that were not available at the time the framework was first developed, which is consistent with the basic premise that social phenomena are evolutionary and not static; and lastly, *Understanding*, which means that conceptual frameworks aim to help us understand phenomena rather than to predict them (Jabareen, 2009:58).

1.2 BACKGROUND REMARKS ON ESKOM

Security at Eskom forms part of an important and valuable component to protect Eskom's assets. Cable (copper) theft has become an increasingly common crime in recent years, but the lack of data has limited research into this growing problem (Pretorius, 2012). The copper theft from Eskom happens both during construction stages and when the sites are operational (Nkabinde, 2014; Ogle, 2014; Booysen, 2014).

Direct jobs are provided within the Eskom Group to close to 41 800 people. This makes Eskom one of South Africa's top 20 employers (Eskom Factsheet, 2014). Eskom is also indirectly responsible for an estimated 32 000 jobs at coal mining companies, such as Anglo American subsidiaries, Exxaro and BHP Billiton (Eskom Factsheet, 2014). In total, more than 129 000 people in South Africa are employed (formally) within the Eskom sector (Eskom Factsheet, 2014).

The security guarding contracts in Eskom are not based solely on the number of Eskom employees or indirect employees, but also on the needs for safeguarding of all Eskom's assets, which includes equipment, material and buildings.

Although Eskom also uses aluminium cables in its operations, it is Eskom's copper cables which are mostly targeted by thieves. The frequency of the copper thefts appears to follow the price of copper in the scrap metal trade, which naturally follows the market price of copper (Horn, 2012). With the demand for scrap copper and the copper prices remaining relatively higher than those of other materials, such as other scrap metal and aluminium, it is envisaged that cable theft will continue to rise in the coming years.

When referring to ‘copper theft’ in this study, it predominantly implies ‘copper cable theft’. Copper cables constitutes more than 90 % of all copper thefts, with the remainder consisting of copper items used in direct support of the copper cable network, for example earth mats from High Voltage (HV) yards at Eskom substations and buzz bars from transformers.

An issue of concern that needs to be addressed in this study is the extent of cable theft at Eskom (Cf. Chapter Three) and to ascertain what Eskom and private security contractors must do to prevent cable theft (Cf. Chapters Four to Six). The study further determined what action steps must be taken by Eskom’s internal security management team and those responsible for the capturing of all relevant information related to cable theft (Cf. Chapters Six to Seven).

This chapter reviews some of the literature on cable theft and its impact on the global economy, as well as the damaging economic effects on South Africa. There is significant evidence that shows that the escalation of cable theft and vandalism in South Africa’s major cities, and its harmful effects on the social fabric and financial base of the electricity generation and distribution utilities, as well as a lack of effective public interventions for addressing these challenges, are all widely documented in literature (Pretorius, 2012; Solomon, 2013; Dzansi, Rambe & Mathe, 2014).

1.3 THE DANGERS OF CABLE THEFT

Cable theft has been blamed for several deaths due to electric shocks and burns arising from illegal tampering with electricity (Peters, 2014; Dzansi *et al.,* 2014). The increase in the price of copper (experienced in the past decade) has made this type of crime more attractive to criminals, but the activities involved in copper theft can injure or kill those stealing the copper and also endanger the lives of the public (Cf. Annexure A2). Copper theft is a problem for most power utilities worldwide, and Eskom is no exception (Sidebottom *et al.,* 2014).

Pretorius (2012) pointed out that not only has theft increased, but the criminals are becoming increasingly bold in their actions and taking greater risks to get the valuable metal. Copper theft means more than just lost revenue for Eskom. It affects everyone in South Africa, whether they realise it or not. Power outages caused by cable theft not only inconvenience consumers, but can also affect the viability of business, in some instances leading to job losses and businesses closing down.

1.4 THE ROLE OF SECURITY IN ESKOM

It is important to note the diverse make-up of the security set-up within Eskom. Although there is a theoretical distinction between Eskom's in-house security and its contracted private security providers, in other words between security officers working for Eskom on a full-time basis and other private security contractors, they are all private security officials in terms of the law governing private security services.

Contract security companies offer a wide array of services to Eskom. These include providing static security officers; providing security technologies, such as surveillance systems and access control systems; being responsible for conducting investigations in areas where Eskom does not have capacity; and acting as a liaison between Eskom and state law enforcement during the investigation process of the cases that Eskom has tasked them with. While Berg and Nouveau (2011) have said that in the past a company's in-house security would have been responsible for internal investigations, companies like Eskom, for example, now contract private security providers to do some of the investigations for them.

Eskom's in-house security measures (see sections 4.2, 4.3, 4.6, 4.7, 4.8 & 4.9) consists of security personal and equipment used by Eskom security management to protect Eskom's interests. Eskom's internal security divisions (see sections 4.5 – Generation, Transmission, and Distribution) work independently from each other. These divisions have their own security structures and report to non-security regional structures. Group Security (the national body responsible for security within Eskom) has its own internal employees that are referred to as business partners, who are assigned to the Eskom regional security divisions to provide guidance on legislative and regulatory compliance (Private Security Industry Regulatory Authority Act No. 56 of 2011, Firearm Control Act No. 60 of 2000, PSIRA levies Act No 23 of 2003, National Key Point Act No. 102 of 1980, etc.).

Eskom's generation power stations (see section 4.5.1), which are all National Key Point (NKP) sites, only make use of Eskom's in-house security officers. Former Eskom CEO, Brian Dames, said in 2013 that all NKP sites must deploy only Eskom security officials to NKP sites and not outsource the NKP sites to other private security companies. Eskom is currently in the change phase to implement this recommendation. The current situation is that Eskom does have private security officials working at non-generation NKP sites at this stage, but as mentioned, is substituting the private contract guards with Eskom's own in-house

security members at some Eskom facilities. Eskom uses a hybrid system, where in-house security officers work together with the private security employees.

This study has explored the role of security at Eskom (both in-house and private security) to ascertain why security cannot prevent cable theft from Eskom's facilities (Cf. Chapters 4 & 5).

1.5 SOME PROBLEMS OF CABLE THEFT OCCURRING AT ESKOM

Some of the currently occurring problems of cable theft have to do with, inter alia, the following matters – the vast area, unplanned interruptions, the high prices paid for copper, private security not doing their work, and the lack of intelligence gathering regarding copper theft, vetting, Eskom's ENECC reports, as well as the lack of proper reporting.

Vast Area: In a meeting held on the 26 August 2014 in Pretoria, Leon van den Berg[i] explained that copper theft is a major challenge facing the Eskom network that consists of 395 419 km of overhead lines, 11 018 km of underground cable and 351 297 installed transformers (http://www.issafrica.org/events/cable-theft-is-strangling-sas-economy-can-we-escape-the-noose). The researcher extracts the point from the statement by Van den Berg that the Eskom network is too big to manage in an effective manner (Cf. Annexure C1). Eskom operates primarily in South Africa, but it also has two subsidiaries that operate electricity generation concessions in the African countries of Mali, Senegal, Mauritania and Uganda (Eskom directors report, 2014; http://integratedreport.eskom.co.za/financials/fin-dir-report.php).

He (Van den Berg) said that "Eskom has developed a 'network equipment crime strategy' that seeks to promote cooperation across the industry, regional cooperation in Southern African Development Community (SADC) as well as technology solutions…. The strategy targets organised criminal groups and low-level thieves" (http://www.issafrica.org/events/cable-theft-is-strangling-sas-economy-can-we-escape-the-noose). In other words, the area to police to prevent copper theft is so vast that it needs proper crime prevention networks.

Unplanned interruptions: One of the reasons cited in Eskom's Annual Report 2008 for its poor distribution performance was the increase in unplanned interruptions such as theft, and in particular, conductor (cable) theft. According to this report, losses to the entity due to

conductor theft (including copper and cable) during 2008 totalled R25 million (up R9 million in 2007) and these involved 1832 incidents (Hi-Tech Security Solutions, http://www.securitysa.com/article.aspx?pklarticleid=5592).

The high prices paid for copper: According to Etzinger (2008), copper cable theft was an ongoing problem for Eskom. He said that an increase had been noticed which was costing Eskom 25 million rand a year. He attributed the increase in this crime to the high price of copper and the depressed economic situation. Etzinger (2008) indicated they had seen steady increases, from 446 incidents in 2005 to 1 059 in 2007 and 1 914 in 2008[2], and that it was going to increase.

Private security not doing their work: There is currently a problem with the high number of security officers who are PSIRA trained and registered, but do not possess the appropriate quality of standards required by Eskom. Nkabinde (2014) says that the private security officers working at an Eskom facility are doing their work, but not as effectively as they should. He says in some instances cables are stolen while they are on duty and some of the security officers have a negative attitude in the execution of their duties, while in some cases, the guards help themselves to the cables.

Nkabinde (2014) further mentions that incidents, which happen in the field where there are no guard/s deployed, are understandable (as there is nobody monitoring those lines), but where cables are stolen from the premises/yard where security officers are deployed, it is unacceptable. Berg and Nouveau (2011) say, in referring to reputation, that good relations with associates will determine future employment. A private security company has to consistently prove itself and maintain a positive reputation with its clients in order to retain a security contract. This “positive reputation” seems to be lacking in Eskom.

Training: Private security officers must be trained on the safety and security requirements, specifically adapted for working at Eskom facilities, prior to their deployment, and ongoing formal training sessions during their deployment stage must also become a compulsory feature. Security officers must be thoroughly briefed on the value and importance of the Eskom assets that they need to protect. At this stage, it seems that it is not the case. Security officers must be thoroughly briefed on the value and importance of the Eskom assets that they need to protect. At this stage, it seems that it is not the case (Govender, 2014). Providing

[2] This is historical data and not the present figure.

security services is a high-risk occupation; hence, security personnel should undergo intense training programmes to ensure both the security of the organisation and their own survival (Du Preez, 1991:85). According to Berg (2007:23), low training and low recruitment standards impact negatively on the professionalism of the security industry, as well as on accountability.

Security performance: More needs to be done towards creating awareness of the importance of Eskom's security performance in reducing cable theft and preventing losses from Eskom facilities. If Eskom's management team fully understands, through the Eskom Network Equipment Crime Committee (ENECC) reports (see section. 6.9) where cable theft losses are occurring (at Eskom facilities secured by security officers, Unprotected Eskom facilities, and open networks), and all Eskom's security employees are contractually made aware of their role and responsibilities towards ensuring that private security companies are contracted to prevent losses, and not simply to post bodies, then they (private security companies) can be held accountable for failing to prevent cable theft from Eskom and displaying poor contract implementation over their private security employees. The key to any successful security programme designed to improve security performance begins with an experienced management team (Dalton, 1995:260). Security management's responsibility in improving performance is to ensure that the employee has dignity, has pride in his or her uniform and workplace, and shows personal responsibility at work (Sennewald, 2011:52).

Vetting: Abrahamsen and Williams (2005) mention that, given the unevenness of training and standards, concerns are frequently raised about the quality and integrity of security staff, with allegations be raised that guards are in collusion with criminals. While most companies claim that they undertake some form of recruitment vetting, and require potential employees to certify that they have no criminal record, they freely acknowledge that the reliability of this information is highly questionable. Given the strong concerns over collusion between guards and organised criminal activities, vetting and background checks are of vital importance to the reputation of the sector (Abrahamsen & Williams, 2005).

Eskom's ENECC reports: The security culture in Eskom is highly dependent on the knowledge obtained from the crime statistics report [Network Equipment Crime Committee (ENECC)] report (See Section. 6.9) to establish the numbers and nature of crimes experienced within Eskom. Crime statistics may also be used as a standard to monitor and

evaluate the effectiveness of the strategies and actionable crime information products (Garcia, 2008: 5).

The key element here is that the committee which receives this information must be able to support regions where crime is on the increase in Eskom. The report should further provide an immediate scanning of poorly performing security companies which can be useful in determining the potential threat to Eskom assets. The use of an accurate, computerised analysis, and its results, to reduce crime and to increase detection rates and prevent losses is not unique to modern times (Garcia, 2008: 8-9) and is strongly recommended.

This creates an opportunity for management to get to know if the security companies contracted to Eskom are indeed protecting the assets and adhering to their mandate to protect Eskom's cables (and other assets). Nkabinde (2014c) says that the cable theft information must stand out in any report, because of the negative impact it creates in service delivery and the high losses that Eskom suffers. The chances of identifying poorly performing security companies will be immediately noticed and action can be taken immediately by the committee.

If Eskom's management team identify a threat, which includes the security companies contracted to protect Eskom assets that have the potential to adversely affect Eskom, then they can immediately prepare a security plan to manage this problem which includes the immediate termination of contracts to prevent further losses (Garcia, 2008: 6-8).

Lack of proper reporting: CURA[3] is the name of a risk management software program which Eskom investigators utilise to report incidents of cable theft from Eskom facilities (amongst other places of theft) (see section 6.7); however this system does not make provision for independently advising the management of the security companies contracted to prevent cable theft at those facilities (CURA, 2014). This information is clustered on the CURA system (See Section 6.8), hence the focus of the performance of the security companies is not adequately reflected.

More accurate data, in the hands of the right persons, will lead to more effective proactive, predictive, and intelligence-led strategies at Eskom. It is important to note that the extent of cable theft in Eskom will never be completely measured. Only cable theft incidents that have

[3] CURA in this study is not an acronym. It is the name of a risk management software program.

been reported can be measured. Fischer, Halibozeck and Green (2008), although not related to cable theft, say that a culture of security awareness has become a common theme considered by almost every person in the world. This "awareness" is definitely a necessity, if Eskom's cable thefts need to be stopped.

According to Garcia (2008: 15), to understand an organisation, information on many different aspects of the organisation must be obtained and reviewed. This includes obtaining information on the threats, as well as the targets that need to be protected. The required information needs to be defined by management and organised to make it usable. The information on adversaries may include information on their motivation and potential goals, based on targets, tactics, numbers and capabilities.

At present, Eskom's crime statistics only reflect those incidents that have been reported (ENECC, 2016; see section 1.12.2). Chapter Three (The Extent of Cable Theft at Eskom) provides a better understanding of the cable theft crime statistics at Eskom. Understanding how cable theft is reported will help Eskom's security to undertake future estimations of the costs of cable theft, and more importantly, to assist in the evaluation of crime prevention programmes. Information is everywhere and investigators simply need to know what to look for and what questions to ask. It is important to encourage proper workplace investigations in order to acquire proper data and comprehensive and precise feedback reports (Nemeth, 2010: 87).

At Eskom, cable theft information is limited to information collected by security personnel in the regions, and by the level and accuracy of details recorded on the CURA system. The CURA system was designed and is maintained to meet organisational needs and report Eskom crime incidents. The crime statistics, based on cable theft incidents, may therefore fall short in providing an accurate and comprehensive picture of the nature and extent of where the cable theft has been occurring at Eskom.

Furthermore, the Eskom statistics may reveal more about the efficiency, or inefficiency, of Eskom's security personnel in recording the reports of crimes of cable theft, rather than reflecting any real change in crime levels. At present, Eskom's ENECC reports, recorded via its CURA system, are used to produce annual national crime statistics at Eskom and, as a result, such crime data which is available is not sufficient for Eskom's management team to make informed decisions.

This study, inter alia, has addressed this issue (see sections 7.10–7.11).

1.6 RATIONALE/REASON FOR THIS STUDY

The rationale for this study was to investigate and gather relevant data in order to understand the problem (especially the extent) of copper theft from Eskom facilities in greater detail. This study further investigated the role of private security contracted to Eskom to protect its cables (see section 5.8.1–5.8.7), and the role of Eskom's internal security management team, including its security management system, to oversee private security contractors (see section 6.1–6.10) and to conduct investigations into cable theft incidents. This study also examined what action steps (see section 7.1–7.11) should to be taken by Eskom's contracted private security companies and Eskom's internal security management team towards preventing copper theft from Eskom.

At the beginning of the study, it was found that some of the private security officials employed at some of Eskom's sites were seemingly not able to curb or prevent cable theft. There is no doubt a problem with the work performed by private security at Eskom, and in addition to that, there seems to be a problem with Eskom's security management and Eskom's information management system (ENECC report), which is not thorough enough to pinpoint exactly where thefts take place and what can be done to prevent it.

Private security is not a new idea. Since the beginning of society, security has been part of the protection of mankind against threats from nature, creatures and other humans (Simonsen 1998:1; Minnaar, 2007:132). Persisting risks, such as cable thefts that emanate from the latter category, and the role that private security could play in protecting Eskom assets against criminal onslaughts, have prompted the researcher to undertake this research, with the purpose of acquainting Eskom's top management with the dynamics underlying this potential and formidable source of protection. The expectation of the Eskom Security Management Department is that any security service must be performance driven and deliver a good quality security service to Eskom (Govender, 2014). According to the Private Security Industry Regulation Act, 2001 (Act No. 56 of 2001), a security service provider employing any person in the private security industry must comply with every obligation imposed by the Act, and with other supporting legislation, and generally contained in the whole body of law applicable to this specific industry. Eskom's top management expects all the private security

companies and its in-house security officials to abide strictly with the laws stipulated in the PSIRA Act.

Achumba, Ighomereho and Akpor-Robaro (2013:96) say that security should be seen as being everybody's business. Security, just like other elements in the business environment, enhances and optimises business activities, while the lack of good security hinders these activities and constitutes a threat to business organisations. Tai-hoon and Sakurai (2008:63) believe that security-level management is the activity required to sustain a security level that is defined as being essential by considering the operational environments. Security-level management is not simply the checking of a temporary status in a short time, but the continuous observation of the variable environment.

1.7 RESEARCH HYPOTHESES

Two research hypotheses were formulated for examination in this research.

1.7.1 First Hypothesis

A better comprehension of the extent of cable theft at Eskom will assist us in preventing it.

1.7.2 Second Hypothesis

The present strategies to prevent cable theft are ineffective and need to be revised to prevent it.

1.8 RESEARCH AIMS

Emanating from the above hypotheses, the following research aims were formulated:

1.8.1 To provide a general orientation to the study (Cf. Chapter One)

1.8.2 To discuss the research methodology (Cf. Chapter Two)

1.8.3 To establish the extent of cable theft at Eskom (Cf. Chapter Three)

1.8.4 To discuss Eskom's in-house security and cable theft (Cf. Chapter four)

1.8.5 To discuss private security in Eskom and cable theft (Cf. Chapter Five)

1.8.6 To discuss Eskom's internal security management team and those responsible for the capturing of all relevant information related to cable theft (Cf. Chapter Six)

1.8.7 To present actions steps to prevent cable theft (Cf. Chapter Seven)

1.8.8 To discuss the findings, conclusions and recommendations (Cf. Chapter Eight).

1.9 RESEARCH OBJECTIVES

The following three specific research objectives were formulated:

- To establish why private security contractors seemingly cannot protect Eskom's cables (see sections 5.8 – 5.14).
- To see why Eskom's internal security team seems unable to stop copper theft (see sections 6.4 – 6.7).
- To determine what action steps must be taken by Eskom to ensure that no cable theft occurs (see sections 7.1 – 7.11).

1.10 BASIC RESEARCH APPROACH

The researcher has focused mainly on the qualitative research method to conduct the study. In qualitative research, data is gathered through interaction with people, rather than through numerical analysis of questionnaires (Creswell, 1994: 145). The researcher interacted with participants through semi-structured interviews, telephonic conversations, electronic mails, and personal conversations in order to gather data to obtain facts, opinions and attitudes in relation to this study. Another method used by the researcher was natural and participant observation of security operations by security officers posted at Eskom facilities (Cf. Ras 2006; 2010; Tewksbury, 2009:38).

The study was conducted within a qualitative design approach. A qualitative study, inter alia, allows researchers to examine the places where events occur in their natural settings. In this way, the researcher was able to better comprehend the factors that lead to cable theft at Eskom. Tewksbury (2009:56) says qualitative research is the ballet-like, interpretative dance approach to science. While there are steps to be done, it is more important to produce a smooth, well-connected, emotionally infused product. Qualitative research does not rely on the mechanical precision of steps being performed, but rather focuses on how the overall

product communicates a message and moves people, both emotionally and intellectually (Tewksbury, 2009:56).

In addition, the qualitative research approach seeks to understand a given research problem (in this case, Eskom's cable theft) or topic from the perspectives of the local population it involves. Qualitative research is especially effective in obtaining culturally specific information about the behaviours, modus operandi, and views and opinions, as well as the social contexts of particular populations, of those involved in the prevention of Eskom's cable theft (Ras, 2015a; Bouma & Ling, 2004:165; Dey, 1993:15).

The qualitative research design approach is distinguished from others in terms of the following key features:

- Research is conducted in the natural setting of the social actors;
- The focus is on the process rather than on the outcomes;
- The actor's perspective (the insider) is emphasised;
- The primary aim is to gain an in-depth description and understanding of actions and events;
- The main concern is to understand social action in terms of a specific context rather than attempting to make generalisations as to some theoretical populations;
- The research process is often inductive in its approach; and
- The qualitative researcher is seen as the main instrument in the research process (Babbie & Mouton, 2009: 270–271; Ras, 2015b).

1.11 RESEARCH METHODS AND TECHNIQUES

In this study, the researcher has used various methods to collect data, namely interviews with individuals, personal conversations, telephone interviews, guided conversations with groups of individuals (focus groups), document analysis, and observations of people, places and actions/interactions in order to investigate cable theft at Eskom. This was done not only for purposes of this research, and also because the researcher is part of the security team at

Eskom. He was also involved in action research at times and was also, inter alia, a participant observer.

1.12 BRIEF REMARKS ON CABLE THEFT IN VARIOUS COUNTRIES

In this section, the author has briefly placed cable theft in historical perspective so that the reader can understand that it is a universal social phenomenon.

General remarks on cable theft: Throughout the developed world, stealing valuable metal, and more especially copper cables, has become a serious concern for businesses in functioning efficiently, and at the same time, it poses a difficult problem for law enforcement agencies that must manage and control it. Not only does this problem affect businesses, it also affects the communities at large.

Collaborative efforts to combat copper theft have occurred for several decades. However, reports of increases in copper theft are occurring throughout the world. The primary targets are usually substations, transformers, utility lines and underground cabling. Vandalism and theft of electrical equipment at electrical substations is, at times, not only catastrophic for thieves, but also for the electricity maintenance staff who routinely service these disrupted or unstable power environments (Geldenhuys, 2008; Burger & Lancaster, 2014).

The copper and electricity relationship: Evans (2011) avers that copper theft has always been a problem. Copper is perfect for conducting electricity, so it was ideally suited to support the telegraph boom of the mid-nineteenth century. Evans (2011) also refers to a British government report of 1860 which made it clear that copper's "value to robbers renders it inapplicable for open air lines", so iron wire had to be used instead. However, iron wire has only one-tenth of the conductivity of copper, but its scrap value is much lower than that of copper.

Copper wire was restricted to environments that were especially testing and in which only copper would do. Submarine cables, which had to carry signals across extreme distances under very testing conditions, were of the finest copper because ocean depths offered excellent protection against theft (Evans, 2011).

However, overland telegraph lines, that are basically copper lines, have required special security measures. This was a particular difficulty when lines were extended through parts of the world where the authority of the state was weak, as in the Ottoman Empire, across which

the British were hoping to build a direct telegraph link to India in the mid-nineteenth century. The various ethnic tribes under Ottoman rule were not always friendly towards the authorities in Istanbul (Evans, 2011).

Evans (2011) says that it was certainly the case in what is now Iraq, across which a line was to be strung in the 1860s, linking Baghdad to the Persian Gulf. Early plans to lay a cable along the bed of the Tigris were abandoned as being impractical. The only way in which the wires could be protected was to organise a special security guard force, the Cavus Lar, who would patrol the line on horseback.

The members of Cavus Lar were recruited locally and well paid for their work. The effect, as one historian has noted, was to integrate what had been seen as an alien intrusion (i.e. the British introducing cable lines) into the fabric of local life, while at the same time contributing to the local Ottoman economy (Evans, 2011).

1.12.1 The Extent of Cable Theft in Africa

Countries within the Southern African Development Community (SADC) (Cf. Annexure C2, Map of Africa, which includes the SADC countries) are suffering economically owing to problems associated with copper cable theft. Media platforms in these countries are full of stories of such incidences. Sadly, both rural and urban areas are heavily affected, and this is hindering sustainable social and economic development in the region (Sauti, 2012).

Libya: Libya in North Africa is, for example, a country that is experiencing a copper theft problem. The *Libya Herald* reports that thieves are threatening the country's already overstretched electricity resources by stealing power supply cables. According to Shaban (2013), "This is not the first time this has happened [*sic*]". Shaban (2013) said "… *These people steal the cables and then sell all the copper from them …* [*sic*]*"*. He further said that the Sirte site was the latest area to fall victim to the copper theft crime spree. Local residents had suffered severe power shortages, following a spate of thefts from power stations and pylons around the town.

Shaban (2013) further pointed out that the thieves "sell the stolen copper to neighbouring countries". The theft of cables, as well as maintenance vehicles, has so far cost General Electric Company of Libya (GECOL) millions. He blamed the country's power cuts not only

on the theft of cables, but also the recent strikes at the country's oil fields and export terminals.

Nigeria: According to a report by Adepoju (2013), police officers in Lagos had arrested 17 suspects, including a warehouse manager, at Nigerian Telecommunications Limited (NITEL), for allegedly stealing cables valued at 50 million naira (the Nigerian currency, then amounting to US$318 000), belonging to the country's former telecommunications company (http://www.humanipo.com/news/3316/nitel-warehouse-manager-among-17-arrested-for-cable-theft-in-nigeria/). Adepoju (2013) reported that the ringleader, Safui, had promised one of the police officers at the station two million naira (US$12 700) to assist them in stealing the cables.

Adepoju (2013) also said the police mentioned that the suspects attempted to bribe the police officers on duty with 700 000 naira (US$4 500) to facilitate their release (http://www.humanipo.com/news/3316/nitel-warehouse-manager-among-17-arrested-for-cable-theft-in-nigeria/).

According to a report by Okolie (2013), the Nigerian police attached to the Dolphin Estate Police Station arrested two cable thieves in possession of 117 pieces of cables stolen from a manhole along Kakawa Street in Lagos Island. Okolie (2013) said that the telecommunication manholes along Lagos Island and its surroundings have been severely vandalised by a notorious gang of cable thieves, forcing the new area commander of the police to order a total clampdown on their activities (http://www.vanguardngr.com/2013/04/nitel-cable-theft-i-have-no-regrets-suspect/).

Okolie (2013) further said that the 28-year-old suspect who was arrested with the 117 cables said that he had no regrets over his actions. He said he adopted cable theft as a means of a livelihood when he could not secure a decent job. The suspect said *"... I have no regret for my actions. I have done this for about 10 times and I ventured into it because there was no job... [sic]"* (Okolie, 2013)

The suspect further revealed: "*I am the leader of my own group and I steel cables from several manholes in Lagos State. I started last year and I usually operate in areas where I knew the police do not patrol regularly. The job that gave me out was at Broad Street by Kakawa on Lagos Island, we did that for about two days and when we were about conveying the cables out of the area [sic], the police intercepted us along Osbon-Ikoyi Road. I was*

formally selling the cables at Marine Beach in Ajegunle but I stopped selling it there when Fashola demolished the shanties under the bridge. This time, I wanted to sell to a man called Uche and he said he wanted large quantity that was why we had large numbers [sic]" (Okolie, 2013).

Uganda: According to Masinde (2014), electricity and telephone cable thefts have been rampant in Uganda since the year 2014 began. Power and telephone cables worth sh280 million (Uganda's currency is known as the *Ugandan shilling*) were recovered at Mpoma sub-county in Mukono in an operation aimed at curbing power and telephone cable vandalism. Umeme, Uganda Telecom and the Police conducted the operation. Four tons of dismantled cables were found in tightly guarded and fenced premises (http://www.balancingact-africa.com/news/en/issue-no-332/telecoms/copper-thieves-conti/en).

Kenya: According to Salim (2014), cable vandalism has jeopardised Kenya's ability to communicate and had led to losses amounting to sh500 million a year (Kenya's currency is known as the *Kenyan shilling*). Salim (2014) said, "The continued decapitation of Telkom cables and lines appears to be a well-coordinated effort of sabotage. … These thefts are seriously affecting the country's ability to communicate and heavily impact on the valued infrastructure put in place at the taxpayers' cost around the country and as a result Telkom Kenya is faced with mounting financial pressure from losses accumulated." (Salim, 2014).

Namibia: Namibia recently reported that Telecom Namibia is concerned about the growing incidents of cable theft from, and vandalism of, network infrastructure all over the country. Angula says: "Thieves have opened manholes at different points in the country to cut and steal copper cables". Another author has noted that "Criminals are causing massive damage to Telecom Namibia networks through copper theft and sheer vandalism, resulting in electricity interruption to customers costing the company millions in losses" (Sauti, 2012).

The Namibia Telecoms Report (2012) suggests that Namibia Telecom suffered losses amounting to N$760 000 (Namibian dollars) in 2012 through copper wire vandalism and theft (http://www.balancingact-africa.com/news/en/issue-no-332/telecoms/copperthieves-conti/en). "Cable theft and the consequent interruption of power supply to commerce and industry has led to major negative economic impacts in the form of increased costs and reduced profits" (Angula, 2012).

Zimbabwe: Irrefutably, cable theft has become a thorn in the flesh of most – if not all – countries in the SADC region, as it is costing member states billions of rands. The costs can be even higher, taking into account the disruption of essential services such as health, communication and transport (Sauti, 2012). In Zimbabwe, the Zimbabwe Electricity Transmission and Distribution Company (ZETDC), a subsidiary of power utility ZESA Holdings, recently said in a newspaper article that "… it is grappling with cable theft". ZETDC said that 30 000 kilometres of copper cables, valued nearly US$180 000, had been stolen in the southern region of the country in the first quarter of 2012 (Sauti, 2012).

Mozambique: The media reported in Mozambique's private daily paper *O Pais* that Mozambique's power utility, *Electricidade de Moçambique* (EDM), has lost more than U$323 000 in Manica province over the past nine months due to theft of cables and metallic parts of power pylons, Tomo (2013) said that 50 separate cases of theft and sabotage of power equipment had occurred during the past nine months. He also said the thefts and sabotage of equipment are frustrating the company's plans to expand its services and called on local communities to notify EDM of any damages to its equipment.

According to a Police spokesperson in Manica, Muthisse, the police had arrested five individuals suspected of being part of a network of criminals specialising in the theft of power cables. Muthisse said the five are members of a much larger criminal ring, which extended into neighbouring countries: "We have information that these same goods (the cables and items made from them) were sold in Zimbabwe" (http://en.starafrica.com/news/moz-power-utility-loses-us323000-to-cable-theft-sabotage.html).

1.12.2 The Extent of Cable Theft in South Africa

In the decade 1992–2002, copper and cable theft had escalated to such an extent that losses ran into millions of rand annually. In the financial year 2001/02, Eskom, Telkom and Spoornet alone lost more than R300 million rand as a result of nonferrous metal theft (Horn, 2012).

This sum includes an amount of R80.9 million spent by Transnet on increased security costs in 2011/12. Copper theft had jumped by 26 % in 2013, according to the South African Chamber of Commerce and Industry (News24.Com, 2014

http://www.news24.com/SouthAfrica/News/4-things-you-didnt-know-about-copper-theft-20140626).

According to Geldenhuys (2008), the actual loss of copper cable in South Africa (Cf. Annexure C3, Map of South Africa) could be multiplied tenfold to determine the actual overall economic loss. The costs imposed on all the victims who had been without essential services had not been included in the calculation (Pretorius, 2012). Geldenhuys (2008) said the problem of cable theft was recently further exacerbated through the theft of parts of power pylons and the theft of cables connected to railway tracks.

Burger and Lancaster (2014) have correctly pointed out that cable theft is a concern to businesses. It places a burden on companies, as it often leads to protracted power outages, which leads to a loss of productivity, among other things. This particular crime statistic, reported annually by the South African Minister of Police, is hidden in a general catch-all crime category named 'all theft not mentioned elsewhere'. In 2012, the then police Minister, Nathi Mthethwa, estimated that cable theft costs South Africa approximately R5 billion a year, but other sources have placed this figure at closer to R10 billion a year (Burger & Lancaster, 2014).

Solomon (2013) mentions that the real problem is that copper is easily stolen, almost impossible to secure, and has become a secondary industry for people living on or below the breadline. Even death by electrocution is a risk worth taking for some copper thieves. If the value of the rand were to fall further, copper, chrome and ferrous metals would become even more valuable commodities. Solomon (2013) also asks whether it would be justifiable to curb exports, and whether this would work, and at what cost to jobs and the economy.

Peters (2014) correctly pointed out that in the past, many people died in their attempts to steal copper: they have burned and electrocuted themselves. The cumulative damage to the economy of this country, its organisations and its individuals, is staggering. The previous Public Enterprise Minister, Barbara Hogan, said that copper cable theft was so rampant that it was costing the South African economy approximately R7 billion a year (Phakathi, 2010; Pretorius, 2012). Singh and Omar (2011) say that hundreds of tons of scrap metal, including stolen copper cables and pipes, are shipped out of Durban harbour to Eastern countries, where there is a substantial demand.

Currently, copper and cable theft after unwanted strikes (Ras, 2015) poses the biggest threat to the mining industry in terms of risks to life and production losses. Copper and cable theft is classified as one of the Top 5 priority crimes in the mines (Horn, 2012). According to a study done by Horn (2012), a participating mine in the research study explained that during 2009, the criminal threat changed from opportunistic crime to organised crime, and the mine had to deal with trespassers accessing redundant underground mining areas to steal copper cable.

Horn (2012) also says that while offenders who operate on the surface are limited in what they can conceal and carry, the underground thieves had weeks to strip underground copper cables and were able to move vast amounts of stolen copper, thereby increasing the losses exponentially. Horn (2012) further says that the study found that losses recorded from underground copper-related thefts showed a significant increase (79 %) during 2009 over 2008 (Cf. Annexure A1). Horn (2012) further mentions that this reflects the highest increases recorded loss due to underground copper-related thefts, compared with all the other years, and comprised 63 % of all the losses (Horn, 2012).

In addition to the R9 219 115 loss that the participating mine recorded pertaining to copper-related incidents in this five-year period (2006–2010), an additional amount of R4 607 616 in production losses was recorded as a result of copper-related thefts, mostly when cables that provided electricity to operations were cut, and an interruption in production was experienced (Horn, 2012).

In an article written by the Chamber of Mines of South Africa in the Hi Tech Security magazine (http://www.securitysa.com/article.aspx?pklarticleid=5592), the Chamber said that the mining sector faces risks in the form of organised crime, which includes the theft of vital infrastructural items such as copper cabling and operational equipment (Hi-Tech Security Solutions, 2009). The Chamber of Mines (2010) also mentions that cable theft continues to impact on the heavy-haul Sishen to Saldanha ore railway line, and that Transnet and the mining companies were all attempting to address the various problems that continue to inhibit further growth (Horn, 2012). About R400 million was allocated to theft management by Transnet Freight Rail to undertake crime prevention (Chamber of Mines, 2010; Horn, 2012).

In an article published on 06 October 2014 in the City Press (http://www.citypress.co.za/news/cable-theft-treated-petty-crime-andries-nel/), Minister Andries Nel said: "… *There is a huge impact on the broader provision of basic services, where electricity supply is interrupted, that can also lead to the interruption in the supply of*

water such as we have seen in Gauteng recently. The theft of non-ferrous metals could also impact social stability …. any of the protest actions that we see as service delivery protests, once you investigate more closely, often come back to interruptions of services which in turn are occasioned by the theft of public infrastructure ...." (http://www.citypress.co.za/news/cable-theft-treated-petty-crime-andries-nel/).

According to an article published by Fin24, the South African Chamber of Commerce and Industry (SACCI) says the value of copper stolen increased to R15.4 m in May 2014, whereas it was R12.5 m in April 2014 and R11 m in March 2014 (Fin 24; http://www.fin24.com/Economy/Sacci-calls-for-copper-theft-unit-20140626). SACCI noted that the May 2014 figure was 71.1 % higher than the previous year, and was the third consecutive monthly increase. The volume of copper stolen increased to 214 metric tons in May 2014, from 176 metric tons in April 2014, and 153 metric tons in March 2014.

Business Against Crime (BAC) has estimated that copper cable theft is costing South Africa over R5 billion a year, with the damage done amounting to far more than the value of the stolen material. Driven by high prices, copper theft brings down telecommunications, transport and electricity services, impacts on living standards, and drives up the costs of goods and transport (http://www.securitysa.com/article.aspx?pklarticleid=6974).

In an article published by the City Press on 06 October 2014 (http://www.citypress.co.za/news/cable-theft-treated-petty-crime-andries-nel/), the South African Chamber of Commerce and Industry's CEO, Neren Rau, said in response to a question, that the demand from China was driving up the price of copper. "Diplomatically we cannot go to a different country and ask them to take responsibility for a problem we couldn't control", he said, "We would also be entering the discussion with an accusatory tone, which we also don't want to do with a key trading partner" (http://www.citypress.co.za/news/cable-theft-treated-petty-crime-andries-nel/).

According to Eskom's Annual Report (2016), Eskom experienced losses from conductor (cable) theft, cabling and related equipment for 2016, totalling an amount of R85 million, involving 5 161 incidents (Cf. 3.4). The figures for March 2015 were R102 million in losses, with Eskom experiencing 5 680 incidents (Eskom, 2016). The combined effort between the South African Police Services and Eskom security resulted in 229 people being arrested. During March 2015, 297 people were arrested for cable theft crimes (Eskom, 2016).

1.12.3 The Extent of Cable Theft in Asia

In this section, the researcher will describe the extent and the impact of copper cable theft in some Asian countries (Cf. Annexure C4 Map of Asia, which includes the countries mentioned below).

China: Copper is used widely for industrialisation and infrastructure projects, and because of this, it is often seen as a barometer for the global economy. According to a study by the Institute for Security Studies (ISS), they found in 1999 that the price of copper had hit a 60-year low, as demand from post-industrial societies had slowed down, but in the next decade, the rapid industrialisation of China spurred copper prices ahead again to reach an all-time high of just above $10 000 a ton in February of 2011 (News 24, 2014; http://www.news24.com/SouthAfrica/News/4-things-you-didnt-know-about-copper-theft-20140626). According to Evans (2011), the price of copper has soared upwards in the last two years, driven up by booms in construction and industrial investments in China and India.

According to the ICSG's (the International Copper Study Group) latest figures, China is by far the largest consumer of refined copper, accounting for about 40 % of world demand. According to Hammer and Jones (2012), China is now the world's largest consumer and producer of copper. Its demand for the commodity has soared in tandem with the country's industrialisation process, given copper's extensive use in infrastructure (example plumbing, telecommunication wiring, and building materials) and manufacturing equipment (for example, electric power generation and transmission equipment). To meet its growing copper demand over the last decade, China has imported increasing amounts of copper ores (mostly from Latin America) and copper waste/scrap (mostly from the United States) for domestic processing, which is either locally consumed or re-exported.

As a result of the increased demand for copper, a robust international trade in copper has been created and the market for illicit copper is rising alongside it (News24.Com, 2014). In early 2002, copper prices hit record lows, falling to 65 cents a pound on the London Metal Exchange. However, this has changed as other Asian countries began to rapidly industrialise, especially with China obtaining the most copper because of its 20 per cent global copper consumption and Olympic preparations. According to Kooi (2010), scrap materials became the second-largest American export to China, after electronics.

China's dominance as both a global consumer and a supplier of copper, as well as the changes in China's domestic market conditions, can noticeably influence copper's world price (Hammer & Jones, 2012). China is the largest global producer of copper, even though it mines a limited supply of copper ores. This is explained by the fact that China imports significant quantities of copper ores and waste and scrap for smelting and refining into pure forms of copper to sell on domestic and international markets. Industrialisation and the building of infrastructure rely heavily on copper (Hammer & Jones: 2012).

China continues to increase its reliance on imported copper. According to Hammer & Jones (2012), China's imports account for about two-thirds of the raw materials used in its copper industry. The rising price of copper in global commodity markets over the past decade has provided incentives for Chinese copper-processing enterprises to expand production and export their refined products. According to the ICSG's recent forecast, China's demand for copper was foreseen to continue to grow by 4 % in 2012 and 5 % in 2013 (Hammer & Jones, 2012).

High global consumption rates, alongside the development and industrialisation of emerging economies such as China and India, have seen available copper reserves strained under mounting demand (International Copper Study Group, 2013). Binderman (2012) has also pointed out that there is a large market for nonferrous metals in Asia. To curb the export of stolen goods, the South African government is aiming to implement the draft Export Control Guidelines, No 24 of 2013. This South African initiative aims to control nonferrous and ferrous metal waste and scrap exports.

According to World Bank figures, 44 per cent of China's copper demand was used in construction and infrastructure, compared with the global average of around 33 per cent used in the same sector (Roberts & Rush, 2011).

There is no doubt that China's rapid industrialisation has contributed to its high demand for copper. According to the intergovernmental International Copper Study Group (ICSG), the World Bank figures confirm that 56 % of China's refined copper is used for infrastructural development and construction. Hammer and Jones (2012) say that refined copper has also been widely used as an input into consumer goods (27 %), industrial equipment (6 %), transportation (6 %), and other sectors (5 %).

Pakistan: Pakistan Railway's (PR) authorities mention that a train with copper wire on board was despatched from Khanewal to Lahore where the copper wire was to be stored at Mughalpura Workshop; however, the train was routed to Kharian where the copper wire, worth millions of rupees, was stolen. Pakistan Railway pointed out that there have been similar cases of this nature concerning the theft of copper from its freight trains. The Pakistan Federal Government announced an assistance package worth Rs11 billion (Pakistan's currency is known as the *Rupee*) to rescue the PR, which had been incurring losses worth billions due to mismanagement and corruption (http://tribune.com.pk/story/250715/pakistan-railways-arrests-major-in-copper-heist-case/).

India: In India, the state-owned telecommunications utility company, Mahanagar Telephone Nigam Ltd (MTNL), has offered its citizens, who tip off the state-owned company about the theft of its cables, a reward of Rs11 000. "The theft of copper cables from Mahanagar Telephone Nigam Ltd (MTNL) has always inconvenienced our customers and caused losses to the company. Services are affected when theft occurs and customers complain of poor connectivity" (Akkalkot, 2013). Akkalkot (2013) also said that if information leads to the arrest of persons responsible for stealing copper cables, the informer would then be notified and asked to collect a reward (http://timesofindia.indiatimes.com/city/mumbai/MTNL-announces-reward-to-curb-telephone-cable-theft/articleshow/22783146.cms). This example can be used by Eskom to provide financial rewards to people that provide information concerning copper theft.

Rajasthan: According to Sharma (2014), in Rajasthan (Cf. Annexure C4 Map of Asia, which includes Rajasthan which is a large state located at the north-western part of India) there were about 140 cases of cable theft lodged with the police in 2013, as against 56 in 2012, adding that 193 people were arrested in 2013, and cable worth Rs90 lakh was recovered from them. Sharma (2014) says that, with cases of power cable theft on the rise, the Rajasthan Police have appointed 120 Home Guards, called "wind dragons" – a dedicated force who will keep round-the-clock vigil in the border district of Jaisalmer – to check up on the crime. They would work under the guidance and instructions of the office of the Jaisalmer police. There are about 2 000 windmills, producing over 2 200 MW power, in Jaisalmer District, (Sharma, 2014; http://ibnlive.in.com/news/wind-dragons-to-check-power-cable-theft/443592-3-239.html).

According to Kamath (2012), long-distance trains plying the Konkan railway route between Panvel and Ratnagiri stations were paralysed for four hours because of the theft of a telephonic communication cable wire near Rasayani station. Kamath (2012) says that the incident took place on 2 October 2012 at around 9pm. Some thieves cut the telephonic communication wire near Rasayani station, which led to the failure of India's UPS system, PRP and automatic signalling of level crossing gates (Kamath, 2012).

1.12.4 The Extent of Cable Theft in Europe

According to Straker (2012), cable theft is a very serious issue for railways. Rising copper and metals prices have spurred this illicit market. The World Bank's commodity forecast shows that copper prices rose from $1 813 per metric tonne in 2000 to $8 828 in 2011. Starker (2012) says that, although there is no evidence that Europe's economic slowdown has driven the trade, "there is the coincidence of rising copper prices and unemployment levels at a time of growing criminal activity" (Straker, 2012; http://www.euractiv.com/transport/growing-cable-thefts-prompt-rail-news-515740). The above-mentioned article makes it clear that South Africa and other countries are also suffering the effects of cable theft and need to implement one or other preventative measures.

United Kingdom (UK): Metal theft has emerged as one of the fastest-growing types of crime in the United Kingdom (Cf. Annexure C5 Map of Europe which includes the UK) (Bennett, 2008a; Haynes, 2008; Sidebottom *et al*., 2011). Copper cable theft has recently been described as a "strategic priority" by the British Transport Police (BTP). The BTP are responsible for policing the railway system of England, Wales and Scotland, as well as the London underground network. While the cash price of copper on the London Metal Exchange was less than US $3000 per tonne at the start of 2009, it is now more than US $9000 per tonne (and had breached the US $10 000 barrier early in 2011). Evans (2011) says for that kind of money, criminals will take risks – even the life-threatening risks involved in stealing cables that could be carrying a live current.

The UK railway system network comprises over 16 000 km of tracks (connecting all major cities and most towns) and around 3 000 railway stations and depots, and services an estimated 6 million rail passengers a day. High-volume rail offences include applying graffiti, theft of passenger property, theft of motorcycles at railway stations, and violent crime. Evans (2011) says the approach taken towards modern offenders in the UK is rather different.

Copper theft threatens major damage to the electrical infrastructure and modern communications systems upon which ordinary life now depends and the government has increased its support for the police to arrest those responsible for these crimes.

Combating cable theft is now a major area of activity for the BTP, who are struggling to prevent cable theft that accounts for thousands of cancelled trains. But while the overall costs of this crime are huge, the returns to individual criminals are often very small. The return, as Evans (2011) correctly has mentioned, can also, of course, come in the form of electrocution and death.

According to Sidebottom *et al.* (2011), the recurrent explanation is that metals have become attractive targets for theft due to the soaring price of scrap metal. This is generally attributed to global demand for metals exceeding supply. Consequently, it is proposed that price increases have stimulated the creation of illegal markets that provide opportunities to sell stolen metals at financially rewarding prices. The researcher believes that the high international demand for copper has also contributed to the increase in cable theft in South Africa.

The Netherlands: Due to rising copper prices in the Netherlands in recent years, the number of thefts also increased. In 2011, the Dutch government started a campaign to stop copper theft. The cabinet set up a compulsory identification requirement for anyone who wishes to sell copper or copper alloys (http://www.shanghaidaily.com/article/article_xinhua.aspx?id=239539).

The Shanghai daily newspaper reported that on 5 September 2014, the rail traffic service between the Dutch Schiphol Airport and Amsterdam was cancelled or disrupted on that Friday due to power cable theft. The theft of cable caused considerable damage to the track. The train running between Schiphol and stations Amsterdam Zuid and Amsterdam Lelylaan were therefore not available and other routes suffered heavy delays (http://www.shanghaidaily.com/article/article_xinhua.aspx?id=239539). It is clear that incidents like this emphasise the serious consequences of cable theft.

Germany: Germany's state rail company reported that metal theft grew 50 % from 2010 to 2011 (Spence, 2012). The report says that besides electricity and signalling cables used on rail corridors, the telecommunications industry had also reported rising thefts of copper

cables, while rail authorities also say thieves are dismantling safety fences and selling the metal for scrap (Spence, 2012).

Germany's state railway is using artificial DNA to mark its infrastructure to make recovered goods easier to trace. In July 2012, *Deutsche Bahn* joined with leading telecommunications and energy companies to establish an association of German metal traders so that dealing in scrap could be more closely monitored (http://www.euractiv.com/transport/growing-cable-thefts-prompt-rail-news-515740). The marking of infrastructure and the establishment of an association for German metal traders are good examples for what can be done in South Africa to better prevent cable thefts.

Belgium: The German report further mentioned that authorities at Infrabel, the Belgian rail infrastructure company, had cited the theft of copper cables that convey electric current to locomotives as a frequent cause of delays on its regional and international lines. On 25 October 2012, the removal of railway cable at night on a major commuter line between the south-western Belgian towns of Mons and Brussels disrupted trains for hours while Infrabel workers replaced stolen cabling.

France: France's rail operator, SNCF, has used helicopters to patrol railway lines to deter criminals. Courts in France and the United Kingdom recently convicted individuals involved in cable thefts, although the authorities have acknowledged that a larger problem of organised crime remains.

Portugal: According to the news website in Portugal, Pol-PRIMETT II (http://www.pol-primett2.org/news/2784/latest-metal-theft-news-from-portugal), in the town of Arroeiras-Mafra, two individuals were arrested on the 7 November 2014 by police, following an incident of metal theft. The thefts occurred in three garages and warehouses. The police were alerted by local residents and caught the thieves in possession of goods and materials worth approximately €25 000.

Pol-PRIMETT II (http://www.pol-primett2.org/news/2784/latest-metal-theft-news-from-portugal) further mentions that on 24 November 2014, a 35-year-old man was arrested on suspicion of metal theft in the town of Abitureiras-Santarem. The man was caught while trying to steal a number of copper cables from inside a building, after causing significant damage to the building's doors and windows. It was later discovered that the man had a number of outstanding arrests warrants.

Greece: In Greece, the cash-strapped national rail company says that cable thefts have cost €12 million in recent years (http://www.euractiv.com/transport/growing-cable-thefts-prompt-rail-news-515740).

European Union (EU): On the 27th and 28th May, 2014, a two-day operation against metal thieves, which included 17 European Union (EU) member states, was undertaken. The following countries participated in the coordinated operation: Austria, Belgium, Bulgaria, Cyprus, Estonia, Finland, France, Germany, Hungary, Ireland, Italy, Lithuania, the Netherlands, Portugal, Romania, Spain and Sweden. The Belgian Federal and Judicial Police were the main drivers of the operation. (https://www.europol.europa.eu/content/newsletter-17-eu-member-states-coordinated-action-against-metal-thieves).

The two-day law enforcement operation has sent a strong signal to gangs of organised metal thieves who operate all over Europe, and to the many scrapyards that simply accept all kinds of metal, with 'no questions asked' (https://www.europol.europa.eu/content/newsletter-17-eu-member-states-coordinated-action-against-metal-thieves).

The law enforcement authorities carried out checks at scrapyards, on construction sites, and along border roads and railway tracks. Specific scrapyards suspected of handling stolen goods were also investigated. Intelligence shows that stolen metal is often transported across several borders and sold as scrap, or for recycling, far distant from the scene of the crime. Intelligence gathered during this operation was further analysed by Europol in order to pinpoint the main modus operandi and the people and gangs involved in this illegal trade (https://www.europol.europa.eu/content/newsletter-17-eu-member-states-coordinated-action-against-metal-thieves). Arrests were made in several countries, including 37 persons who were arrested in Bulgaria. In Italy, more than 120 tonnes of copper was confiscated.

Fines were also issued for receiving stolen goods and violation of environmental regulations (https://www.europol.europa.eu/content/newsletter-17-eu-member-states-coordinated-action-against-metal-thieves). It is clear that the EU member states intend to send a strong message to cable thieves that their illegal activities will not be tolerated.

According to Wainwright (2014: (http://www.euractiv.com/transport/growing-cable-thefts-prompt-rail-news-515740), "There are many organised crime groups involved in the large-scale theft of metals. They and the scrap dealers, who buy copper cable stolen from railway tracks or plaques from gravestones, now realise that this kind of cross-border crime is being

taken seriously. The crime often affects critical transport, communication and power networks, causing considerable disruption, and the costs associated with replacing and repairing the damage caused often exceeds the value of the metal stolen" (http://www.euractiv.com/transport/growing-cable-thefts-prompt-rail-news-515740).

European Commission report: This report, entitled *Cable theft surge prompts railways to seek EU action*, was published on the 29th October, 2012, by The European Commission (http://www.euractiv.com/transport/growing-cable-thefts-prompt-rail-news-515740). In it, the Commission states that maintaining progress in infrastructure quality and service has been hampered by a more perverse problem: theft and vandalism. They mentioned that the tough economic times and high metals prices have led to the theft of rail and electrical cabling, to be resold as scrap. They also say that thieves are targeting signalling cables, overhead power lines and even metal fences to sell for scrap.

The October 2012 report states that rail officials had been complaining for months about growing incidents of cable theft. Straker (2012) says that involvement in the Commission has grown since it was started in 2010. Britain, Bulgaria, France, Greece, Italy, the Netherlands, Poland, Portugal, Spain and Sweden are all participating countries. The partnership is studying models for potential EU-wide standards to curb metal theft. France, for example, has adopted a law requiring anyone selling scrap to be registered, while Portugal and the United Kingdom have barred cash payments for metal scrap (Straker, 2012; http://www.euractiv.com/transport/growing-cable-thefts-prompt-rail-news-515740).

The Community of European Railway and Infrastructure Companies (CER) report: This report appeared in 2014, entitled *Metal Theft*, and mentions that metal theft is considered as an organised, cross-border crime in Europe. This is also acknowledged by Europol in the Serious and Organised Crime Threat Assessment (SOCTA) report from 2013 as being one of the major crime threats facing the EU, which has had a significant impact on the daily lives of people and railway businesses in Europe, and had already been a problem for decades. The major target of metal thieves is copper. According to the World Bank Commodity Price Data, the annual price of copper rose from approximately US$1560 per tonne in 2002 to approximately US$8000 in 2012. Recently, the price of copper decreased to 6650 US dollars per tonne (Position Paper Metal Theft, 2014).

The number of metal theft incidents has been increasing across Europe, which is also attributable to the growing global metal demand, consequently increasing prices of metals.

The thieves target any kind of metals – copper, aluminium, lead, brass, zinc, nickel, platinum, and bronze.

The CER 2014 report further says that besides the financial attractiveness, other factors that unfortunately contribute to the rise of metal thefts are the availability of, and accessibility to, metals, the simplicity of metal sales, the low risks and penalties involved, the difficult real-time detection and tracking of malicious acts and cable cutting (for instance on rail networks), and problems for law enforcement in obtaining evidence as soon as the metals enter the recycling process, as well as poverty, unemployment and low incomes (CER2014 report; http://cer.be/).

The CER 2014 report continues, saying that in the railway sector, the criminals are particularly targeting the signalling and power cables, but also attack rail fastening systems, rails, and certain elements from bridges, as well as elements from wagons and braking systems, which are all essential for the functioning and the efficiency of rail services. As such, the whole railway sector is affected by metal theft. Metal thefts, occurring every single day across Europe, lead to delay and even cancellation of thousands of trains, and affect millions of passengers and freight customers (CER2014 report; http://cer.be/).

According to this report, organised metal theft criminal groups, as well as metal theft opportunists, attack not only railways but also energy networks, telecommunications, construction sites, churches, war and grave memorials, heritage sites and even scrap metal dealers. The thieves steal anything that is made from metal, e.g. street signs, manhole covers, and shopping trolleys. This leads to physical, economic, social, psychological, spiritual, historical and political losses. Furthermore, as a consequence of metal theft, innocent victims, such as the staff members of railway companies, emergency services, and law enforcement agencies, as well as passengers, are exposed to higher risks when they are in the vicinity of the crime areas. Stealing copper can also lead to the death or injury of offenders who are stealing high-voltage cables. Moreover, and especially in the railway, energy and telecommunication sectors, metal thefts result in disruptions of vital infrastructure services, which can cause widespread cascade effects (CER2014 report; http://cer.be/).

The rail networks are too large to fence or guard entirely, and any immense and fundamental modification of the rail system would involve enormous structural and financial requirements. All CER members are facing the problem of metal theft and endeavour to find the best solutions on how to protect their businesses and their customers, for example by

replacing copper with other less-expensive metals where possible (however, copper is an excellent conductor of electricity, and thus irreplaceable for railway power cables), by protecting metals as much as possible, installing CCTV systems, perimeter violation detection systems, access control systems, intrusion detection systems, fire alarm systems, cable marking technology, and anti-theft alarm systems for copper cables, as well as also taking appropriate protection measures before, during and after transport of (scrap) metals via rail and other transport systems (CER2014 report; http://cer.be/).

This, however, is simply not enough, and because of the wide extent of the European railway networks, the costs of the above-mentioned measures are enormous, not always affordable and, last but not least, always need to be adapted to the prevailing risks involved (CER2014 report; http://cer.be/).

The CER 2014 report further suggests that, in most of the cases, the stolen metal is being sold to scrap metal dealers, where the offenders receive their reward (usually in cash). The financial attractiveness and the simplicity of metal sales is the driving force behind this specific crime. The scrap metal dealers also need to become part of the solution in tackling metal theft, as they are also affected by metal theft (CER2014 report; http://cer.be/).

There is no doubt that criminal sanctions can have a particular deterrent effect, as potential perpetrators can be expected to make certain risk calculations before deciding to engage in criminal activities. The introduction of minimum sanctions is consequently considered necessary to ensure that an effective deterrence all over Europe can be achieved. The fear of receiving a more severe legal punishment can prevent some of the offenders from committing this kind of crime (CER2014 report; http://cer.be/). It is clear that it is not only South Africa that is wrestling with copper theft. The CER 2014 report has made it clear that Europe is also especially targeted by copper thieves.

1.12.5 The Extent of Cable Theft in the Americas

This section briefly focuses on the United States of America and Brazil.

The United States of America (USA): The United States Department of Energy has released a report (2010) entitled, *An Updated Assessment of Copper Wire Thefts from Electric Utilities*. According to this report, copper theft continues throughout the United States of America (USA) (Cf. Annexure C6 Map of the Americas, which includes the USA), but the magnitude of this theft has been reduced considerably. The problem is not likely to cease as

long as copper prices remain sufficiently attractive to would-be thieves. However, the combined efforts of electric utilities, lawmakers, scrap metal dealers, and local law enforcement officers have succeeded in reducing the problem and driving a wedge between copper price increases and comparable increases in copper theft.

Copper is attractive to the electric utility industry because it is an excellent conductor of electricity, it resists corrosion, and in spite of recent price increases, it is inexpensive relative to alternative metals. Because of its properties of high ductility, malleability, and electrical conductivity, it has become the benchmark for almost all types of wiring (US Department of Energy, 2010).

The price of copper has been the major factor directly influencing general copper theft and copper wire theft from electric utilities. In 2004 and 2005, reports of copper thefts began to rise dramatically, as copper prices increased. When copper spot prices rose above $3.00/lb in 2006, the magnitude of thefts began to grow exponentially. General copper thefts, excluding copper wire, increased more rapidly than copper wire thefts. As copper prices cycled up and down during 2006, 2007, and 2008, copper thefts moved in similar directions (US Department of Energy, 2010).

When the price of copper began to decrease in the summer of 2008 and continued falling throughout the year due to the recession, the number of reported copper thefts began to drop. In the spring of 2009, the price of copper began to rebound, but the price was still too low to encourage a resurgence of copper theft. It was not until the price began to average over $3.50/lb that reports of thefts began to climb. Even so, a significant price increase did not occur until the end of 2009. For that reason, reports of copper theft in 2009 were down 79 per cent from the peak year of 2008. It is noteworthy to mention that in 2009 and 2010, copper wire theft was a much smaller portion of all copper theft reported (US Department of Energy, 2010).

A study of one US County by Taylor *et al.* (2003) found a link to drug and/or alcohol dependency during a study of 8 intruders fatally electrocuted between 1981 and 2001 at electricity substations (Bennett, 2008a). The average age of the deceased was 33 years, five of whom were found to have been intoxicated (either with cocaine or alcohol).

American Scrap Coalition: A group of United States (US) steel scrap industries created the American Scrap Coalition in response to global scrap metal trade barriers. While the price of

metal rose dramatically, many countries restricted their exports, but US exports continued at record levels. The scrap metal supply did not keep pace with the international demand, causing a crisis of scrap metal availability and increased pay from scrap metal dealers (Kooi, 2010).

Copper theft has risen sharply in the United States (Kooi 2010; Whiteacre *at al*., 2008; Sidebottom *et al*., 2011). The FBI warned in 2008 that copper thieves in the US were targeting electrical substations, cellular towers, telephone land lines, railroads, water wells, construction sites and vacant homes. Despite the FBI's warning, figures from the National Insurance Crime Bureau show that the number of reported copper thefts more than doubled, from 13020 in 2006–2008, to 32568 in 2010–2012 (News 24, (http://www.news24.com/SouthAfrica/News/4-things-you-didnt-know-about-copper-theft-20140626).

Utilities have become targets for copper theft because tons of copper are used in each electric utility substation, mostly in transformers. Utilities also maintain large concentrations of copper wire at utility construction sites and storage yards, in the back of utility trucks, and in transmission and distribution lines (US Department of Energy, 2010).

Brazil: According to Buckley (2014), Brazil's regional telecommunications service provider, Sercomtel, continues to experience copper cable theft incidents. Buckley (2014) confirms that thieves stole 1 724 metres of telephone cables in January 2014 alone. These 19 incidences in 2014 cost Sercomtel $26 000 in equipment and labour costs to repair the lines. The copper theft trend has continued, with seven incidents and more than 800 metres of cable stolen since the January 2014 incidents.

The above-mentioned examples indicate that copper theft is not a uniquely South African phenomenon, but an international crime.

1.12.6 The Extent of Cable Theft in Australasia

Australia: According to Narayan and Regan (2013), the increase in copper prices and copper theft has now become a major problem for the telecommunications industry in Australia (Cf. Annexure C7 Map of Australasia and New Zealand). The copper thefts occur either during construction stages or later on when the sites are operational. If the theft occurs during construction, then there is an economic loss and an annoyance. However, theft of copper from operational facilities is a larger concern because it brings about a serious safety

problem, not only for the copper thieves but also the general public. There is serious impact on noise levels at a telecommunications site when the ground grid is removed, causing interference with radio communications and broadcast transmission, and this has operational ramifications (Narayan & Regan, 2013).

According to Burgess (2008), Victoria Police had cracked the state's largest copper theft racket, which they say had netted more than $1 million. The copper wiring, believed to have been stolen from a variety of locations, including rail tracks, power stations and scrap metal depots, was destined for the Asian black market. Burgess (2008) states that the police had identified several people believed to have been involved in stealing copper wiring and were trying to export it overseas. Burgess (2008) avers that a search of a second-hand dealer store in Boronia, to the east of Melbourne, uncovered four tonnes of copper wiring.

Burgess (2008) also says that if you consider the cost to the community and businesses every time copper wiring is stolen, requiring repairs and maintenance to train tracks and power stations, it is quite significant. The actions of the police must send a clear message to people engaging in this sort of activity that the police are watching them and that they will be caught. According to Burgess (2008), the police stated that they had seized 8.3 tonnes of stolen copper wiring.

According to a report published in *3 News* on the 01 February 2008, there is a lethal new twist in the nightmare world of drug dependency: drug addicts are stealing copper wire from high voltage power lines to fund their drug habits (http://www.3news.co.nz/nznews/p-addicts-ignore-danger-to-steal-live-cables-2008020116#ixzz3M9Z9O9Fm).

The soaring price of scrap metal means that they are, in money terms, better off stealing a cable than a wallet. Professional tools are used to bring down and strip the power lines before the cables are sold for scrap metal. However, it is not just rural areas that are being targeted (http://www.3news.co.nz/nznews/p-addicts-ignore-danger-to-steal-live-cables-20.

The frequency of the copper thefts seems to follow the price of copper in the scrap metal trade, which naturally follows the market price of copper. With the demand for scrap copper, copper prices remain high and it was envisaged that this problem would be on the rise in months and years to come, should this trend continue (Narayan & Regan, 2013).

New Zealand: *3 News* in New Zealand has reported that the problem of cable theft occurs because people steal to support their drug habits and that the number of drug addicts is

growing in New Zealand. The article further says that in November and December 2007, there were 20 incidents of live cable theft in Pukekohe alone (http://www.3news.co.nz/nznews/p-addicts-ignore-danger-to-steal-live-cables-2008020116#ixzz3M9Z9O9Fm).

With scrap copper prices being the highest they have been in almost 30 years, and with the lowest grade point of 'P' (another name for the drug methamphetamine) costing $40, some addicts are prepared to interfere with live electrical installations to fund their addiction. The *3 News* also said it had learned of an incident in December 2007 where a man in his forties had died after being electrocuted while stealing live copper wire from a west Auckland construction site. It is believed that the man was taking the cabling to help fund his drug addiction (http://www.3news.co.nz/nznews/p-addicts-ignore-danger-to-steal-live-cables-2008020116#ixzz3M9Z9O9Fm). The problem of cable theft to support the drug habits of drug addicts is thus growing in New Zealand, according to 3 News (http://www.3news.co.nz/nznews/p-addicts-ignore-danger-to-steal-live-cables-2008020116#ixzz3M9Z9O9Fm).

According to Narayan and Regan (2013), copper is widely used in grounding applications in both bare and insulated forms because conductors used in this application are often perceived to be "not live", and this form of copper use has become a prime target for copper thieves.

1.13 FACTORS CONTRIBUTING TO CABLE THEFT

The following factors have been found to be contributing to cable theft:

Unemployment and Poverty: There is no doubt that many people steal copper to help them to survive and to fulfil their basic needs. Binderman (2012) points out that unemployment is one of the main drivers of nonferrous metal theft, as people need money for basic necessities. He also added that crime syndicates use unemployed people to their advantage to steal cables on a large scale. He further avers that some thieves are well-organised into groups and move around in the country to hit "soft targets".

It seems clear that cable theft and vandalism are not necessarily geographically bound, but can be found in all main cities in South Africa, and abroad, owing to the multiple challenges of urban growth, such as surging unemployment, abject poverty and squalor, increasing inequality and perceived social deprivation (Dzansi *et al.,* 2014). It is well known that high

unemployment levels often reduce the capacity of people to participate in legal activities to gain a legitimate income.

Demand for copper: In South Africa, the demand for copper makes the stolen copper cables extremely easy to sell, due to eager scrap dealers, looking to profit from the global price increase (Booysen, 2014; Nkabinde, 2014; Krause, 2014). Theft of electricity cables, like most theft, is more about socio-economic challenges than plain theft. Motivating factors behind theft of cables vary. There are thieves who steal cables opportunistically (Maseema, 2013), but there are others who steal cables out of need, and there are yet other people who steal out of greed.

Much of the work of scrap collectors is legal, albeit informal, whereas the illegal trade in metal is far more lucrative, and consequently, very attractive. Scrap collectors are often tempted to supplement their earnings by stealing a few metres of copper cable from sources close to home (Moodley, 2014; Booysen, 2014; Nkabinde, 2014; Krause, 2014).

The lack of effective security at Eskom: It is clear that if Eskom's security was effective enough, there would not have been constant reports made of copper thefts that are taking place.

Carelessness of project management staff during and after Eskom projects: Eskom suffers heavy losses from its projects because cable that is supposed to be recovered (either redundant cable or left over from the project) is left on site once the project is complete (Cf. Annexure A20 & A21). In many instances, the project officer/clerk of works does not make arrangements to recover the cable for storage, nor do they (at most times) provide safe and secure facilities for the excess cable (Rajkumar, 2014; Maxwell, 2014).

Decisions regarding the safe storage of cables (both new and redundant cables) before, during, and after a project should be subjected to more rigorous security assessments by Eskom's security. Determining the most effective approach to protecting these cables will be based on a security assessment and possible needs of those likely to be entrusted with the responsibility for safeguarding the cable (security officers). Experience has shown that the actual work of evaluation needs to be supported by appropriate mechanisms that must be in place to protect the cable (regular site visits by the project officer, daily accounts of the cable used, daily accounts of the cables recovered) and that regular and timely feedback on these

findings from these assessments should be passed back to the responsible managers for record and intervention purposes (Rajkumar, 2014; Nkabinde, 2014, Ogle, 2014)

1.14 DEFINITIONS

In exploring the topic, *Investigation towards the prevention of cable theft from Eskom*, it is important to understand certain pertinent concepts. Steenkamp (2002) has correctly pointed out that definitions are "statements of what something is". It is important to know what exactly a person means when he or she is using a particular term or word (Ras, 2015b). The following are some of the terms referred to in this study:

Cable theft: Cable theft is the theft of physical electrical cable (http://en.wikipedia.org/wiki/Cable_theft). In South Africa, cable theft for many people is a synonym for copper theft. In Eskom, cable theft signifies the theft of copper cables (conductors) used by Eskom. However, aluminium is also used when copper is too heavy or too expensive to use. In this study, the emphasis is on cable theft at Eskom which includes copper and aluminium theft (Cf. Annexure B27).

Conductor: A wire or combination of wires not insulated from one another, suitable for carrying an electrical current (Network Planning Guideline for Eskom Lines and Cables, unique number 34-619).

CURA system: This is an Eskom governance, risk and compliance software system, which Eskom utilises, inter alia, to report all criminal activities. This system enables Eskom to gain a more coherent and holistic view about all "inside" statistics.

Disciplinary problems: "Disciplinary problems" refer to disruptive behaviour that "significantly affects other people's fundamental rights to feel safe, to be treated with respect and to learn. This encompasses behaviour that interferes with the rights and welfare of others, it is offensive or inconsiderate behaviours, and dangerous to persons or property" (Mabeba & Prinsloo, 2000: 34-41).

Distribution: This refers to the local transmission of electricity from smaller substations to the end-user customers, and this covers the final part of Eskom's energy supply chain.

Eskom's ENECC report: This is Eskom's Network Equipment Crime Committee Report, which reflects the monthly crime reports relating to Eskom's equipment theft.

Eskom Standards: These refer to all related policies, procedures, work instructions and standards in Eskom.

Generation: This pertains to the generating unit within Eskom which is responsible for electricity production at power stations.

HV (High Voltage): This refers to networks with nominal voltages from 44 kV to 132 kV.

KPI: Key performance indicator, which is used to evaluate the success of a company regarding a specific key figure and indicator.

KWh/MWh/TWh: Kilowatt, megawatt, and terawatt hours, respectively, are measures for quantifying units of electricity production or consumption; the measure of electricity, Watt, is multiplied with time in order to get a quantifiable measure for the use of electricity over time. It is usually used to calculate the cost of electricity, since the measure of time is necessary to calculate the amount of total electricity used.

Private Security: Private security refers to all people involved in security and to all the efforts the efforts by individuals and organisations to protect their assets from loss, harm and reduction in value, due to threats. These assets may include people, fixed and immovable property, business rights, information, company image, operational strategies, contracts, agreements and policy (Bosch, 1999: 4).

Private Security Industry Regulatory Authority (PSIRA): In terms of the Private Security Industry Regulation Act, 56 of 2001, PSIRA is the statutory body set up by the Act with the primary objective to regulate the private security industry and to exercise effective control over the practice of security service providers in the public and national interest, and in the interest of the private security industry itself (PSIRA, 2015a).

Risk analysis: Addison (2002: 2) describes risk analysis as a form of security assessment. It focuses on the process of identifying risks and their causes and their consequences, as well as the impacts of their occurrences.

Risk: According to Le Roux (2004:19), risk is defined as the chance or likelihood of an undesirable event occurring and causing harm or loss. The key element of risk here is uncertainty, without which there is no risk.

Security business (service provider): According to the Private Security Industry Regulation Act, 56 of 2001, "Security business means, any person who renders a security service to another for remuneration, reward, fee or benefit, except a person acting only as a security officer" (PSIRA, 2015a).

Substations: Substations are self-contained units which are controlled from the main control centres and are mostly situated in remote areas. They are specially designed to work 24 hours a day without attention and to operate outdoors in all weather conditions (Cf. Annexures B15 – B23).

Security service: According to the Private Security Industry Regulation Act, 56 of 2001, "Security service means protecting or safeguarding a person or property in any manner" (PSIRA, 2015a).

Security risk control measures: According to Rogers (2008: 152-161), security risk control measures refer to all the security measures that must be implemented for deterrence, deflection, detection, delay, reaction, identification, rectifying identified security weaknesses, detention of perpetrators, and the recovery of losses from insurance.

Security officer: In terms of Section 1 (1), security officer means "any natural person who is employed by another person, including an organ or department of the State and who receives or is entitled to receive from such other person any remuneration, reward, fee or benefit, for rendering one or more security services" (Private Security Industry Regulatory Act, No 56 of 2015a).

The National Grid: The network of high-voltage power lines linking power stations to the cities, towns, rural and residential areas where electricity is used is called the national grid or an interconnected grid. All electricity that Eskom generates is fed into this grid for national distribution. However, Eskom does not distribute electricity directly to all consumers. Most municipalities buy electricity in bulk from Eskom and resell it to consumers (Eskom factsheet, 2014) (Cf. Annexure C1).

Theft: This is the unlawful and intentional removal of movable property belonging to another (Snyman 1986: 511). In the context of Eskom, it will mean the removal of Eskom's cable.

Threat: An individual or group with the motivation and capability for undertaking crime, terrorism, foreign intelligence, illicit commercial or industrial competition, and malicious or

other malevolent acts that would result in loss of assets at a facility, is a threat (Garcia, 2008: 302).

Transmission of Electricity from Eskom network: This is the transportation of electricity. Power stations all over South Africa are linked by overhead transmission lines. The transmission lines are supported by towers called pylons and transport the electricity by means of thick aluminium and copper wires. The network of transmission lines is called the National Grid.

1.15 STRUCTURE OF THE THESIS

This present study has been divided into eight chapters.

CHAPTER ONE: GENERAL ORIENTATION TO THE STUDY

This chapter has outlined the introduction and provided a foundation for the study, together with a description of some of the occurring problems (see section 1.5), the rationale for the research (see section 1.6), the research hypotheses which were formulated in this research (see section 1.7), the research aims (see section 1.8), the research objectives (see section 1.9), the basic research approach, methods and techniques (see section 1.10), action research (see section 1.111), cable theft in historical perspective (copper theft in Africa, Asia, Europe, USA, Australia and New Zealand) (see section 1.12) and some factors contributing to cable theft (see section 1.13).

CHAPTER TWO: RESEARCH METHODOLOGY

This chapter focuses on research methodological issues, describing, inter alia, the qualitative research approach and methods used in this study.

CHAPTER THREE: THE EXTENT OF CABLE THEFT AT ESKOM

This chapter focuses on the extent of cable theft from Eskom in South Africa. Some issues addressed are the reasons for the increase in copper theft and why thieves prefer it to aluminium. Also discussed are Eskom's financial losses experienced with cable theft, the economic sabotage caused by cable theft, the hidden costs of cable theft, the role scrap dealers play in the promotion of cable theft, Eskom's partnerships in the prevention of cable theft, and finally, the specific responses that Eskom has in place to deal with cable theft.

CHAPTER FOUR: ESKOM'S IN-HOUSE SECURITY AND CABLE THEFT

This chapter discusses, inter alia, the origin of Eskom's in-house security, its effectiveness in curbing cable theft, and the difference between Eskom's in-house and private security guards.

CHAPTER FIVE: PRIVATE SECURITY IN ESKOM AND CABLE THEFT

This chapter discusses private security in Eskom and sets out an organogram of Eskom's security structures, as well as a description of Eskom's requirements for security companies that wish to render a contract security service and a discussion concerning why private security contractors cannot prevent Eskom's cable theft.

CHAPTER SIX: ESKOM INTERNAL SECURITY MANAGEMENT TEAM AND THOSE RESPONSIBLE FOR THE CAPTURING OF ALL RELEVANT INFORMATION RELATED TO CABLE THEFT

Chapter Six examines Eskom's internal security management team and those responsible for the capturing of all relevant information related to cable theft.

CHAPTER SEVEN: ACTION STEPS TO PREVENT CABLE THEFT

This chapter highlights in detail what new action steps should be taken to prevent cable theft at Eskom.

CHAPTER EIGHT: SUMMARY OF FINDINGS, RECOMMENDATIONS AND CONCLUSIONS

This chapter sets out the summary, findings, recommendations and conclusions of this study. A summary of the research findings is given, arising from this study. The contribution of this study is discussed, and recommendations and suggestions are made to Eskom on how to prevent cable theft. Finally, the chapter ends with a conclusion.

1.16 SUMMARY

This chapter has outlined an introduction to, and provided a reason for, this study, and has outlined the areas of interest noted in subsection 1.15 above.

In the next chapter, the researcher gives an overview of the research design and methodology used in this study.

CHAPTER TWO
RESEARCH METHODOLOGY

2.1 INTRODUCTION

The aim of this chapter is to outline the qualitative research method that was followed in this thesis (see item 1.8 above). The present research was not concerned with philosophical issues in science and research (Cf 1.1), or about the theories and various kinds of reasoning about research methods or statistical empiricism, rather, it was about addressing the specific research objectives related to cable theft at Eskom (see section 1.9) (Ras, 2006:76; Berk *et al*., 1992; Cullen, 2011; McNeeley & Warner, 2015). In other words, the researcher wished to assist Eskom in incurring no further cable theft losses.

The previous chapter gave a general orientation to this study and the reader was oriented regarding the global problem of cable theft. Although Eskom is a major victim of cable theft in South Africa, other South African businesses are also experiencing a major problem with cable theft. There is no doubt that cable theft is a global problem. This chapter discusses the research methodology that directed this study.

The purpose of this chapter is to explain the rationale behind the methodology that was used and to indicate how the research was conducted. In this chapter, particular attention has been paid to the qualitative research approach related to this study.

2.2 THE REASON FOR THE PRESENT RESEARCH

The reason for this research was to investigate, and gather relevant data in order to understand the extent of, cable theft in Eskom and what can be done to prevent it. The perception at the time of the start of the research was that cable theft is simply too high and that all security personnel working within, and for, Eskom, whether in-house or private security contractors, are simply unable to prevent it. This study was done to formulate clear solutions to this problem so that cable theft can be effectively stopped (Cf. section 1.5 &1.6).

2.3 RESEARCH APPROACH THAT IS USED IN THIS STUDY

In the study *Investigation towards the prevention of cable theft from Eskom,* a qualitative research method approach was used in order to gain a more complete understanding of this unwanted criminal social crime or phenomenon (Ras, 2006; 2010; Tewksbury, 2009:1). According to Tewksbury (2009:38), the numerous advantages of qualitative methods provide a depth of understanding of crime, criminals, and justice system operations and processing that far exceeds that offered by detached, statistical analyses.

Tewksbury (2009:38) further avers that because of the differences in the data, how data is collected and analysed, and what the data and analyses are able to tell us about our subjects of study, the knowledge gained through qualitative investigations is more informative, richer and offers enhanced understandings, compared to that which can be obtained via quantitative research. The researcher used the qualitative approach because it is a more in-depth and thorough look at any phenomenon (Ras, 2006; 2010; Bouma & Ling, 2004:165). Dawson (2002:14) and Bouma and Ling (2004:165) point out that this approach also explores behaviours, experiences and thought processes – which are important in getting to the heart of Eskom's copper theft problem.

Kvale (1996:1) states, "The qualitative research interview attempts to understand the world from the subjects' point of view, to unfold the meanings of peoples' experiences, to uncover their lived world prior to scientific explanations".

2.3.1 Action Research

In the context of this study, the researcher used Action Research (AR) to find ways in which this study could identify methods to prevent cable theft from Eskom. In other words, Action provides change, and Research provides understanding. Winter's (1996:14) description of action research is similar, and in his words, "Action research … refers to ways of investigating professional experience which link practice and the analysis of practice into a single productive and continuously developing sequence …." Action Research was chosen because it could be applied in collaboration with people that were actively involved in the prevention of theft – the research problem under investigation.

With this purpose in mind, the following features of the action research approach are worthy of consideration (Koshy, Koshy & Waterman, 2010:1; Ras, 1996: 99-104):

- Action research is a method used for improving practice. It involves action, evaluation, and critical reflection, after which – based on the evidence gathered – changes in practice are then implemented.
- Action research is participative and collaborative; it is undertaken by individuals with a common purpose.
- It is situation-based and context specific.
- It develops reflection based on interpretations made by the participants.
- Knowledge is created through action and at the point of application.
- Action research can involve problem solving, if the solution to the problem leads to the improvement of practice.
- In action research, findings will emerge as action develops, but these are not conclusive or absolute (Koshy *et al.,* 2010: 1; Ras, 1996: 99-104).

Kurt Lewin is recognised as being one of the originators of AR and defined "Action Research" as a process of organisational change having "a spiral of steps, each of which is composed of a circle of planning, action and fact-finding about the result of the action" (Lewin, 1946: 38).

By explicitly rejecting notions of objectivity, the AR researcher is clearly acknowledged as a key participant and to many, this lends strength to research aiming for relevance and utility (Dash, 1999:479). Participant validation can be particularly valuable in action research projects, where researchers work with participants on an ongoing basis to facilitate change (Barbour, 2001; Brydon-Miller, Greenwood & Maguire, 2003). Action research has a complex history because it is not a single academic discipline, but an approach to research that has emerged over time from a broad range of fields (Brydon-Miller *et al*., 2003). Action Research was chosen because of two things; firstly, the researcher is an active and registered private security officer who has an in-depth knowledge of cable theft and prevention (Cf. 2.10) and secondly, because it was applied in collaboration with people that were actively involved in the prevention of the research problem under investigation.

In light of Lewin's definition and the views of Dash (1999), the researcher has used his involvement as an advisor to Eskom and could thus use his knowledge, insights and

experiences obtained within Eskom to actively contribute to a better understanding of cable theft and its prevention in Eskom. In Chapter Seven, the researcher will mention the necessary action steps to prevent cable theft, based on the action research that was done for this study (See Chapter Seven). Huffman (2013:7) believes that good participatory action research does not merely advance knowledge, but aspires toward the positive transformation of social and material conditions.

2.4 THE REASONS FOR USING QUALITATIVE APPROACH IN THIS STUDY

The reason why the researcher has used a qualitative research approach, to investigate cable theft at Eskom, in order to prevent it, was simple. A qualitative approach is always about quality research, it is more in-depth in terms of its approach that a quantitative one and it has provided opportunities to people, who are tasked within Eskom to prevent cable theft, to speak their minds and to meaningfully and freely express themselves openly in any manner they wish (Tewksbury 2009:38). McMillan and Schumacher (2001: 395) refer to qualitative research as recording and analysing descriptions of people, together with their beliefs, thoughts and perceptions. This research approach will ensure that people's views will be incorporated in this study. Qualitative methods constitute an approach that centralises and places primary value on complete understanding, and on how people (the social aspect of our discipline) understand, experience and operate within milieus that are dynamic and social in their foundation and structure (Tewksbury, 2009:38).

By gathering as much real data, such as the opinions and views of people inside Eskom, it was possible to come up with more precise and comprehensive data that might prevent cable theft. A qualitative approach was used so that participants could freely express themselves and share their news and practical experiences related to this type of theft. It also has allowed the researcher to ask broad, open-ended questions to the participants in order to acquire more precise phenomenological data within Eskom's organisational environment. Although qualitative research is less common than quantitative research in criminology and criminal justice is, it is recognized for the value and unique contributions it can make (Tewksbury, 2009:40).

2.5 THE PRAGMATIC RESEARCH APPROACH

Nowell (2015:141) believes that in adopting a pragmatic philosophy, knowledge is understood as being constructed, based on the reality of the world we experience and live in,

and encompasses not only the reality of the past but also what is possible to create for the future. The knowledge one has, and the quality of believing this knowledge to be true, depend on one's real world experience and interests. Huffman (2013:4) says that pragmatic fieldwork draws inspiration from many facets of qualitative methods. Huffman (2013:5) further says that pragmatic fieldwork lives in the rich tradition of qualitative research that urges researchers to go, usually with their bodies, into the places they want to learn about. This study is not based on the well-known criminological theoretical studies. Rather, it is a pragmatic practical study that endeavours to contribute to the prevention of cable theft at Eskom, and serves as a topic for scholars to debate, which could lead to other theoretical developments, although this is not the primary objective of the study. There is unfortunately the erroneous perception by outsiders and scholars[4] that a company such as Eskom is straightforward and simple. This is definitely not the case: from organisational design to leadership, and to practical know-how on the ground, there are constant and dynamic security challenges because Eskom is a National Key Point (NKP) service provider, as well as owner of many other non-NKP sites which are highly complex and technical environments.

There is sadly a belief that a person cannot make a cutting-edge contribution to a discipline like criminology that is not thoroughly grounded in theory. However, according to Ras (2006; 2010; 2012a; 2012b), this is definitely not the case because any theory that is not driven by practical knowledge and problems is not a theory that is based on proper observation and rational thinking processes. Ritchie, Lewis, Mcnaughton nicholls and Ormston (2013:8) say that there are those who argue for a pragmatic theory of truth, which rests on the premise that an interpretation is true if it leads to, or provides assistance to take, actions that produce the desired or predicted results. Pragmatic fieldwork seeks democracy through enabling various voices to shape the research process, which allows research to be more responsive to a diverse set of interests (Huffman, 2013:7).

Although many philosophers have rejected pragmatism due to the previously identified limitations, many have chosen pragmatic philosophy to underlie their scientific practice (Nowell, 2015:145). In questioning the possibilities and limitations of this philosophy, a greater understanding of the implications for choosing pragmatism has been established. Ritchie *et al*., (2013:24) say that there has been a widening of interest in the use of qualitative

[4] There is no mention in any academic criminology books explaining practical ways to prevent cable theft at Eskom

methods in disciplines that previously relied on quantitative research and experimental methods, and in more applied fields. This is part of a broader recognition that researchers may need to adopt a more pragmatic stance in their research and draw on different resources available to them (both qualitative and quantitative) to address research questions.

Tewksbury (2009:52) argues that qualitative research is often critiqued by quantitative researchers as the form of research which provides initial theoretical constructs and tools for developing measurements (variables) that are used in statistical research to produce specifics about unique relationships among specified pieces (variables) of settings, groups and actions/interactions. Quantitative research may be valuable for evaluating theory and testing whether theory holds up under a variety of circumstances and instances. But, it is qualitative research and gaining various understandings that provide scholars with the insights to conceptualise issues and problems differently, thereby providing the foundation and building blocks for theoretical advancements, refinements and even initiations. This point is even acknowledged and conceded by defenders of quantitative methods' superior status in criminology and criminal justice (Tewksbury, 2009:56).

2.6 RESEARCH DESIGN

According to De Vos, Strydom, Fouché and Delport (2000: 77), a research design is a "blue print or detailed plan of how a research study is to be conducted." It is basically an overall plan of how data is going to be collected and how it is going to be analysed. For the researcher, it is a master plan that will eventually bring about the research results (De Vos, 2002: 337).

Babbie and Mouton (2001: 272) say that the research design denotes the plan of action for the research study. In other words, the research design is a plan of how to proceed. It describes what the researcher is going to do. The researcher has designed his plan in light of the qualitative approach (Cf. section 1.14).

2.7 DATA COLLECTION TECHNIQUES

The researcher has taken efforts to ensure that the critical issues of data collection are taken into consideration. According to Lumina (2006:102), a questionnaire is defined as a set of questions used to gather data from the participants and is designed specifically to attain the research objectives. In this study, the main data collection method used semi-structured, face-

to-face interviews with the participants. According to Ras (2015a; 2006, 2010; 2012a; 2012b), research methods are the specific procedures that are used to carry out research work. Through the use of various research methods, the researcher is able to identify the different phases of the research process which include, for example, data collection, the systematisation of the data, the processing of the data, and its explanation (Van der Walt *et al.,* 1982: 168-169). This study is not about the exposition of coding and the in-depth explanation of theories; it rather specifically discusses the heart of the issue for the study (Ras, 2006:76).

Briefly speaking, this researcher planned his activities to collect data for this study using. personal interviews, telephone interviews, focus group discussions, document analysis, literature review, and observations. The researcher conducted follow-up exercises whenever it was necessary to acquire further information or clarity for this study.

2.7.1 Personal interviews

Since interviews are one of the most commonly recognised forms of the qualitative research method (Mason, 2002: 62), the researcher used unstructured interviews as one of the data collection methods (Cf. Annexure J). The purpose of the interviews was to retrieve information concerning the feelings, viewpoints, beliefs, experiences and problems related to cable theft that the participants had brought up. Participants were approached and the purpose of the study was explained to them. No remuneration was offered and they were informed of the opportunity to withdraw at any stage of the research. Individuals who refused to participate were not coerced in any way. The interviews only commenced once the participants were comfortable and had no objections to the conducting of the interviews.

Through the interviewing method, people get an opportunity to share their beliefs, knowledge and reasoning, and researchers can discover their motivations, feelings, thoughts, experiences and ideas (Ras, 2014). Through this, one can make generalisations and also compare one's own experiences with that of the research participants. Interviews also allow for consequential interaction between researchers and participants (Babbie & Mouton, 2001: 278; McMillan & Schumacher, 2001: 269; McMillan & Schumacher, 2010). There are no fixed rules as to the ideal number of interviews. Some qualitative researchers believe that the more interviews one has, the more scientific and precise the research results are (Kvale, 1996: 103; Ras, 2015b).

All of the questions used by the researcher were open-ended and this encouraged the participants to analyse and explain issues relating to cable theft in their own unique way. The open-ended questions also stimulated the thinking capability of the participants and forced them to investigate their own ways of thinking about how the problem of cable theft can be resolved, even in Eskom's work environment.

2.7.2 Personal Conversations

Ronna (1969:4) concludes that personal distance is the most appropriate distance for casual conversation between two strangers placed in a situation encouraging verbal interaction. In the broadest terms, people would not probably come into close physical contact with people whom they consider socially distant. The researcher purposely opted for personal conversations with people related to cable theft in Eskom because this had not been done before. Personal conversations are much more informal, intimate and also reflect the views of people who normally would not have the opportunity to express themselves (Maseko, 2011). While the personal interviews were specially focused on cases related to cable theft, the personal conversations were broader and incorporated many more issues. While talking with people, they often mentioned some matters related directly or indirectly to cable theft, which the researcher has included in the research.

The researcher was very aware of the contents of section 16 (1)(b) of the Constitution of South Africa (1996) which prescribes that "Everyone has the right to freedom of expression which includes the freedom to receive or impart information" (South African Constitution, 1996: 9).

The researcher also made notes of the points, remarks, comments, and appraisals made by the participants – mostly after the conversations took place. Participants were allowed to express themselves freely and fully. The researcher believes that the more the participants participated, the more effective their contributions became, which had a great the impact on the development of this study.

The personal conversations conducted were held anywhere, for example at offices, homes, or at Eskom facilities (Cf. Annexures A11 – 13). The conversations allowed the researcher to ascertain the views and stories that the participants had to share on the research topic. Some conversations took longer than others because some of the participants had many years of experience working and investigating cable theft incidents. As soon as practicable after the

conversations took place, reflective field notes were made. Each time a new topic of conversation regarding cable theft was introduced, a change of subject was recorded. Most participants did not want to be recorded on tape, but chose to speak freely and engaged the researcher openly when they knew that they were not being recorded.

Ronna (1969:36) believes that conversation utilizes past, present, and future time orientations. If people feel personally involved in a situation, this attitude could be revealed by speaking more in the present tense than in the past or future tense. It is expected that conversants within an intimate space would feel more involved by their proximity to each other. A heavier use of present tense verbs is expected than in personal or social distance conversations. A declining use of the present tense is anticipated in personal distance; even fewer references are expected at social distance (Ronna, 1969:36).

2.7.3 Telephone interviews

Owing to the vast nature of this research, various methods were used to collect data. One method was the use of telephones and cellular phones. The use of telephones assisted the researcher to reach many people within a relatively short space of time and proved to be very cost effective for the researcher, as opposed to driving a vehicle or using an aeroplane to visit the participants. Also significant in this decision was the resource and logistical implications of extended national road travel in order to conduct more interviews. All the interviews lasted for a minimum of 10 minutes. As with the conversations, reflective interview notes were made as soon as practicable after the interviews were concluded.

According to Novick (2008), telephone interviews are largely neglected in qualitative research literature and, when discussed, they are often depicted as a less attractive alternative to face-to-face interviewing. The absence of visual signs via telephone is thought to result in loss of contextual and nonverbal data and to compromise rapport, probing, and interpretation of responses from the side of the researcher. Nevertheless, telephone conversations may allow participants to feel relaxed and become able to disclose sensitive information, and according to Novick (2008), evidence is lacking that they produce lower quality data.

Irvine (2010) says that telephone interviews offer a range of potential advantages for qualitative research projects. Most obviously, they remove the need for travel, thus reducing both time and cost. They also allow participants to remain more anonymous if desired, they

may feel less emotionally intense or intrusive, and there may be physical safety advantages for both researcher and participants.

It was important for the researcher to follow the same ethical guidelines to ensure informed consent as one would in conducting a face-to-face interview. Although the reduction in travel means that it was possible to do more interviews in less time, the researcher was aware of the temptation to fit too many interviews into one day. The researcher found that qualitative telephone interviewing requires just as much stamina and concentration as face-to-face interviewing does, if not more. The researcher also received calls from people who wanted to share their information on cable theft with him.

2.7.4 Group interviews

Where the researcher found it convenient, and it was agreed upon by the participants, group interviews and conversations were conducted. These were conducted especially in relation to the security operational meetings which were being held. At these meetings, the researcher had the opportunity to engage security managers, security investigators, and security operational staff (inspectors and security officers) of both Eskom and the private security sector (Cf. Annexure M).

At various external group meetings, the researcher interacted with other security specialists from other companies, including Telkom, Transnet and Spoornet. These interactive sessions exposed the researcher to more inputs from security industry experts working with copper theft and security preventative methods, than from normal individuals' perspectives.

The researcher also obtained valuable information relating to the situation of cable theft at the various companies and to insights which might establish whether the preventative measures applied at those companies were successful. The researcher was able to probe the situation of the private security companies working for other large businesses in South Africa and to establish if those companies had been able to prevent asset thefts at those businesses. All the group discussions lasted for a minimum of one (1) hour. As soon as practicable after the discussions were concluded, reflective interview notes were made.

2.7.5 Document analysis

Documentary studies were conducted for this research. The examination of documentary evidence provides a method to cross-validate information gathered from interviews and

observations, given that sometimes what people say may be different from what people do (Noor, 2008: 1604). Additionally, documents provide guidelines in assisting the researcher with the inquiries during the interviews.

The researcher had to request the official documents and statistics on cable theft before the commencement of the study, as participating departments might have been unwilling to share these documents. Ethically, the researcher also had to negotiate with the senior manager of Eskom group security for permission to access the statistics of the past twelve months to validate the data retrieved in the interviews and observations. The researcher assured the senior manager, Mr Martin Strauss,[ii] of confidentiality when working and presenting the statistics in the study. According to McMillan and Schumacher (2010:321-322), "document analysis describes functions and values and how various people define the organisation." Applicable to this research, Eskom's internal documents have also assisted the researcher to better comprehend Eskom's internal processes so as to better understand this argumentation dealing with copper theft.

The document analysis provided the researcher with very important sources of information and showed the high number of thefts of copper cables from Eskom (McMillan & Schumacher, 2010: 321). The researcher used document analysis to complement the observations and interviews, thereby ensuring accountability and consistency. However, it was imperative for the researcher to consider the validity, reliability and authenticity of the documents before they could be used in the research study. The main documents that the researcher used in this research study were as follows:

- Crime stats ENECC report (Eskom Network Equipment Crime Committee) for Eskom's national conductor theft for the period 2013–2014 and 2014–2015.
- Investigation reports for conductor theft incidents
- Eskom internal fatality reports for security officers killed on duty
- Eskom security contract documents
- Non-conformance reports issued to private security companies contracted to Eskom
- Integration of the Group Security Sustainability Division Operational Plan 2013/16 (Unique Identifier 240-56629733).

The researcher studied the official documents for reasons of confirming reliability, validity and authenticity. In addition, through a close examination of the documents, the researcher was able to explore the high number of thefts and to look at some of the subsequent actions by Eskom security to find solutions to the high rate of thefts from Eskom. Ultimately, the documents were used to establish accountability within Eskom security for the high numbers of cable thefts from the Eskom facilities, which at most times are secured by private security companies contracted to Eskom.

Further scrutiny was made of the crime statistics ENECC report (Eskom Network Equipment Crime Committee) (see section 6.9) for details of thefts of Eskom's national conductors for the period 2013–2014 and 2014–2015. Also scrutinised were investigation reports for cable theft incidents and the Eskom internal fatality reports for private contract security officers killed on duty.

The use of field notes, brochures and other relevant documents also formed a crucial record of reference for the researcher during the data collection process, interpretation and analysis. The term "field notes" refers to cryptic or skeleton notes that the researcher had made to refresh his memory on what someone had said about a particular issue of policing, or possibly what he had seen or had experienced. These field notes are a record of peculiar sayings, names of places, and other remarks made during the data collection trips (Ras, 2006: 95; Maseko, 2011).

These field notes include details of:

(a) The location of the interviews or conversations, as well as the person, institution or organisation (representative) being interviewed,

(b) The date of the interviews or conversations,

(c) The background information about the participants, and the immediate observations of the researcher of the situation surrounding the discussion, and

(d) An indication of whether sufficient information had been obtained (Saunders *et al*., 2007: 326- 327; Maseko, 2011).

All electronic correspondence that the researcher had, like emails (sent, received), were regarded as part of the document studies analysis because such correspondence is nothing

else than electronic documents containing research data information constitute electronic equivalents of physical documents (Ras, 2006).

2.7.5.1 Literature review

A literature study was conducted to accommodate the qualitative research approach (Fouché & Delport, 2011: 134). It was used to formulate the rationale for the study, the problem statement, the research questions and the research objectives. The research questions were, in turn, used to formulate questions for the interviews and group studies.

A literature review forms a distinctly recognisable section near the beginning of a study and leads on to the more specific and practical description of the research activities (Walliman, 2011: 56). Literature review entails locating and summarising the existing studies on a topic. The use of literature varies considerably, depending on the particular research being conducted. There is no single way to conduct a literature review. Gray (2009: 133) further elaborates to advise that literature will identify who are the dominant and influential writers in the field. In this study, the researcher conducted a literature review before the commencement of the study, during the title choice, when formulating the research questions, and to validate statements.

The researcher searched through different fields of study and areas of interest, such as law, criminology, policing, private security, the media in South Africa and abroad, security services, the method of investigation of copper theft cases by Eskom internal investigators, private security companies contracted to Eskom, and SAPS investigations on cable theft. The researcher also consulted with relevant persons in the South African private security industry, with metal theft experts in the United Kingdom (UK), scrap metal association (SA) and the SAPS for literature on the same topic as a basis for the research. The researcher studied the relevant literature to search for best practices in the national and international arena.

2.7.5.2 Photographs

The researcher has also attached some photos to the study in order to present the reader with some relevant historical background (Cf. Annexures A23 – A31), crime incident photos (Cf. Annexures A19 – A22), Eskom asset and cable specifications (Cf. Annexures B15- B31) and matters relevant to this research (Ras, 2014a).

2.7.5.3 Field visits to Eskom facilities

Eskom facilities are situated all over South Africa (see section 4.5). Time and resource constraints did not permit site visits to all Eskom facilities. However, the researcher visited some of Eskom's facilities in KwaZulu-Natal and Gauteng for this research study.

Field visits were supported by the taking of comprehensive notes and photographs, which documented pertinent elements of security and cable theft. Overall, with each Eskom facility being a significant part of Eskom's infra-structure, and having been so for a considerable period of time, it was considered vital for the researcher to form an opinion on the way security is being deployed and the manner in which they protect Eskom's cables on site.

The field notes recorded impressions such as the performance of security personnel on site; the way they were being managed, the manner in which the cables are safeguarded, and the seriousness of the attitude of security personnel on site. The photographs supported these notes and recorded the visits, and also provided a significant source of visual data. Selected photographs are included below (Cf. Annexure A11). The researcher's experiences were that these interviews were very fruitful, definitely useful, and provided very up-to-date, precise and reliable information.

2.7.6 Observations

Marshall and Rossman (2006:107) say that observation entails "the systematic noting and recording of events, behaviours and artefacts (objects) in a social setting chosen for the study". During the non-participant observations, the researcher did not influence the behaviour of the people under observation. Moreover, the observations were done using an observation guide (Cf. Annexure N) and the researcher recorded the actual activities taking place at the research sites. As Corbin and Strauss (2008:29) put it, observations are important because "it is not unusual for persons to say they are doing one thing but in reality they are doing something else". The only way to verify this is through observation. People may also not be consciously aware of, or be able to articulate, "the subtleties of what goes on in interactions between themselves and others" (Corbin & Straus, 2008:30).

Within this research, the researcher was able to engage in observation study. In this, the researcher visited the natural setting (Eskom premises where private security officers are deployed) to observe how the private security officers go about protecting Eskom assets

(copper cables) and to see how Eskom takes measures to protect its assets (the copper cables). The observation method used here is considered vital to the study as it added significant depth to the research study.

The researcher explained to the security officers and Eskom site supervisors that he was patrolling on site as an observer as part of his research study. Importantly, the researcher was able to explore and examine their thinking processes and their actions during the security patrols. The researcher further explained to the security officers that it was advantageous for him to use observations in the research as he would be able to observe how they (the security officers) go about protecting Eskom's assets.

The researcher explained to the security officers that they should not be hindered by his presence but should carry on with executing their duties and role functions as normal. The researcher observed the way the security officers were going about their daily duties in their efforts to protect Eskom assets (copper cables). It was important for the researcher to understand how security officers viewed the value of Eskom assets and to understand how important it was to them to ensure that the assets are well protected. Moreover, the researcher was able to build good relationships with the security officers and Eskom employees.

In due course, the researcher was able to gain an understanding of how security is being managed on site and how the security personnel are being supervised and motivated to ensure that Eskom assets are being protected. The researcher took down notes and had to further decide what was important; and what data should be recorded. The researcher kept a detailed and accurate record of the field notes which included all the activities, conversations and decisions.

The researcher was able to understand why the security officers fail to protect Eskom assets and what needs to be done by Eskom to improve security and prevent losses from Eskom facilities. The field notes served to supplement the data collected from the interviews and documentary research. The field notes served as sources of data of the evidence of what actually took place during site inspections.

2.7.7 The use of tropes

Tropes refer, for example, to stories, metaphors, anecdotes and jokes (Ras, 2006:96; 2010:79-81). When people are trained to perform a specific function, whether administratively or operationally, instructors very often train their students through linguistic devices that are

called *tropes* (Crank, 1996). Through these institutional argumentation stories (Ras, 2006:96; Ras, 2010:79-81), people remember what they must do and learn quickly about their particular occupations (Crank, 1996). Tropes comprise not only a training technique for memory enhancement, but are definitely without a doubt rich descriptions of data can be collected from participants like security guards and knowledgeable persons about what is going on, in this case, about cable theft (Cf. Ras, 2006:96; Ras, 2010:79-81; Crank, 1996).

Cable thieves are undeterred by previous incidents were people were killed while trying to steal copper cables that are "live". They ignore warning signs that advise them of the dangers of live copper cables and the fact that security systems are in place and that guards are on duty. To be more precise, people learn about "the culture" in which they are going to work (Ras, 2006:96; 2010:79-81). Security officers are trained in a specific manner, and "tropes" are used, inter alia, to explain to members what is expected from them and how they must behave (Ras, 2006:96; 2010:79-81).

Ras (2006:96; 2010:79-81) says the importance of tropes is that they grab the imagination of people because they deal with the "imaginative", and in that sense, they "stick" or "glue" to the listener. The reason for tropes (narratives/stories) will vary, but it might be, for example, to inform, instruct, persuade, to illustrate some idea or to stir the imagination (Ras, 2006:96; 2010:79-81).

2.8 POPULATION AND SAMPLING

The researcher decided to choose the security officials that had knowledge of cable theft from Eskom in South Africa as the study population for this research. 'Population' is a term used is setting boundaries for the study units. It refers to individuals in the universe who possess specific characteristics (Akrava & Lane, 1983: 27). The population itself was too large to study. It was therefore divided into a representative sample (Powers *et al*., 1985: 235). According to Hinds (2008:59), sampling is defined as the identification of a subset of a larger population. In this study sampling means the act, process, or technique of selecting a suitable and representative subset of a population for the purpose of determining the characteristics of the whole population. The meaning of the population in this study is the set of all items that could be sampled. However, according to Lumina (2006:99), the population of any research is defined as the total group of people from whom the information is drawn. Sampling is used

to obtain a representation from the population, as it is often too expensive and time-consuming to include the whole population in a research study (Wiid & Diggines, 2013:188).

According to Steyn (2002: 71), the results of a research study can be generalised to groups that participated in the research study. The results need not be generalised to the private security industry in general. The aim of the researcher was to study a representative number of people and to generalise the findings to Eskom and the security companies contracted to Eskom, and not to generalise the findings to the security industry nationally.

2.8.1 Participants of the Study

For this study, the researcher chose participants that would be able to supply information and validate the different remarks/opinions which emerged during the literature review, focus group discussions and documentary study conducted for the study. This process was done to allow the researcher to gain an understanding of the cable theft problem at Eskom and to establish what needs to be done to prevent this from happening. The participants in the research are all involved in one way or the other in their respective work environments in combatting cable theft. Fifty-five (55) participants were randomly chosen (see section 5.8) and comprised the following different security categories of people:

Table 2-1: Participants in the study

1	Eskom Security (ES)	14
2	Industry Security Directors (ISD)	6
3	Industry Security Specialists (ISS)	6
4	Contract Security Managers (CSM)	8
5	Contract Security Supervisors (CSS)	6
6	Contract Security Guards (CSG)	15
	Total participants	55

2.8.2 The sample for this study

The participants (see section 2.8.1), i.e. security managers (both Eskom employees and private security), security officers, private security company and Eskom inspectors, Eskom investigators, Eskom technical staff and industry security managers, were all important to the study as they were each chosen for a specific purpose. Furthermore, all the participants that were chosen were knowledgeable in a specific area of concern and possessed an in-depth understanding of cable theft. Moreover, they possessed the necessary information in regards to the chosen area of investigation, namely cable theft.

2.8.3 Gaining access to the participants

Before any items of data were collected, access was gained by seeking the written permission of Eskom for the researcher to conduct the research (McMillan & Schumacher, 1993:195; See Annexure K, permission letter). The permission of participants for the study was sought from each of them directly, and not through third parties, in order to enhance the voluntary nature of their participation. The aims of the research and what was expected of the potential participants were clearly communicated to them (Marshall & Rossman, 2011:47-48).

Practical aspects of the research, such as data collection methods and recording of data, were discussed with the potential participants in detail (Marshall & Rossman, 2011:47-48). If at any stage of the interview they were uncomfortable with any aspect of the research procedures or questions, they were free to discuss the matter with the researcher, or even to decline to participate.

2.8.4 Sampling Method

The researcher applied the probability sampling method to select the participants for the study. In the case of probability sampling, it can be determined what the probability will be that any element or member of the population will be included in the sample (Welman, Kruger & Mitchell, 2005:69).

For purposes of ensuring that this study would be valid, the researcher wrote down the names of all the people involved with security management and cable theft investigations for Eskom and placed them in six non-transparent bags and labelled according to their job titles. These were Eskom Security personnel, Industry Security Directors, Industry Security Specialists, Contract Security Managers, Contract Security Supervisors and Contract Security Guards.

These participant selections were based on the criteria that they had been involved with security at Eskom and the protection of Eskom's cables for more than a period of five years and were thus knowledgeable and informative about the area of interest in this study, were registered with the Private Security Industry Regulatory Authority (PSIRA), and were willing to participate and contribute to this study. The researcher did not write down the names of participants if they did not meet this criterion.

The researcher then selected samples (14-Eskom Security personnel, 6-Industry Security Directors, 6-Industry Security Specialists, 8-Contract Security Managers, 6-Contract Security Supervisors and 15-Contract Security Guards) from each bag according to the labels to reach the number of fifty-five (55) from this population group.

Dawson (2002:47) says that in qualitative research, it is believed that if the sample is chosen carefully using the correct procedure, then it is possible to generalise the results to the whole research population. All the participants involved in the study were part of the population involved with security management and cable theft at Eskom.

2.9 DATA ANALYSIS AND PRESENTATION

The researcher has used all the gathered data and has endeavoured to present it in as systematic manner as far as possible. Qualitative data analysis transforms data into findings. It brings order, structure and meaning to the mass of collected data (Patton, 2002: 432). According to Corbin and Strauss (2008:480), analysis makes the content interpretable. According to Struwig and Stead (2007:169), data analysis in qualitative research is a process of gathering, modelling and transforming data with the goal of highlighting useful information, suggesting conclusions and supporting decision-making. Data analysis has multiple facets and approaches, encompassing diverse techniques under a variety of names, in wide-ranging business, science and social science domains.

2.9.1 Coding and categorising the data for the interviews

All the data collected during the research was collated, prioritised, clustered in groups or information categories/themes, and interpreted to make sense. The data generated during the interviews were transcribed (transformed into written text). The researcher then organised the data in the form of a table, where the relevant questions from the instruments appeared in the first column, the participant's responses to the questions in the second column, and general

comments were written in the third column. Patterns, trends and themes emerged from the research process, and the role of the researcher was to be able to understand these real-life situations from the point of view of the insider, rather than from that of the outsider. A coding system was then applied to the themes and categories to display the relationships among them, at which point the researcher assigned a code as a form of identification after grouping the similar categories and patterns (Van de Sande & Schwartz, 2011:122). Marshall and Rossman (2011:105) say that coding data is the formal representation of analytic thinking.

2.9.2 Identifying themes and emerging explanations

According to Zhang and Wildemuth (2005:3), an instance of a theme might be expressed in a single word, a phrase, a sentence, a paragraph, or an entire document. When using a theme as a coding unit, the researcher was primarily looking for the expressions of an idea. Themes are common trends or ideas that appear repeatedly throughout the data. The researcher interpreted these themes to bring meaning and coherence to the themes, patterns and categories. According to Patton (2002:480), interpretation means attaching significance to what was found, making sense of the findings, offering explanations, drawing conclusions, extrapolating lessons, making inferences, considering meanings, and otherwise imposing order. Part of this phase is evaluating the data for its usefulness and centrality (Marshall & Rossman, 2006:162).

2.9.3 Presenting the data

The researcher read thoroughly through all the data collected for the study and presented the results in a descriptive or narrative form, which was also supported by direct quotations from the raw data. Berg (2007:3) says that qualitative research refers to the meanings, concepts, definitions, characteristics, metaphors, symbols, and descriptions of things. The numbers, or numerical descriptions of things and their relationships, are not the focus of this qualitative research: that comprises the focus of the "other" form of social science research – the quantitative method. The researcher utilised elementary data statistics to represent the percentages of participants that *"Agree", "Disagree"* or are *"Unsure"* with the security statements discussed. The data was presented using tables (See Chapters Five and Six). The researcher used XL spreadsheets for the retrieval, evaluation and presentation of the data, which is an indication that the researcher has tried his best to be as relevant and recent, and as innovative, as possible so as to be in line with national and international study standards.

2.9.4 Observations, documents and personal conversations

As discussed in section 2.7, the researcher used observations, documents, and personal conversations to generate data. In doing so, the researcher had to constantly revise the data during the field work until the researcher was sure that he had enough information for the study. Once that was completed, the researcher transcribed the data from the observation checklist**,** typed the field notes, summarised the findings from the documents, and then stored the information inside the folders which were created on a computer. By reading through the data and reflecting on it, the researcher was able to interpret themes to bring meaning and coherence to the themes, patterns and categories.

2.10 DATA SATURATION

Nieuwenhuis (2012:79) says that data saturation is the point in data collection when new data no longer brings additional insights to the research question The researcher selected an appropriate sample consisting of participants who best represented, or had knowledge of, the research topic.

2.11 THE DANGER OF BECOMING A 'FIELD WORK JUNKIE'

Ras (2006: 108-109; 2010:83; 2012:83) warns of the danger faced by qualitative researchers that they can easily become 'fieldwork junkies'. Ras (2006:108-109; 2010:83; 2012:83) describes a 'fieldwork junkie' as someone who is suffering from the 'one-more-interview syndrome' and advises that it is the quality of the gathered data that counts, and not the quantity of how many people were interviewed, that is decisive.

In terms of this research, because the researcher endeavoured to 'immerse' himself in all relevant information, he was thus able to obtain relevant and sufficient data on Eskom's cable theft problem. He then has made a decision that if the gathered data did not bring any more new information to the fore, then he would not need to continue to undertake further interviews. By doing so, he avoided to become a fieldwork junkie himself.

2.12 PERSONAL INVOLVEMENT IN THE RESEARCH

The study is based on exploring an *Investigation towards the prevention of cable theft from Eskom*, which investigates and explores the problem of cable theft at Eskom and endeavours

to understand why cable theft occurs, notwithstanding that Eskom has deployed security officers to prevent it.

The researcher was able to draw on his 20 years of experience working in the security and investigations environment. Included in the 20 years of functional experience, 17 years were in the corporate section (Telkom and Eskom, respectively). The researcher worked at Chubb Alarms from 1993 to 1998 as an armed response officer and shift supervisor. The duties included armed response call-outs to businesses and residential premises, conducting in-depth evaluations to determine risk profiles of properties, first line investigations, and follow-up actions to these investigations.

On 01 October 1998, the researcher was employed as a Security Accounts Manager at Telkom's Asset and Revenue Protection Service Department (TARPS) and thereafter moved to the investigation division to work as a forensic investigator, working with the cable theft and network fraud division. The researcher was deployed to many different regions during his 11 years of employment at Telkom. The researcher was a recipient of two 'names in lights awards' from Telkom SA (See Annexure E). This initiative highlights the hard work and commitment displayed by an employee. The researcher was also appointed in an acting capacity as the regional security manager in Kwa-Zulu Natal (KZN) on many different periods during his employment at Telkom.

The researcher's main responsibilities included: preparing the overall security plan; managing the security operations of the organisations; site assessment planning and staffing; directing the investigations of fraud, theft and unlawful activities; providing timely reports to the senior management; managing all the security costs and budgets through financial analysis and contract negotiation; maintaining and conducting routine inspections of several facilities and analysing problem areas; monitoring the performance of the security systems at the facilities in the region and reporting the problems to the internal clients; researching the security market constantly to gain knowledge of the latest trends in security system implementation and possible security threats; recommending installations of new/latest security systems or a possible upgrading of the existing systems; and conducting annual research on crime risk analyses for the facilities in the region, in the light of prevailing crime rates present in the specific areas.

The researcher was also part of the elite VIP Protection Unit responsible for body guarding several of Telkom SA's dignitaries, including the CEO and many other top executives. The

researcher was also part of the National Cable Theft Task Team which was deployed to many provinces in South Africa, working with cable theft regional teams (which included the SAPS and clients ("victims") of cable theft.

On 01 May 2009, the researcher commenced employment as an Area Officer for Eskom and was responsible for the management of security contractors within the Eastern Region (KZN). The researcher worked in this position from the 1 May 2009 to 1 February 2013. The researcher's duties did not differ much from the main responsibilities at Telkom. During the researcher's employment as an Area Officer, the researcher was part of the National Study Group (NSG) for Distribution, working on security policies and safety procedures. The researcher also acted in the position of Regional Security Manager KZN on different occasions with full authority (delegation) powers to sign and approve security matters.

On 1 February 2013, the researcher was promoted to managerial level of Eskom as a Senior Advisor for Eskom's Group Security. The researcher's post description included being regarded as a business partner to the Generation Division, and because security is regarded as mandatory by Eskom, the duties included working in an advisory capacity to ensure compliance with security legislation.

The duties included providing an advisory service on legislative compliance issues to the Generation security environment and conducting pre-audits on all the Generation facilities, which included Koeberg Nuclear Power Station in Cape Town. During November 2013, the researcher was reassigned to the Transmission Division where he is currently working as a business partner to ensure legislative compliance (amongst other duties) in the security division.

The researcher is also part of the national cable task team. The researcher was assigned to this division based on this research study and the experiences that he had accumulated while busy with cable theft investigations.

The researcher completed his Master's Degree in Security Management at UNISA in 2014 (Govender, 2014, "*A case study of factors contributing to discipline problems of security officers: Eskom distribution centres, KwaZulu-Natal North Coast region*") (See Annexure F). In 2010 he completed the one-year Security Risk Management IV programme (SRM 401 S) module with UNISA.

In 2012 he completed a security advisory programme (NQF level 6) with the South African National Academy of Intelligence (SANAI), previously known as NIA (National Intelligence Agency). Today they are called the State Security Agency (SSA). In 2007 he obtained a Batchelor's Degree in Forensic Investigation from UNISA (See Annexure G). In 2005 he obtained a Diploma in Forensic Investigation and Criminal Justice from the University of Johannesburg (UJ).

In 2001 he received a Diploma in General Management from Intec College and in 2000 received a Higher Diploma in Commerce (Labour Relations) from Intec College. In 2000, he completed a one-year certificate course in Security Management from Intec College.

The researcher completed the following training programmes as part of his career development: Technical Report Writing (In-site Training, 2006); Forensic Interviewing (NQF level 5) (Mega Plan, 2006); Advance Security Management (Pretoria Technikon, 2003) (See Annexure H); Initiating Disciplinary Hearing (Telkom, 2001); Training course with IBO data in Johannesburg, which entailed the operation and programming and developing of ID cards on the mobile ID card system; A Security Instructors course from 10/04/2000 to 16/05/2000 with Ishikova Security Training Academy in KZN.

The researcher completed the following courses: Occupational Health and Safety course at Telkom Centre for Learning (2000); Investigation Course (Spoornet Training Academy, 1999); SAPS training and Swat Course held with the Internal Stability Unit in Tongaat (KZN) from 1993-04-18/19 to 1993-04-22/23 (See Annexure I); Management competency course Telkom Centre for Learning (CFL); Advanced driving and 4x4 driving course with Advance Driving Academy, together with an advance-driving course at Pinetown (KZN); and a course on Selection Criteria for interviewing (Deloitte Training Academy). The researcher has attended various other courses related to safety at Eskom, which is logged on Eskom's internal management system. The researcher has also attended various management and safety related courses during the 11 years spent at Telkom SA. The researcher is registered as a Grade A security officer with PSIRA (See Annexure D).

The researcher has acquired the following important key skills and core competencies (amongst others) during his current career: motivating and directing people; agile thinking and attention to detail; in-depth knowledge and understanding of security legislation; ability to handle confidential information (the researcher has a security clearance certificate (secret)

from the State Security Agency 'SSA'); able to work independently and as a team member; knowledge of the security environment and related hazards and strong problem solving skills.

During the researcher's time at both Telkom and Eskom, he attended numerous regional and national cable theft meetings, seminars and focus group discussions on cable theft. These meetings were also attended by clients that had become victims of cable theft (in some instances) and by both Eskom and Telkom security divisions.

The researcher had a strong belief that this research was important, that it needed to be done, and that his experiences could provide a valuable perspective and fill gaps in the literature about copper cable theft at Eskom and in South Africa. All the above-mentioned qualifications and experiences have prepared the researcher to better comprehend the extent of cable theft and to be able to present action plans to prevent further incidents of cable theft.

2.13 RESEARCH DELIMITATION

Eskom has three main lines of business in South Africa, namely Generation, Transmission and Distribution (Eskom, 2014) and is one of the largest employers and buyers of goods and services in the country. In addition to the over 40 000 people that Eskom employs directly, its suppliers employ an even larger number of people whose jobs are indirectly attributable to Eskom's activities (Eskom factor, 2014).

Private security companies are deployed to Eskom facilities to prevent asset theft (Eskom copper cables included). In certain facilities of Eskom, the private security companies are deployed together with Eskom's in-house security personnel.

This study was confined to the problems of cable theft from the three main line facilities of Eskom's business where private security personnel are deployed, but the focus was on cable theft from Eskom from within its premises (see section 3.1). Although Eskom has partners in the prevention of cable theft (see section 3.8), they are not legally or contractually responsible to prevent cable theft from Eskom, whereas only the private security contractors are, and this is why this study is only focused, inter alia, on what security guards and management must do to prevent cable theft from Eskom. The private security personnel interviewed personally by the researcher for the study were only those in KwaZulu-Natal. Telephonic and email interviews were undertaken with people outside Kwa-Zulu-Natal, but within the borders of South Africa.

2.14 VALUE OF THE RESEARCH

Eskom is a critical and strategic contributor to the government's performance in providing the country's citizens with a secure supply of electricity. In pursuing its mandate, Eskom's purpose is to provide sustainable electricity solutions to grow the economy and improve the quality of life of the people in South Africa and the region (The Eskom Factor, 2014). One of the ways Eskom can achieve its mandate is to prevent cable theft and divert the money being spent on cable theft to expand its network.

The financial benefit accruing from Eskom's experiencing no cable theft losses would allow Eskom to become financially strong and would allow the utility to spend millions more on capital projects to provide more people with electricity. This would also mean that more people would be employed by Eskom to cater for the increase in Eskom's network coverage, thereby increasing the number of people participating in the economy. Eskom would also borrow less money to fund its operations and would be able to divert the money saved from the interest on those loans to areas where people desperately need access to electricity (Eskom, 2014; http://www.eskom.co.za/AboutElectricity/ElectricityTechnologies/Pages/Understanding_Electricity.aspx).

The findings and recommendations of this research study will benefit Eskom and other businesses that operate in South Africa and abroad that are also victims of cable theft and use private security officials to safeguard their assets. The security companies will benefit through this research in terms of acquiring knowledge, skills and attitudes to protect their clients' facilities and businesses while Eskom will benefit from a much safer and more secure environment.

2.15 VALIDITY

Validity has to do with the question of the research that has been done was valid or not. The researcher applied the methods described by Bouma and Ling (2004:83) in this section to ensure validity. The problem of validity is most acute in the construction of questionnaires or interview schedules to measure persons' attitudes, beliefs or values. Validity is considered to be present in research when the measuring instrument accurately represents what it is supposed to measure (De Vos *et al.*, 2005:162). This relates to the accuracy with which the information is gathered, asked and interpreted. Validity of the research instrument was

evaluated for its content, especially, although face and construct validity were also kept in mind.

2.15.1 Content validity

The content validity of the questions asked was determined by the literature review, as well as by the researcher's own experience while working in the security environment. All the questions posed to the participants were relevant to the study, thereby ensuring validity. The literature used in the research was also considered to be valid, because it consisted of subject-specific books, journals, articles and other sources, thereby ensuring validity (Mouton, 2001:101).

All the questions asked, the data collected, and the explanations received from the sample and experts were considered to be relevant to the topic, specifically to ensure that the research would be valid. Because the researcher endeavoured to measure the proceedings in a natural environment, interruptions had been minimised. The participants were encouraged to also act naturally, as far as was possible.

2.15.2 Face validity

Face validity refers to the extent of the research instrument and what it intends to achieve. The interview questions were designed and decided on, after considering Eskom's activities, duties and security issues (Welman & Kruger, 2005:174).

2.15.3 Construct validity

Construct validity is more concerned with the underlying attributes of the results of the interviewing questions. The question of validity in itself was convergent with the way the researcher has done self-reflection, both explicitly and implicitly, about the inquiry conducted (Marshall & Rossman, 2011:42).

2.16 RELIABILITY

Reliability relates to the credibility of the findings of a particular research study (Welman & Kruger, 2005:145). According to De Vos *et al.* (2005:162-163), reliability refers to the consistency of the measurement, which means that every time the same variable is measured under different conditions, it will still provide the same or similar results. The researcher

needed to determine whether the evidence gathered would stand up to scrutiny. The literature used in this research relates to the research questions, and is therefore reliable.

The researcher has used purposive sampling or convenient sampling, to select the participants of this study. The researcher selected the sample participants from people who were attached to Eskom, by working as contract security officers, contract consultants, or as permanent staff at Eskom KZN, or as security professionals in the security industry. The items of evidence ("observed through what the researcher and others has 'heard. and 'seen' and 'experienced'") were clearly indicative of the real security challenges and what needs to be done to prevent cable theft. If a research finding can be repeated by another researcher and achieve the same results, the research can be considered reliable (Welman & Kruger, 2005:145).

2.17 ETHICAL CONSIDERATIONS

Important matters relating to research ethics include obtaining informed consent and ensuring the right to privacy and protection of participants from harm, be it physical, psychological or social (Bogdan & Biklen, 1992:515). Ethics are moral principles and rules of conduct dealing with what is right and what is wrong (De Vos *et al*., 2005:57).

There were a number of ethical issues that were adhered to in this study. The researcher adhered to correct ethical behaviour, guided by the Constitution of the Republic of South Africa, 1996, when dealing with people.

These included (a) obtaining permission from the Senior Manager of Group Security in Eskom; ensuring that only voluntary participants took part; (b) undertaking to treat all information received as confidential by protecting the identity of participants who declined to have their information disclosed; (c) not identifying the participating Eskom sites; and (d) not divulging Eskom's confidential documents. The compliance with ethics in any research is aimed at ensuring that no individual will be subjected to any harm as a result of the research.

All participants were informed about the goals, objectives and purpose for the study and what it set out to achieve. Participants were informed and reminded throughout the study that their participation was voluntary (Cf. Annexure L). The researcher ensured that the appropriate confidentiality procedures were implemented (where this was required). On the 17 November

2015[5] the university ethics committee considered and approved a condonation request for the ethical clearance certificate for the study because the study was already completed and Eskom had provided permission for the study prior to the commencement of the study (Cf. Annexure K).

All findings were formulated in a complete and honest fashion, without misrepresenting what had been done or intentionally misleading others as to the nature of the findings (Leedy & Ormrod, 2004: 107-108).

2.18 SUMMARY

This chapter focused on research methodology. The following matters were discussed: Introductory remarks were made (see section 2.1), the reason for the present research (see section 2.2), research approach (see section 2.3), reasons for using the qualitative approach (see Section 2.4), the pragmatic research approach (see section 2.5), research design (see section 2.6), data collection methods (see section 2.7), population and sampling (see section 2.8), data analysis (see section 2.9), data saturation (see section 2.10), the dangers of becoming a fieldwork junkie (see section 2.11), personal involvement in research (see section 2.12), research delamination (see section 2.13), value of the research (see section 2.14), validity (see section 2.15), reliability (see section 2.16), and finally, ethical considerations (see section 2.17).

[5] The researcher was notified in writing on the 19 April 2016

CHAPTER THREE
THE EXTENT OF CABLE THEFT AT ESKOM

3.1 INTRODUCTION

The electricity market in South Africa is regulated by National Energy Regulatory South Africa (NERSA) in terms of the National Energy Regulatory Act, 2004. NERSA issues licences, regulates all tariff increases and provides national grid codes. Eskom is South Africa's national electricity utility company that produces approximately 40 000 megawatts of electricity every year to industrial, commercial, agricultural, and residential customers, as well as to redistributors (municipalities) under a licence agreement that in turn redistribute electricity to businesses and households within their areas (Eskom, 2014).

Eskom's function is to generate (Generation business unit), transmit (Transmission business unit) and distribute electricity (Distribution business unit) (Eskom, 2014). Eskom generates approximately 95 % of the electricity used in South Africa and approximately 45 % of the electricity used in Africa. Eskom operates 23 power stations with a total nominal capacity of 42 090MW, comprising 35 721MW of coal-fired stations, 1 860MW of nuclear power, 2 409MW of gas-fired, 600MW of hydro, and 1 400MW from pumped storage stations, together with the 100MW Sere Wind Farm. Eskom is in the process of constructing new power stations (See Section 4.9.1 – 3) and high voltage power lines to meet South Africa's growing energy demand which are expected to be completed by 2021(Eskom, 2014).

The high number of recorded cable theft losses is a clear indication that Eskom is one of the major "victims" in the copper theft onslaught in South Africa (Makubu, 2013). Resources that could have been used to expand infrastructure now have to be used to repair damaged services, which in economic terms, and in terms of service delivery mandates, results in the continued deprivation of basic services to outlying areas. Eskom further experiences cable theft from its premises which at most times are guarded by security guards with physical and electronic security aids such as fences, CCTV surveillance and alarms.

For the purposes of this chapter, cable theft is categorised in two ways: i) the theft of copper cable from Eskom's open network lines outside its premises; and (ii) the theft of copper cables from within its premises (protected by security officers). This chapter is concerned with the particular problem of cable theft from Eskom within its premises. This chapter has

focused on the extent of cable theft, in particular the harmful consequences and losses it generates for Eskom.

3.2 WHY IS ESKOM COPPER CABLES PREFERRED TO ALUMINIUM CABLES?

When considering cable theft from Eskom, a distinction can be made between thefts of copper cables and aluminium cables that are in use as part of the network, such as overhead cables, cables found in the High Voltage (HV) yards (known as 'live' cable), and theft of other cables, such as cable found abandoned after a project, or cables found stored at Eskom premises. The classification of a 'live' cable does require the cable to be carrying electric currents at all times.

Although Eskom experiences cable theft of both copper and aluminium cables, copper cables are targeted 95 per cent more than aluminium cables because copper is approximately twice the weight as aluminium with the equivalent conductivity. The weight of copper, coupled with its value, is the main driver for this specific cable theft (ENECC report, See Section 6.8).

On 26 January 2015 the researcher conducted a short survey by contacting five scrap metal dealers in South Africa to confirm the prices they are currently paying for copper cables and aluminium cables. The copper prices per kilogram ranged from R37.62 to R56. 43. The scrap dealers advised the researcher that these prices will depend on the grade and quality of the copper, stripped from the PVC casing or still in its original form, and if the colour is shinny or dull. The dealers advised that more money is paid if the copper is stripped and shiny. The aluminium prices for cables ranged from R9.69 to R16.13 per kilogram. According to them, the high price paid for copper is the main reason why copper cables are preferred and stolen more often than aluminium cables are.

Whyte (2004) says that the London Metals Exchange prices for copper and aluminium dictate the type of conductor that is most cost effective at any particular time. Whyte (2004) confirms that Eskom has standardised on using copper conductors for the following reasons:

- to minimise the stockholding requirements to cater for both types of cable (example. lugs, ferrules, cable, etcetera);

- the core and outer diameters of a copper conductor cable are smaller for equivalent ampacity than an aluminium conductor cable, facilitating easier working when jointing and terminating;
- conductor jointing using compression methods are simple for copper conductors, whereas there are numerous differing opinions regarding the crimping requirements for aluminium cables; and
- to avoid the bimetallic corrosion problems associated with termination and jointing of aluminium cables (example brass or copper terminals on equipment) (Whyte, 2004).

3.3 SOME OF THE REASONS WHY CABLE THEFT HAS INCREASED AT ESKOM?

The researcher believes that it is relevant to point out some of the reasons why cable theft has increased at Eskom:

3.3.1 High price of copper

In an article by Ndlovu and Magwaza (2008; http://www.iol.co.za/news/south-africa/metal-theft-is-crippling-industry-1.409566) Andrew Etzinger, an Eskom spokesperson, said that copper cable theft was an ongoing problem for Eskom. He added that an increase had been noticed which was costing Eskom 25 million rand a year. He attributed the increase in this crime to the high price of copper and depressed economic situations. Etzinger indicated that Eskom had seen a steady increase, from 446 incidents in 2005 to 1 059 indicated in 2007, and to 1 914 indicated in 2008, and according to him, it was going to increase (Pretorius, 2012).

John Cross, chairman of the Copper Producers' Association, stated: "The consistently high price of copper makes it a valuable commodity for illicit business, and what drives the price up is massive demand from China and India, whose urbanising economies are voracious consumers of copper" (Planting, 2011; Pretorius, 2012; Nel, 2014). These remarks indicate that Eskom can assume that the exporters of copper are the culprits because they "move" or "transport" the copper (Ras, 2015).

According to a study by Horn (2012), the increase in the international copper price and accessible black market in South Africa largely contributed towards the increases and decreases in copper-related incidents at the mine in Horn's study. Horn (2012) found a strong

correlation between the international copper price and the threat of copper-related thefts at the mine, with a further "displacement" correlation between the threat of copper-related incidents and other property theft-related incidents (Horn, 2012). When the international copper price decreased, a corresponding decrease in copper-related incidents occurred, while other property-related thefts showed an increase (Horn, 2012).

3.3.2 Eskom's unsecured asset on its open network

Copper is widely available, poorly secured and easy to steal due to the extensive Eskom power networks. Eskom network consists of 395 419 km of overhead lines, 11 018 km of underground cable and 351 297 installed transformers (http://www.issafrica.org/events/cable-theft-is-strangling-sas-economy-can-we-escape-the-noose). The researcher wishes to point that that it would be impossible to deploy security patrols to safeguard all of Eskom's assets over these distances.

In an article published by Fin24, (http://www.fin24.com/Companies/Cable-theft-down-57-20040811) Eskom's group risk manager for Distribution, Beulah Misrole has correctly pointed this out by saying, "In total, South Africa has 400 000 km of distribution lines. To patrol and protect all this is impossible". The researcher confirms Misrole's remarks that she made 11 years ago. Ben Coetzee, a senior researcher working at the Institute for Security Studies (ISS) Arms Management Programme, in his white paper of February 2008, highlights the point that the challenge that Eskom is facing is represented in the long distances that electrical cabling must cover in order to supply electricity to rural areas, where these cables are extremely vulnerable to theft (Hi-Tech Security Solutions (http://www.securitysa.com/article.aspx?pklarticleid=5592).

In a report published in IOL news, Colonel Gerhard Pistorius of the SAPS said that petty thieves that are stealing cables were the biggest problem. He said: *"They are unpredictable, poor people, many drug addicts, so it is hard to know where they will strike next. We have a non-ferrous metal crime combating committee in place which targets the organised syndicates and have managed to curtail this to a certain extent"*.

Col. Pistorius further stated that new legislation which dealt with second-hand goods had worked initially, but now thieves were bypassing dealers and were taking the stolen copper and metal to containers and exporting them directly (http://www.iol.co.za/news/crime-courts/classify-cable-theft-as-sabotage-1.1761319). The researcher wants to point out that if

thieves are bypassing dealers, and exporting the copper directly in order to fetch a higher price than that offered by the local dealers, then it means that attention must also be given to those exporting shipping containers.

Cornelius Vermaak, Eskom's security manager for the Eastern Region (KZN), said "cable theft syndicates from Gauteng preyed on overhead cables in Newcastle, Mooi River and Estcourt, and underground cables in Mandeni and Howick, while the theft of transformers was prevalent in Greytown and its surrounding rural areas" (Singh & Omar 2011; Pretorius, 2012). These important remarks of Pretorius and Vermaak call for definite actions to be taken and the researcher has addressed this later in his action plans (see section 7.2 – 7.6).

3.3.3 The difficulty to identify Eskom copper cables after it has been stolen

The impracticality of properly identifying stolen copper cables remains one of the main reasons why copper cables are so easily reintroduced in the recycling industry. Nkabinde (2014) says, in terms of copper, "… *It's still a big challenge as we cannot identify it once it is stripped or burnt. It is only aluminium that is manageable. I was told that Eskom have started marking our copper but it's going take a while as there is a lot of our cable out there….*"

Many companies have patented and developed various solutions to try to prevent thieves from pulling copper cable out of the ground or to make authorities aware of when and where it is happening, Eskom must do the same immediately and also find a way of marking existing cables (Ogle, 2014; Booysen, 2014).

According to the Southern Africa Revenue Protection Association's (SARPA) technical advisor, Rens Bindeman, one of the most inventive and cost-effective solutions involves the marking of cables at set lengths in order to prove, in court, that the suspect was illegally in possession of a particular piece of cable which had been installed at a specific place, for a specific service provider.

Binderman says, to prove this, the cable needs to have a unique mark every 10 to 20 centimetres down the length of its copper or aluminium core. This unique mark is presented in the format of sequential numbers; the starting and ending numbers are then recorded during installation at the cable's specific location (Traceable solutions: 2012, http://www.tracesol.co.za/about/articles/traceability-solutions-joins-the-fight-again-copper-cable-theft).

Kyle Parker, Managing Director (MD) of Traceability Solutions says, "Marking the cables will definitely make the product traceable, and together with the Second-Hand Goods Act which came into effect earlier in 2012, should put a check on copper cable theft." The Second-Hand Goods Act fundamentally stipulates that any person buying stolen goods, including cables, is as guilty as the person who stole the goods; if found guilty, individuals may face a prison sentence of up to 10 years (Traceable solutions: 2012, http://www.tracesol.co.za/about/articles/traceability-solutions-joins-the-fight-again-copper-cable-theft). The researcher supports this idea of marking the cables and also discusses this in Chapter Six (See Section 6.6.10). In fact, Eskom is now doing this (Nkabinde, 2014).

3.3.4 Lack of commitment and dedication by private security officers deployed to Eskom premises

Eskom experiences huge losses from its premises where there are contract security officers guarding the sites on a 24-hour basis. Many of these thefts have been linked to the security guards entrusted with the responsibility of securing Eskom assets (Nkabinde, 2014; Booysen, 2014). It seems that the apparent reason why thefts occur when security guards are involved is the desire to supplement their income.

Financial motive (to augment meagre income) is among the chief reasons for cable theft (Nkabinde, 2014; Booysen, 2014). The researcher argues that if the security officers remain committed in their profession and appreciate their careers, then they have no reason to involve themselves with theft, other than the fact that they are motivated by greed.

3.3.5 Lack of adequate security measures at Eskom facilities

Baccus (2015) feels that the lack of adequate security measures and competent security providers contribute to why Eskom has inadequate security measures to safeguard its facilities. Jenkins (2015) says that cable theft from substations increases because security systems are not properly maintained and the lack of competent security providers and their security personnel further exacerbates this problem.

Jenkins (2015) also feels that a security official does not pose any danger to criminals as they are ill equipped to protect Eskom installations. Due to lack of funds and experience, new security technology is not properly explored and applied at Eskom facilities (Jenkins, 2015). He is referring to outdated stand-alone systems which require a person to physically

download the information from the guard patrol systems, instead of Eskom utilising modern technology that works by remote activation and with real-time monitoring and tracking of the security guards' movements while they are working.

According to Govender (2014), the expectation of Eskom's Security Management Department is that any security service must be performance-driven and that a good quality security service must be rendered to Eskom. Despite the large number of security breaches that cost Eskom millions of rands annually, many business units in the various regions implement security solutions that are inadequate. It is also true that business units are spending "enough" money on security, but spending it in the wrong places or otherwise inappropriately (Jenkins, 2015; Meek, 2014).

Baccus (2015) mentions that many people fail to understand the business needs for security. In spite of efforts to implement some sort of security measures, many departments find that the solutions they implement are simply inadequate because they do not do proper threat and risk analysis to fully understand the risks.

Crime prevention measures such as security searches, patrols, access control and surveillance can be very effective, if enforced properly. However, if physical and technology security measures are not reinforced with proper controls, continuous maintenance and effective audits, these measures could give a "false sense of security" (Meek, 2014; Maxwell, 2014; Moodley, 2014).

3.3.6 Poor control for stock (cable) movements and unused materials on construction / project sites

Material and other equipment left at project sites are exposed to theft and items are often stolen. These losses are more than just the costs of losing expensive equipment and materials, there are also costs of downtime and project overruns that delay the project, which further impacts negatively on Eskom.

With regard to Eskom, most participants noted and commented that people working for Eskom must be more responsible in the way in which they manage Eskom's assets. In line with this, articipant 14 commented as follows:

"… Eskom suffers heavy losses from its construction sites because cable that is supposed to be recovered (either redundant cable or left over from the project) is left on site and thereafter stolen after the project is complete …."

Participant 17 said:

"… In many instances the clerk of works does not make arrangements to recover the cable for storage nor do they (at most times) provide safe and secure facilities for the excess cable …."

The researcher discusses the importance of good and poor housekeeping in Chapter Five (see section 5.16.4).

3.3.7 Socio-Economic Factors (Unemployment and Poverty)

According to Stats SA, the unemployment rate during 2013 in the country stood at 25.4 %. (http://beta2.statssa.gov.za/?page_id=737&id=1). The unemployment figure for 2015 was 25 % (Statistics South Africa, 2015). Baccus (2015) believes that some of the main reasons for cable theft at Eskom are related to the socio-economic factors relating to the country's failing economic climate, unemployment and poverty. Jenkins (2015) also says the crime situation in South Africa has escalated due to lower income per capita in specific areas, while Nkabinde (2014) also avers that the lack of employment and dissatisfaction (poor wages) among the guards is another cause for cable theft.

Economic factors, such as poverty and unemployment, have also played a major role in the continuous development of the private security industry. The illiteracy rate, as well as lack of tertiary education, was found to be a leading contributor to the high unemployment rates in the country. The South Africa Quarterly Labour Force Survey report 2013 revealed that unemployment had increased by 100 000 to 4.6 million, resulting in an increase in the employment rates to only 25.2 %. The most affected provinces, when it comes to unemployment, are North West with 39.6 %, Mpumalanga with 36.7 %, and Gauteng with 34.4 % (Statistics South Africa, 2013). While many people are losing their jobs, and as a result start to steal to obtain money, more opportunities arise in private security because people want to protect their assets.

Nkabinde (2014b) and Ogle (2014) mention that drug addicts commit this crime to fund their addiction, particularly in South Africa, and that socio-economic conditions caused by unemployment and poverty also contribute to the problem of cable theft. Patrick *et al*. (2012)

mention that socio-economic problems lead to drug abuse. The drug users often turn to crime to support their habits.

Maseema (2013) says the nyaope[iii] thieves, also known as the 'N-thieves', are those who steal out of need. They are usually forced by some circumstance to steal. They steal any valuable property, including cables, if they happen to be the most valuable or convenient property available at the time. Many 'N-thieves' are dependent on (addicted to) substances – such as drugs (nyaope, dagga, alcohol) and their plan is to steal enough copper to sustain their drug habit for some time.

Maseema (2013) say they are neither sophisticated nor knowledgeable about electricity – to the extent that they are sometimes electrocuted while trying to steal cables. Crime is a socio-economic problem – not a technical challenge – and therefore according to Maseema, requires a holistic solution.

Nel (2014) mentions that socio-economic issues are factors that can have negative influence on people's economic activity, where they lack education and so are unemployed and then turn to stealing cables to survive and support their families. Van den Berg (2014) basically says the same, namely that cable theft crime has socio-economic roots and mentions that the stolen copper ended up at scrap metal dealers, where thieves exchange it for cash. He further states that the copper found inside the cable is the main reason for the cable theft. Van den Berg says the stolen metal is recycled for electrical wires and to create jewellery and chandeliers, among other things (http://www.timeslive.co.za/thetimes/2014/08/27/coppers-targeting-copper-thieves).

3.3.8 Criminals are brazen in their attacks on Eskom

Generally, crime syndicates are not afraid to steal cables, given that they are brazen in their approach and will resort to violence before they attempt to steal cables (Jenkins, 2015).

There is a growing awareness among security professionals that criminals monitor the security guards on site and when they do not see them, they cut the fence and enter the site, very often with weapons. The guards are very often assaulted, stripped of their weapons and mobile phones before they are tied up and left in a corner until someone discovers them or they manage to free themselves (Cf. Annexure A10).

The criminals cut the gate locks with bolt cutters and drive their bakkies (light delivery vehicles) and trucks on to site to load the cables (Nkabinde, 2015; Ogle, 2014; Booysen, 2014). In view of these facts, the strengthening of methods by which the security guards conduct their business of securing Eskom assets, so that criminals are detected or arrested, would undoubtedly result in some degree of deterrence.

There can be little doubt, moreover, that emphasis on being extra vigilant and observant as an instrument of deterrence would result in criminals being detected before they enter the facility. The researcher wishes to point out that the comments made by Nkabinde, Ogle and Booysen point to the fact that the security officers are not observant enough on site, and by being unobservant and not alert, criminals will enter Eskom premises unhindered.

To achieve the maximum deterrent effect, it would be necessary either to impose strict restrictions against the guards relaxing in the security room, instead of being outside and patrolling, or to ensure that they deploy themselves strategically. In fact, security guards should be patrolling and looking out for intruders all the time during their deployment. They should be trained to observe and respond before they are attacked. They should raise the alarm to alert their supervisors, and the armed response company, of the attack and then take evasive action until the response vehicles arrive to assist them.

3.3.9 The involvement of the private security industry and law enforcement personnel in cable theft

It is true that another group that is benefiting from copper cable theft comprise elements in the private security industry (Institute of Security Studies 2010, http://www.issafrica.org/iss-today/who-profits-from-copper-theft). Private security firms, or persons within them, have the potential to profit from copper cable theft. Similar to the reasoning of racketeering, private security companies depend on the continued problem of cable theft to ensure that their contracts also continue (Booysen, 2014; Nkabinde, 2014; Meek, 2014).

Being convinced by experience and the many investigation reports, Ogle (2014) says that many security officers working at Eskom premises have been arrested and criminally charged for stealing cables. They usually cut small pieces of cable at a time during their night shift patrols and either put these in their bags or leave the pieces in bags, close to the fence. They retrieve the bags in the morning after they have completed their shifts. Booysen (2014) believes that many of security officers themselves comprise one of the biggest threats to cable

theft at the Eskom premises where they are deployed because of the large number of security guards working for Eskom who have been arrested. There have been many arrests of security guards for stealing cables at the Eskom premises. No regular polygraph exercises are done to ensure that they remain ethically crime-free at all times.

According to a News24 report, four men, including a security guard, were arrested for allegedly stealing copper cable at Transnet's warehouse in Germiston, east of Johannesburg. The men, aged between 23 and 45, were allegedly caught stealing two 500 m lengths of copper cable worth R170 000 each (http://www.news24.com/SouthAfrica/News/Copper-thieves-caught-with-R170-000-worth-of-cable-20140106).

Certain elements of the police, who are tasked to prevent crime including cable theft, are also involved in cable theft. One major theory about cable theft is that even the most trusted people who have permanent employment, with all the benefits (medical aid, housing allowances, bonus cheques, pension funds, retirement plan), are benefiting from cable theft because of the financial rewards that it brings to these people. Abrahamsen and Williams (2005) say that the relationship between private security providers and the public police are crucially important in the effective delivery of security.

News 24 reported that a Limpopo police officer was arrested when he bought cables from an undercover Hawks (Directorate for Priority Crime Investigation) agent (http://www.news24.com/SouthAfrica/News/Limpopo-cop-held-after-copper-sting-20120122). Another report by News.24, also in the Limpopo province, reported that a police constable and four other people appeared in the Phalaborwa Magistrate's Court on charges of theft and possession of stolen copper worth more than R80 000, taken from Foskor Mine premises. The constable was driving a marked police vehicle http://www.news24.com/SouthAfrica/News/Limpopo-cop-appears-for-copper-theft-20140714-4). The researcher wishes to point out that the consistently high price of copper makes it a valuable commodity for illicit business transactions, even by the most trusted employees.

3.4 ESKOM'S FINANCIAL LOSSES EXPERIENCED DUE TO CABLE THEFT

According to Eskom's Annual Report (2016), Eskom experienced thefts of conductor (cable), cabling and related equipment in 2016 that totalled R85 million, involving 5 161 incidents (Cf. 1.12.2). The figures for March 2015 were R102 million in losses, with Eskom

experiencing 5 680 incidents (Eskom, 2016). The combined effort between the South African Police Services and Eskom security resulted in 229 people being arrested. During March 2015, 297 people were arrested for cable theft crimes (Eskom, 2016).

According to Eskom's Annual report (2014), Eskom had experienced losses totalling to R68 million due to conductor theft (including theft of copper cable, transformers and tower-related structures). In 2013, this amount was R51 million. Eskom (South Africa) experienced a total of 7 166 incidents of theft from its infrastructure. In 2013, the number of incidents totalled 5 187 incidents involving its infrastructure. The actions to combat these losses are managed by Eskom security and private security contracted to Eskom, as well as in collaboration with affected state-owned companies and the South African Police Services. The combined efforts of Eskom security and the SAPS resulted in 316 arrests. In 2013, 321 people were arrested and stolen material (including copper cables) worth R7 million was recovered (Eskom Annual Report, 2014).

In a 2009 parliamentary session on copper cable theft, it was revealed that Eskom lost R14.8 million in stolen materials and incurred R38.7 million in replacing infrastructure, and R18.2 million in security mitigation for 2008/09 (up from R10.5, 21.5, and R14.5 million, respectively, for 2007/08) (Institute of Security Studies 2010, http://www.issafrica.org/iss-today/who-profits-from-copper-theft). Eskom has incurred losses of more than R350.2 million between 2006 and 2007 due to power outages, replacement costs and the cost of security upgrades as a result of cable theft and vandalism. (Hi-Tech Security Solutions, 2011, http://www.securitysa.com/article.aspx?pklarticleid=6974).

The lack of effective security measures is the main reason why Eskom is losing millions of rand, annually. Through this study, the researcher wants to change the present situation to a more favourable one.

3.5 THE ECONOMIC SABOTAGE CAUSED BY CABLE THEFT

Ras (2015b) insists that cable theft crimes against Eskom are economic sabotage and people apprehended for this type of crime should be punished severely (Institute of Security Studies, 2010; Ogle, 2014; Booysen, 2014). He says that this economic sabotage does not only affect Eskom, but all businesses in South Africa. Companies become less productive, and some are forced to shut down and retrench workers, when the power is disconnected for long periods of time.

This has a huge impact on the broader provision of basic services. The interruption in the supply of electricity has also a large impact on the supply of water. Some of the reasons for service delivery protests are attributable to cable theft (Ras, 2015b). If people were to investigate some of the causes of why there is a lack of supply of electricity, they would find that it is an incursion of cable theft which negatively influences the delivery of electricity supply (Ras, 2015b; Eskom, 2016; Hi-Tech Security Solutions, 2011).

Ras (2015b) says copper theft has a direct effect on the lives of the citizens of South Africa. The cables stolen from Eskom disconnect our communities, especially poorer communities. Eskom then has to spend additional resources replacing infrastructure, being money which could be spent rolling out more services to the areas where electricity is required and to the poor people of South Africa. Eskom's Medupi power station (see section 4.9.1) is also under threat, with further delays caused by labour problems which compromise the security. Mokonyane (2014) concurs with Ras when he earlier said that "Issues of cable theft should be dealt with as economic sabotage".

The justice system must not deal with them as petty crimes, but as economic crimes (Mokonyane, 2014; http://www.fin24.com/Economy/Mokonyane-Cable-theft-economic-sabotage-20140929). Baccus (2015) strengthens the comments of Ras (2015a) and Mokonyane (2014) by saying that the legal experts must look at the current law to establish if the charge of theft can be can be changed to a more serious charge of economic sabotage. Baccus (2015) believes that the charges must send a strong signal to criminals because the current charges are not severe enough. Due to a lack of specific legislation, those arrested for possession of stolen cables are seldom prosecuted or convicted successfully (Ogle, 2014; Booysen, 2014, Nkabinde, 2014).

One of the reasons cited in Eskom's Annual Report 2008 for its poor distribution performance was the increase in unplanned interruptions such as theft, and in particular conductor theft.

According to this report, losses to the entity due to conductor theft (including copper and cable) during 2008 totalled R25 million (up R9 million on 2007) and involved 1832 incidents. (Hi-Tech Security Solutions, http://www.securitysa.com/article.aspx?pklarticleid=5592); secondly, load shedding removes any deterrent value linked to the danger of being killed by electrocution when tampering with electrical cables ….” (Hi-Tech Security Solutions (http://www.securitysa.com/article.aspx?pklarticleid=5592).

In a meeting of the Parliamentary Monitoring Group on Copper Theft, & Solar Water Heating held on the 28 February 2012 (http://www.pmg.org.za/report/20120228-departments-energy-public-enterprises-justice-salga-transnet-and-esko), Ms Ayanda Noah, (Eskom Group Executive: Distribution), said that 1 591 conductors were stolen in 2011 which cost Eskom more than R22 million, while only R2 million of the total amount had been recovered. The cost of attempting to manage the problem was not factored into this figure. In 2009, the repair cost of damage caused by theft was R300 million. This amount included security, the awareness campaigns and the unserved energy.

Noah said “that Eskom structures were also being tampered with, which resulted in unbalanced conductors. The biggest challenge was the theft of the pylons, because Eskom has a large footprint in the country. However, over the last seven years, incidents on the distribution side had declined so it seemed that Eskom’s plans to address the problems were yielding results. In 2010, when the country collaborated to deliver on World Cup projects, there were positive collaborations with stakeholders, and these had helped to reduce incidents” (http://www.pmg.org.za/report/20120228-departments-energy-public-enterprises-justice-salga-transnet-and-esko).

Noah further said that “Gauteng and the central regions were challenged by high incidence of theft and damage. Conductors were stolen not only for resale, but were used for illegal connections. Eskom also closely monitored theft of transformers containing copper, so it was important to look at the whole effect over all infrastructures. Impact of theft on business was massive. The most important issues concerned safety and security, because disruptions affected business and people’s lives” (http://www.pmg.org.za/report/20120228-departments-energy-public-enterprises-justice-salga-transnet-and-esko).

“Eskom was compromised in security of electricity supply. Those people who operated businesses at home struggled to work if there was a disturbance, and some even claimed damages from Eskom, so Eskom’s insurance costs would rise”

(http://www.pmg.org.za/report/20120228-departments-energy-public-enterprises-justice-salga-transnet-and-esko). Noah concurred "that it was mostly syndicates who were engaging in theft. In some instances, Eskom's security personnel who were guarding sub-stations had been fired at, and security guards had been killed or injured in a number of incidents" (http://www.pmg.org.za/report/20120228-departments-energy-public-enterprises-justice-salga-transnet-and-esko).

In the case of copper cable theft, its implications range from the substantial monetary costs incurred through theft-induced cable replacement to the increased risk of train derailments or collisions through track disruption and faulty signalling (Bennett, 2008b).

3.6 THE HIDDEN COSTS OF CABLE THEFT

In this section the researcher points out the hidden costs of cable theft to Eskom and other state-owned enterprises in South Africa directly linked to Eskom:

3.6.1 The hidden costs of cable theft to Eskom

The problem of cable theft is huge, with the numbers so big and the scale so enormous, that it defies comprehension (Eskom Annual Report, 2014). Cable theft affects not only the supply of electricity, but also everything from telephone connections to train signalling. Maboe Maphaka (Senior Manager at Eskom) estimates that cable theft costs Eskom R45 million a year – in addition to the damage to its image. He further said that cable theft also results in consumers incurring losses from power surges which can damage all equipment – computers, TVs, appliances – plugged in at the time. He added that "When a customer comes down to Eskom to claim for a fridge that has burnt down, and Eskom comes back and say "… look, we can't pay you for this because of this, this and that, as customer you are aggrieved], and then Eskom becomes this uncaring organization …. [sic]" (http://www.voanews.com/content/cable-theft-hampers-economy-in-south-Africa/1603668.html).

The distribution, maintenance and rehabilitation backlog for electricity increased by at least R2.5 billion annually, and in 2012 stood at R35 billion (Van Onselen, 2013). Van Onselen (2013) says that when electricity supply is not being prevented through cable theft, the dilapidated infrastructure causes blackouts and load shedding. Hospitals have often suffered as a result of this. In March 2013, stand-by electricity generators failed to start up at Charlotte

Maxeke Hospital in Gauteng, leaving its intensive-care unit without electricity for four hours. In June 2013, a three-and-a-half-day power outage shut down Somerset Hospital in the Western Cape. The hospital does not have a back-up generator.

Van Onselen (2013) says there is a profound cost attached to all of this, one increasingly being born by the tiny section of the South African population who are able to pay rates and taxes. Where they cannot cover the collective cost of supplying services, huge debts follow. Van Onselen (2013) avers that the South African water boards, for example, are owed more than R1 billion by municipalities and are unable to collect revenue.

Eskom has been forced to raise its rates to astronomical levels in a desperate attempt to cover a maintenance backlog long out of control, as well to counter the same problems the water boards face. In November 2012, Eskom revealed it was owed R3.3 billion by Soweto residents alone (Van Onselen, 2013).

3.6.2 The hidden costs of cable theft to the cities of Durban, Cape Town and Transnet

According to Dawood (2014), Durban electricity thieves cost ratepayers R190 million a year, but the losses climb to R230 million when the theft of infrastructure – including copper cables and 'busbars' (connecting bars) in substations are factored in. He says the municipality suffers from the negative impact of illegal electricity connections which include the "hefty costs" of replacement of infrastructure and hiring security, the shutdown of business operations, loss of income and loss of exports (http://www.iol.co.za/news/crime-courts/electricity-thieves-cost-ratepayers-r190m-1.1788154).

According to the City of Cape Town's official website, the Utility Services Directorate spent R116 million in the 2013/14 financial year on operational security costs, while they are continually exploring alternate ways to tackle the problem of theft and vandalism in a more cost-effective manner. The City of Cape Town called on the community to take ownership of the infrastructure in their areas, and immediately report any suspicious activity. The City of Cape Town say (on their website) that they are engaged in a constant struggle against copper and metals thieves and every year millions of rands are spent on replacements and repairs – money which could have been better spent on providing services to residents. (https://www.capetown.gov.za/en/Pages/Securityserviceshiddencostvandalismtheft.aspx).

In an article published by Hi Tech Security Solutions (2010), the Democratic Alliance's Shadow Deputy Minister of Public Enterprises, Pieter van Dalen, highlighted the repercussions

of this vandalism on the likes of Transnet and Eskom, whose combined losses due to copper theft amounted to an increase in losses of 38,1 % in 2008/09 and replacement costs increasing by 57,4 % (Hi-Tech, 2010, http://www.securitysa.com/article.aspx?pklarticleid=5905).

In the same article, Van Dalen further states that while the combined losses noted above are substantial, it was interesting to note that Transnet is the one company that has shown the most significant increase in material losses, with replacement costs amounting to R30,1 million, more than three times their 2004/05 levels. Eskom, on the other hand, has been more effective in keeping cable theft relatively stable over the last five years (Hi-Tech, 2010, http://www.securitysa.com/article.aspx?pklarticleid=5905).

3.7 THE ROLE SCRAP DEALERS PLAY IN PROMOTING CABLE THEFT

Baccus (2015) mentions that certain scrap dealers report to Eskom and notify Eskom immediately when people come to sell Eskom material, but there are also those dealers that buy stolen metal and then sell it to large-scale scrap dealers. If all scrap dealers were acting legally, the market would cease to exist because nobody would buy stolen cables (Baccus, 2015); nevertheless, Jenkins (2015) believes that scrap dealers create an outlet for cable thieves.

It is true that the consistently high price of copper makes it a valuable commodity for illicit business. Thieves seem to be market analysts, who decide when the price of copper has risen to a point where the theft of this particular commodity (weighed against the risk) is more financially rewarding than any other (Institute of Security Studies 2010, http://www.issafrica.org/iss-today/who-profits-from-copper-theft). Certain scrap metal dealers, who should strictly adhere to the Second Hands Good Act (No 6 of 2009) and who should not purchase stolen copper cables, are also involved in cable theft.

Copper cables are stolen with the intention of selling them for financial gain through scrap dealers, who conduct both illegal and legal operations. It is often the case that the illegal buying and selling of copper cables is done in the shadow of the legal scrap dealer market. Some scrap dealers contribute to the problem by knowingly purchasing stolen copper or deliberately not inquiring as to where the copper originates from (Booysen, 2014; Nkabinde, 2014).

Disreputable scrap dealers have always found innovative ways of dodging legislation by sponsoring 'mobile scrap yards' to buy illicit copper from traveling vehicles, establishing smelters at peri-urban farms to change the appearance of illicit copper, and opening unregulated bucket shops to clean the copper before supplying licensed agents (Institute of Security Studies 2010, http://www.issafrica.org/iss-today/who-profits-from-copper-theft).

According to Singh and Omar (2011), a Durban scrap dealer said that "… while he earned about R60 to R70 a kilo of copper sold on the international market, he paid locals R40 to R50 a kilo for copper. In a month some dealers exported about 15 containers, each weighing 25 tons…."

Nicolaides (2014) reported that a businessman and his alleged four accomplices were found in possession of the copper cable at a scrapyard on the West Rand (greater Johannesburg area). The man allegedly tried to evade arrest by offering police a bribe. The police have confirmed that the businessman tried to bribe the officers with R30, 000, but they refused the payment and arrested him on the scene. The report further mentions that the man owns a house in Atholl (in Sandon) worth more than R10 million and is apparently involved in, or heads, a copper cable syndicate (http://ewn.co.za/2014/10/20/JHB-businessman-in-court-for-cable-theft) (Cf. Annexure A3).

3.8 ESKOM'S PARTNERSHIPS IN THE PREVENTION OF CABLE THEFT

Although Eskom is currently engaged with various role players and stakeholders within the environment where copper cable theft is encountered and participates in various forums, these role players are not contractually bound to prevent cable theft from Eskom; the private security contractors are. The role players include the South African Police Service (SAPS), Asset Forfeiture Unit (AFU), National Prosecuting Authority (NPA), Non-ferrous Theft Combating Committee (NFTCC), South African Revenue Service (SARS), and Business Against Crime (BAC).

The Non-ferrous Metal Theft Combatting Committee (NFTCC): The Non-ferrous Metal Theft Combatting Committee (NFTCC), under the management of Business Against Crime South Africa (BACSA), was formally established in 1993 as an integrated body of role players that provides strategic guidance and direction for the process of preventing and eradicating theft of non-ferrous metals, and copper cable, in particular (Horn, 2012; Nell, 2007). The NFTCC has one national committee and 28 regional committees which are

strongly supported by government (Horn, 2012; Nell, 2007). In conjunction with partner organisations and government departments, the NFTCC developed a revised strategy addressing areas such as the illegal export market, which placed a great emphasis on the need for the full commitment, leadership and involvement of government agencies and stakeholders to drive the initiative, with the appropriate levels of authority, budgets and political will (BACSA, 2009a; Horn, 2012; Nell, 2007).

South Africa Police Service (SAPS): It is the mandated responsibility of the SAPS to lead the fight against copper theft (among other crimes) and thus they also preside over the Non Ferrous Metal Crime Combatting Committee (NFMCCC) (Pretorius, 2012; SAPS, 2015).

National Prosecuting Authority (NPA): The role/purpose of the NPA in this industry is to ensure the successful prosecution of cases involving the theft of copper (among other crimes). In this capacity they would also have an advisory role and thus should ensure that combating copper theft should be partly a prosecution-led approach (Pretorius, 2012; NPA, 2016).

South African Revenue Service (SARS): SARS has the mandate under the South African Revenue Service Act, 1997 and Sections 74 and 74A to 74D of the Income Tax Act 58 of 1962 to conduct lifestyle audits, since it is clear that wealthy syndicates are involved in this type of crime. Together with asset forfeiture, this is a crucial part of investigating this illicit industry (Pretorius, 2012; SARS, 2016).

Business Against Crime (BAC): Business Against Crime (BAC) provides avenues for discussion and coordination. The role of BAC is crucial in creating momentum where it is needed. They should constitute the forums under which industries and service providers should mobilise; alternatively, the businesses affected could create their own platform (Pretorius, 2012; BAC, 2016).

Asset Forfeiture Unit (AFU): In conjunction with the NPA, SAPS and SARS, the AFU is empowered to initiate proceedings for the forfeiture of the assets of culprits involved in this illegal trade. It stands to reason that the more criminal "high flyers" there are who forfeit their assets, the clearer the message will be that is sent out – criminal activity will cost perpetrators dearly (Pretorius, 2012; AFU, 2016).

Council for Scientific and Industrial Research (CSIR): On 01 August 2016, Eskom signed an agreement with the CSIR which established a standing security sub-committee that will identify and deal with security risks that are having a significant financial impact on Eskom's

business. The agreement will focus (amongst other things) on regaining financial strength; security risk management solutions to prevent theft and safeguard high-value assets; cable and infrastructure theft detection and prevention; smart meter protection; and detection and prevention of illegal connections and revenue theft (Eskom internal mail, 2016).

3.9 SPECIFIC RESPONSES BY ESKOM TO REDUCE COPPER THEFT

Partnerships mentioned in this section (3.9) are additional to Eskom's security measures because the private security that Eskom has contracted to protect its facilities is ineffective, and seemingly cannot prevent cable theft. Eskom also has a drive called Operation Khanyisa, which aims to educate communities regarding copper cable and electricity theft.

This campaign has achieved high levels of awareness, with a constant flow of information through radio, print, online news sources and outdoor advertising. According to a report published in Times Live (http://www.timeslive.co.za/local/2014/10/13/phiyega-requests-public-support-in-fight-against-cable-theft), Maboe Maphaka (Senior Manager for Energy Trading and Sales Forecasting at Eskom) said that Eskom made great progress on tackling cable theft, but more needs to be done. He says that more than 10 500 tip-offs had been received to date, resulting in over 130 arrests for crimes relating to electricity theft and more than 60 convictions. While mentioning that this is great progress, he recognised that more needs to be done: "… We will continue to work with the SAPS and the NPA to strengthen the investigation and criminal prosecution of electricity thieves…." (http://www.timeslive.co.za/local/2014/10/13/phiyega-requests-public-support-in-fight-against-cable-theft).

Although Eskom is a responsible and professional employer that provides an equitable and balanced remuneration to its employees and service providers, financial desires comprise one of the reasons why cable thefts occur. The fair and equitable remuneration that Eskom offers to its employees does provides a sense of psychological ownership (Nel, 2014; Nkabinde, 2014), but for some that is simply not enough.

Security in Eskom is managed by security specialists who have the necessary qualifications and accreditation to turn matters (i.e. losses) around. Eskom's security is decentralised and each province of South Africa has its own investigation teams. All security officers and other functionaries that are concerned with combating copper cable theft, whether in preventative security, investigations, arrest or prosecution environments, are trained and sensitised in

connection with copper theft threats, and they also possess the unique skills required to combat it successfully. Eskom is contracted with a company called Combined Private Investigations (CPI) whose function is to investigate (upon request by Eskom) copper cable and conductor theft in South Africa (Nel, 2014; Nkabinde, 2014).

Security officials and endeavours are currently engaged in the Security Recovery Program (SRP) which includes implementing additional security upgrades at substations and main power stations (Cheerkoot, 2014), These should ensure that criminals who commit criminal acts of stealing cables are apprehended. The increasingly strong demand for copper cables has highlighted the vulnerability of Eskom facilities to vandalism and theft. To address the risk and vulnerabilities, the SRP project was initiated to develop a security management framework and security operating model for Eskom (Cheerkoot, 2014).

Eskom is currently embarking on the process of using identification marks on copper cables that are utilised on the network (Nkabinde, 2014). The markings are part of the manufacturing process. The process of easy identification of stolen cables is now less cumbersome during scrap dealer inspections, because if any of this marked copper is found at scrap dealers premises, the dealers can be charged with dealing in stolen goods (see section 3.3.3).

Cable theft is also a major contributor to power failures (see section 3.6.1). Aggressive awareness campaigns have been launched to inform the public of the negative effects of cable theft. Eskom also works closely with communities to encourage them to report any illegal cable thefts (Eskom factsheet, 2014). Eskom has also embarked on various campaigns, such as Operation Khanyisa, which are aimed at highlighting the dangers of the unsafe use of electricity, such as cable theft, illegal connections and vandalism of its networks, which often result in serious injuries and even death. It also has a hotline number for the public to report safety issues (0860037566) and has also requested members of the public seeking more information on electricity safety to send an email to them (safety@eskom.co.za).

3.10 SUMMARY

This chapter gave an overview on the extent of Eskom's presence in South Africa (see section 3.1) and explained some of the reasons why copper cables are preferred to aluminium by Eskom (see section 3.2). It highlighted various reasons which were provided for the increase in cable theft at Eskom (see section 3.3). The study provided details of Eskom's

financial losses due to cable theft (see section 3.4) and the economic sabotage caused by cable theft (see section 3.5).

The hidden costs of cable theft to Eskom (see section 3.6.1) and other state-owned enterprises in South Africa directly linked to Eskom were discussed (see section 3.6.2). A discussion on the role of scrap dealers in promoting cable theft (see section 3.7) and Eskom's partnership in the prevention of cable theft was included this chapter (see section 3.8). Specific responses by Eskom to reduce copper theft (see section 3.9) were also given, as well as a summary (see section 3.10).

CHAPTER FOUR
ESKOM'S IN HOUSE SECURITY AND CABLE THEFT

4.1 INTRODUCTION

While Chapter Three focused on the extent of cable theft at Eskom, this chapter looks at Eskom's in-house security and what they need to do to prevent cable theft. This is in line with research aim four, described in Chapter One (see section 1.8.4).

This chapter clarifies the meaning of the term "In-house security in Eskom". It provides information on the following issues:

- The history of the security function at Eskom
- Eskom's plant vulnerability and its effects on South Africa
- Eskom's new projects and its future security plans
- Eskom's in-house security guard deployment
- The effectiveness of Eskom's in-house security in preventing cable theft
- The difference between Eskom's in-house and private security industry guards
- Eskom's in-house security resources
- Equestrian research conducted by the researcher.

In order to put the remarks that will be made in this chapter in the right perspective, brief remarks will be made from the outset of this chapter.

4.2 THE MEANING OF THE TERM 'IN-HOUSE SECURITY' AT ESKOM

'In-house security' refers to the situation where Eskom employs its own security personnel to protect or safeguard its facilities. These security personnel comprise security managers, supervisors and security guards. All the in-house security personnel are registered with the Private Security Industry Regulatory Authority (PSIRA). It is today a standard requirement for them to also complete National Key Point (NKP) training (if they work at an NKP facility) and to possess a valid firearm competency certificate for handguns (see section 4.3).

4.3 ESKOM'S MINIMUM PSIRA AND LEGAL REQUIREMENTS FOR THEIR IN-HOUSE SECURITY OFFICERS

In addition to the firearm competency certificate, the security guards must attend two training firearm training sessions per year, as opposed to the compulsory requirement of only once per year in terms of Regulation 21 training (Firearms Control Act 60 of 2000). These training sessions must include the safe handling of firearms and the legal compliance with firearms procedures. Eskom has a procedure in place for the appropriate handling of firearms (Handling and safe practices for private firearms and ammunition on Eskom premises, 32-1138).

Eskom subscribes to the PSIRA Code of Conduct for Security Service Providers, 2003, prescribed under the PSIRA Act, 56 of 2001. All of Eskom's security officials (including management) are registered with PSIRA. Eskom further subscribes to the PSIRA Levies Act, 2002.

Table 4-3: The legislated and compulsory training that must be undertaken by all Eskom security personnel working with firearms

ID	UNIT STANDARD TITLE	NATIONAL QUALIFICATION FRAMEWORK LEVEL (NQF)
117705	Demonstrate knowledge of the Firearms Control Act 2000 (Act No 60 of 2000) applicable to possessing a firearm	Level 3
119649	Handle and use a handgun	Level 3
119650	Handle and use a self-loading rifle or carbine	Level 3
119652	Handle and use a shotgun	Level 3
123515	Handle and use a handgun for business purposes	Level 4
123511	Handle and use a self-loading rifle or carbine for business purposes	Level 4
123514	Handle and use a shotgun for	Level 4

	business purposes	

4.4 THE ORIGIN OF ESKOM'S IN-HOUSE SECURITY

The in-house security functions at Eskom started in 1968. The first batch of security guards was employed at Eskom's Arnot, Hendrina, Camden and Ingagane power stations. In 1974, the Security Training Centre opened at Eskom's Arnot power station and played an important role in developing and training security guards for Eskom. The training at Arnot power station compared extremely well with security training in other organisations, which resulted in the centre also training non-Eskom people (http://heritage.eskom.co.za/arnot/arnot.htm).

A number of South African Defence Force and South Africa Police security personnel joined Eskom security department. They completed a training course in six weeks, which concentrated on the development of supervisory skills and leadership orientation training (http://heritage.eskom.co.za/arnot/arnot.htm).

4.4.1 Eskom security dogs

The Eskom Dog Training Centre was opened in 1974 and formed part of the Eskom Protective Services Security Training Centre (Cf. Annexure A23 – A31). The aim was not only to provide a dog patrol security service to Eskom, but also to provide trained security dogs for private companies. The security dogs were trained as patrol dogs and to locate stolen copper cable. In 1974 the first batch of security patrol dogs was trained. In 1982 a study conducted at Eskom ascertained that a further 2 000 dogs would be required for security purposes and that the current facility at Arnot was not equipped to handle such a large number of dogs. Roodeplaat Breeding Enterprises in Pretoria then began to train dog handlers and dogs for Eskom security purposes (http://heritage.eskom.co.za/arnot/arnot.htm), but they did not meet Eskom standards, nor the quality of training required for the dogs.

This resulted in Arnot reopening in 1988. In 1992, Eskom imported seven bitches from Germany to improve its breeding stock. The dog training centre was closed in 1995 because of financial and operational reasons. It had been in operation for 21 years (http://heritage.eskom.co.za/arnot/arnot.htm).

4.4.2 Eskom security training

Following various developments in southern Africa, the issue of security of assets took on a greater importance in the late seventies. In 1975, Dr Ian McRae (now retired Chief Executive, Eskom) arranged for a two-day Security Awareness session at Arnot which was hosted by the Education Department. It was comprised of lectures on security and concluded with the passing out parade of the second-largest group of black security guards. The passing out parade of security personnel was the culmination of a gruelling three-month course which included instruction in drill, physical training, law, criminal procedure, human relations, Eskom security, accident prevention, fire-fighting and dog-handling.

Security officials who had completed the initial supervisor's course could decide in which of the three fields of intelligence, operations or training, they wished to advance to (http://heritage.eskom.co.za/arnot/arnot.htm). During a period of one year, 1080 officials were trained at Arnot (consisting of three Companies and twelve Platoons of thirty cadets) then the numbers were gradually reduced to 530 (http://heritage.eskom.co.za/arnot/arnot.htm).

4.4.3 Integration of the National Key Points Act and training into Eskom

In 1983, the introduction of the National Key Point Act (Act 102 of 1980) resulted in the Arnot Security Training Centre becoming registered as a National Key Point training establishment.

Many security training courses were developed to concentrate on the continuous development of skills and training needs. All security personnel were trained within 12 months of their appointment. The training was work orientated and based on the individual's level of competence (http://heritage.eskom.co.za/arnot/arnot.htm).

The National Key Points Act laid down standards for courses, which meant that students had to obtain 60 % in written examinations to qualify. Internal Eskom examinations in weapons handling required 70 % to qualify. Legal subjects related to the use of firearms required 100 % to pass (http://heritage.eskom.co.za/arnot/arnot.htm).

4.4.4 Eskom's first incident of sabotage

In July 1981 intruders sabotaged the transformers at Arnot. They cut a hole in the security fence and bombed two of the transformers beyond any state of repair. Experts from the South African Police (Middleburg) investigated the site the next morning and found and disarmed a further three limpet mines. After this incident, the fencing of all Eskom power stations was electrified (http://heritage.eskom.co.za/arnot/arnot.htm) and the focus of Eskom security changed, with more importance placed on the different security departments.

4.5 WHERE DOES ESKOM HAVE ITS IN-HOUSE SECURITY DEPLOYED?

Eskom has most of its in-house security guards deployed at its power stations, of which most are located in Mpumalanga, South Africa. A power station is a converter of energy. During the combustion of fuel, a chemical energy conversion process generates heat to convert water into steam at a very high temperature and pressure. The heat energy contained in the steam drives a huge turbine, converting heat energy into rotating mechanical energy in the process. Coupled to the turbine shaft is a generator where electrical energy (electricity) is produced (Eskom fact sheet, 2014).

Mpumalanga has rich coal deposits, concentrated in the north-east of the country, and as such the majority of South Africa's coal-fired plants are located in the Mpumalanga province. Around 77 % of South Africa's energy needs are directly derived from coal, and 81 % of all coal consumed domestically goes towards electricity production (Eskom fact sheet, 2014).

Because of the importance of power stations in generating electricity and the importance of Mpumalanga because of its rich coal deposits, many of Eskom's in-house security resources are deployed in the Mpumalanga province.

Eskom in-house security is deployed at the following business units, listed in Table 4-1 below.

Table 4-1: Eskom Power Stations

Site Name	Location
Arnot Power Station	Mpumalanga
Camden Power Station	Mpumalanga
Duvha Power Station	Mpumalanga
Grootvlei Power Station	Gauteng

Hendrina Power Station	Mpumalanga
Kendal Power Station	Mpumalanga
Komati Power Station	Mpumalanga
Kriel Power Station	Mpumalanga
Lethabo Power Station	Mpumalanga
Majuba Power Station	Mpumalanga
Matimba Power Station	Mpumalanga
Matla Power Station	Mpumalanga
Tutuka Power Station	Mpumalanga

4.5.1 Generation division: Eskom power stations

Most of Eskom's power stations are protected exclusively by in-house security guards. In general, these power stations have between 35 and 85 security guards deployed on every shift to safeguard the facility. The power stations have been registered as NKP sites because of their importance and are regulated by the NKP Act, 102 of 1980 (among other legislative and regulatory requirements).

The map, set out in Figure 4.1 below, indicates the locations of Eskom power stations in South Africa.



Figure 4.1: The map of Eskom power stations in South Africa

Source: Map of Eskom Power Stations in South Africa (http://www.eskom.co.za/Whatweredoing/ElectricityGeneration/PowerStations/Pages/Map_Of_Eskom_Power_Stations.aspx)

4.5.2 Generation Division: Eskom peaking stations

All Eskom peaking stations (see Table 4-2 below) are protected by in-house security guards. In general, all these stations have between 15 and 20 security guards deployed on a shift basis to protect the facility. These power stations are NKP sites and are governed by the NKP Act, 102 of 1980, (among other legislative and regulatory requirements). The security units are well resourced and the peaking stations are guarded adequately by trained individuals.

Table 4-2: Eskom peaking stations

Site Name	Location
Gourikwa	Western Cape
Drakensberg	Kwa-Zulu Natal
Ankerlig	Western Cape

4.5.3 Generation Division: Eskom Koeberg Nuclear Station

The Eskom Koeberg nuclear facility is protected by close to 150 in-house security guards. This facility is an NKP site and strictly complies with the NKP Act, 102 of 1980, (among other legislative and regulatory requirements), and because this is a nuclear plant, the security units are not only well-trained, but also fully equipped to safeguard this strategic site.

Site Name	Location
Koeberg Nuclear Station	Western Cape

4.5.4 Generation Division: Komati water facility

The Eskom Komati facility is protected by close to 10 in-house security guards. This facility is also an NKP site and strictly complies with the NKP Act 102 of 1980 (amongst other legislative and regulatory requirements).

Site Name	Location
Komati Water	Western Cape

4.5.5 Transmission Division:

Generally, Eskom has only a very small number (less than 15) of in-house security officers deployed to the Transmission Division.

4.5.6 Distribution Division:

Similar to the Transmission Division, Eskom has only a very small number (less than 20) of in-house security officers deployed to each Distribution Division.

4.6 WHAT IS THE DIFFERENCE BETWEEN ESKOM'S IN-HOUSE SECURITY AND PRIVATE SECURITY INDUSTRY GUARDS?

Eskom in-house security personnel are employed by Eskom and are carrying out security services. The private security guards work for private security companies that are appointed on a contractual basis, in other words, they are private security contractors. The Eskom selection process is stricter than that of the private security industry is. Better salaries and job opportunities are offered to Eskom in-house security personnel to motivate them to perform better, and which would mean that less copper is stolen.

4.6.1 Appointment processes to employ new security officers for its in-house division

Eskom follows a stringent appointment process to appoint security officers to work at its facilities. The minimum requirement is a grade 12 (previously standard 10) school pass, PSIRA grade C registration, and a driver's licence (minimum code EB).

Eskom further requires applicants to have the following skills and competencies prior to their appointment:

- Physical fitness to perform operational duties.
- Mental fitness (psychometric tests are done by Eskom for appointed contractors prior to the appointment to determine if they can perform under stressful and dangerous situations).
- Good analytical skills
- Good communication skills
- Effective customer care skills
- Sound interpersonal and industrial relations skills

- Creative thinking abilities
- Leadership skills
- Basic computer literacy skills.

Private security companies contracted to those Eskom NKP sites that belong to Eskom, in most cases, simply require a PSIRA registration and (where applicable) possession of the NKP training and a firearm competency certificate.

4.6.2 Salary and benefits offered to newly appointed in-house security officers

Eskom offers a very competitive salary, which is in line with Eskom's task grading for T6 levels. In additional to a competitive salary, Eskom offers its security officers a 13th cheque, performance bonus pay, medical aid, a housing subsidy, leave benefits, study opportunities and a safe working environment. With Eskom's "zero harm" policy, the aim is to reduce the number of fatalities occurring as a result of either its operations or its product to zero by continuing safety trainings and reducing the exposure of employees to potentially harmful situations (Eskom factor, 2014).

The private security contractors appointed by Eskom offer their security officers a PSIRA-regulated salary, without benefits (such as medical aid, housing subsidy and 13th cheque).

4.6.3 Alternate job opportunities for security personnel

Within the Eskom Group, direct jobs are provided to close to 41 800 people (Eskom factor, 2014). This figure includes Eskom security personnel. This makes Eskom one of South Africa's top 20 employers (Eskom factor, 2014). It is an interesting fact that in 2011, Eskom provided approximately 298 000 learning days to their employees (equivalent to seven days per employee). In developing these training programmes, Eskom invested R998 million in training and development throughout the 2011 financial year, corresponding to 5.7 % of labour costs, thus positioning Eskom in the upper quartile, compared with similar utilities in the US and Europe (Eskom factor, 2014).

Eskom security officers have the option of being reskilled and retrained to do alternate jobs within Eskom. This means that they do not necessary have to remain security officers for the duration of their careers within Eskom. Eskom has a clear commitment to the training and development of its employees through its Eskom Academy of Learning (EAL). The EAL has

been repositioned as a professional centre of excellence, tasked with delivering learning in Eskom (Eskom factor, 2014). The private security industry does not offer its employees alternate job opportunities, other than the limited positions of supervisors and managers, which in most cases are not offered to the security officers.

4.7 ESKOM'S IN-HOUSE SECURITY RESOURCES

From Eskom's side, their in-house security is well resourced.

4.7.1 Eskom security manager

Eskom follows a stringent recruitment process to recruit security managers to work at its facilities. The minimum requirement is a grade 12 (previously standard 10) school pass, a relevant post-matric examination security qualification of 3 years' duration, PSIRA grade C registration, holding a security senior supervisory position for 8 years, and a driver's licence (minimum code EB) (Eskom, 2016).

4.7.2 Eskom supervisory staff

Eskom's in-house security supervisory staff members are deployed to manage and supervise the in-house and private contract security officers working at Eskom facilities. An increasing standard of professionalism is being implemented throughout Eskom facilities where in-house security is deployed because of the increasing presence of Eskom supervisory staff that is deployed for each shift. The increased professionalism is driven by the Eskom code of conduct and by the regular training and awareness programmes arranged by Eskom management to improve the skills of the supervisory staff (Eskom, 2016).

4.7.3 Vehicles

Eskom in-house security units are well resourced and have the necessary security equipment. Fully armoured patrol vehicles are supplied, with patrol officers, at each of Eskom's power stations. These vehicles are required to improve policing visibility and to act as deterrents for any emerging threats. These vehicles monitor and conduct surveillance duties at the power stations. It has to be borne in mind that however well designed the vehicles may be, the Eskom patrol officers that operate these vehicles and work in these teams receive on-going training and development to behave and act professionally at all times (Eskom, 2016).

4.7.4 Firearms

Eskom security officers are equipped with 9 mmP handguns, 12 bore shotguns and LM4 rifles (5,56 mm). All these firearms are used in strict compliance with the South Africa's current firearms regulatory framework, which consists of the Firearms Control Act (FCA), 60 of 2000, and its subsidiary legislation, which has been in place since 2004. This framework imposes strict substantive and procedural requirements for obtaining a competency certificate, licence, permit, and authorisation to possess a firearm.

There is an armoury manager working in Eskom Head Office (Megawatt Park) that is responsible for all the firearms at Eskom. The armoury manager conducts regular audits on the firearms to ensure that they are in good working condition and that strict compliance is maintained over the management of these firearms (Eskom, 2016).

4.7.5 Personal Protective Equipment (PPE)

Eskom provides a Level III bullet-proof vest, safety boots and jackets to all in-house security officers. Eskom has control of the quality and appearance of the PPE issued to its in-house security officers (Eskom, 2016).

4.8 HOW EFFECTIVE IS ESKOM IN-HOUSE SECURITY IN PREVENTING CABLE THEFT?

According to Eskom's ENECC report (2015), the Generation environment where Eskom employs in-house security officers experiences, on average, fifteen (15) cable theft incidents per month, to the value of between a hundred thousand rand and five hundred thousand rand (R100 000.00 – R500 000.00). This is to be compared with the Distribution environment that experiences between 150 and 180 incidents per month, to the value of almost R2.5 million. The Transmission environment experiences, on average, twenty-five (25) incidents per month, to the value of R1.5 million.

The researcher wishes to point out that the Distribution environment has almost three to five times more facilities than the Transmission and Generation environments. Private security is not deployed to all the facilities at Eskom and the number of incidents and value reported is an estimated figure, which includes theft of cables from Eskom's open networks. The figures reported are limited to only the information reported on the CURA system. The researcher

also wants to further point out that, due to the confidentiality of the ENECC report, the actual losses reported cannot be made available in this study.

4.9 ESKOM'S NEW PROJECTS AND ITS IMPACT ON IN-HOUSE SECURITY DEPLOYMENT

The researcher would like to provide the reader with information on Eskom's new build projects (Medupi, Kusile and Ingula) that will have a severe impact on Eskom's in-house security for the future. These projects have not been included in detail in this study because these sites have not, as yet, been commissioned (with the exception of unit six at Medupi, see section 4.9.1):

4.9.1 Medupi Power Plant and its current security challenges

Medupi Power Station is a dry-cooled, coal-fired power station being built by Eskom near Lephalale in Limpopo province, South Africa. After completion, the power station will have six boilers, each powering an 800 MW turbine, together producing 4800 MW of power. It is expected to become the largest dry-cooled, coal-fired power station in the world. The first unit (unit six) was commissioned on 02 March 2015. This unit is now actively connected to the national power grid (http://www.eskom.co.za/news/Pages/MedupiSync.aspx).

According to an article published in FIN24 on the 06 May 2015 (http://www.fin24.com/Economy/Eskom/Delays-at-Medupi-as-strike-enters-6th-week-20150506), labour unrest has been plaguing Medupi. Many employees experienced violence and intimidation at the accommodation areas where employees reside. These areas are also situated on route to the project site. (http://www.fin24.com/Economy/Eskom/Delays-at-Medupi-as-strike-enters-6th-week-20150506).

Gernetzky (2015) says that Medupi, which employs nearly 14 000 people, has been experiencing labour unrest problems since 25 March 2015. Workers at the plant went on a sporadic protest march, which devolved into eight weeks of a full-blown unprotected strike. The majority of the workforce had to stay away from work because of intimidation (Gernetzky, 2015; http://www.bdlive.co.za/national/labour/2015/05/19/thousands-of-medupi-workers-return-to-site). These wildcat strikes caused the project to be overdue by more than two years, at a cost estimated at more than R35billon over budget. In 2007, the estimated cost of the project was R78billion, which was to include all six operating units (Gernetzky, 2015;

http://www.bdlive.co.za/national/labour/2015/05/19/thousands-of-medupi-workers-return-to-site).

Cordeur (2015) mentions that Radio 2000 reported that police and private security officers used rubber bullets to disperse striking workers at staff hostels in Lephalale during the March 2015 strike (Cordeur, 2015; http://www.fin24.com/Economy/Irvin-Jim-steps-in-as-Medupi-unrest-intensifies-20150410). The researcher wishes to confirm the high levels of violence currently experienced at Medupi.

Medupi is expected to become a National Key Point (NKP) site when the construction has been completed, and in terms of Eskom's strategic plan, it will have in-house security guards, as are deployed to Eskom's NKP sites according to standard procedures.

4.9.2 Kusile Power Station

Kusile power station is currently being constructed in Mpumalanga, South Africa. The construction of this power plant began in August 2008 and is expected to be completed by 2018. It is expected to become the world's largest coal-fired power plant, when completed. Kusile is the first South African power facility to incorporate wet flue gas desulphurisation (FGD) technology, and the second coal-fired power facility being built by Eskom to generate 4 800MW of power, once it is fully operational.

Kusile power station is also expected to become a National Key Point (NKP) site when the construction is completed, and in terms of Eskom's strategic plan, in-house security guards will also be deployed at Kusile.

4.9.3 Ingula Pump Storage

The Ingula Pumped Storage Scheme (previously named Braamhoek) is currently being constructed by Eskom, and a company called CMC Impregilo Mavundla Joint Venture, in the Drakensberg which constitutes the border between the KwaZulu-Natal and Free State provinces, South Africa (https://en.wikipedia.org/wiki/Ingula_Pumped_Storage_Scheme).

The pumped-storage hydroelectric scheme consists of an upper dam and a lower dam, 4.6 kilometres apart, connected to a power station by tunnels (https://en.wikipedia.org/wiki/Ingula_Pumped_Storage_Scheme). The scheme is being built at a cost of US$3.5 billion (originally calculated as the equivalent of R25 billion). The

construction began in 2005 and the power station was scheduled to begin operations in 2015. The Ingula power plant is currently still under construction (https://en.wikipedia.org/wiki/Ingula_Pumped_Storage_Scheme).

Ingula pump storage will also become a National Key Point (NKP) site when the construction has been completed and in terms of Eskom's strategic plan, will have in-house security guards. This means in practice that well trained and sufficient numbers of guards will guard this NKP.

4.10 EQUESTRIAN ASSESSMENT

During October 2013, a feasibility study was conducted by the researcher to provide Group Security (GS) with recommendations for introducing an innovative and sustainable method to use an in-house mounted unit at Eskom to patrol the power stations. The objectives of the study included gaining an understanding of mounted units, giving a description of the current enforcement problems at Eskom which necessitate the introduction of mounted units, identifying the areas where these units would be more suitable to deployment, quantifying the cost implications of introducing the mounted units, ascertaining the maintenance requirements of the horses, defining the legal requirements to operate a mounted unit, and describing the training aspects for both the riders and the horses of the mounted units.

The researcher supplied the research report to Group Security, recommending that further research be conducted on the logistical arrangements which must be put in place at each of the locations where this service would be required. This project is currently on hold, pending further review.

4.11 SUMMARY

The purpose of this chapter was to discuss research objective four (see section, 1.8.4), which was to discuss Eskom's in-house security and cable theft. This chapter has laid the foundation to explain, in a more meaningful manner, the set-up of Eskom's in-house security structures (see section 4.1).

The researcher explained the meaning of in-house security at Eskom (see section 4.2) and Eskom's minimum PSIRA and legal requirements for their in-house security officers (see section 4.3). The origin of Eskom's in-house security (see section 4.4) and where Eskom has its in-house security deployed (see section 4.5), followed by the difference between the in-

house security and the private security (see section 4.6) were all described. Eskom's in-house security resources (see section 4.7) and the effectiveness of Eskom's in-house security in preventing cable theft (see section 4.8) were discussed.

This was followed by an explanation of Eskom's new projects and their impact on in-house security deployment (see section 4.9). Finally, the researcher provided information on an equestrian assessment that was done in October 2013 (see section 4.10), and concluded this chapter with a summary (see section 4.11).

Chapter Five discusses private security and cable theft at Eskom.

CHAPTER FIVE
PRIVATE SECURITY IN ESKOM AND CABLE THEFT

5.1 INTRODUCTION

While Chapter Four focused on the in-house security at Eskom, this chapter looks at what private security officials must do to prevent cable theft. This is in line with research aim 1.8.5, set out in Chapter One under section 1.8, "RESEARCH AIMS".

In this chapter, there are three questions for consideration:

- Why do the private security guards not prevent cable theft from Eskom effectively enough? (see section 5.8).
- Why do private security supervisors not prevent cable theft from Eskom in an effective manner? (see section 5.10); and
- Why do the security company managers/directors/owners not prevent cable theft from taking place?

A main thrust of this chapter is the discussion of salient aspects pertaining to private security and cable theft in Eskom. It is therefore within this context that the meaning of private security in Eskom will be discussed.

5.2 THE MEANING OF THE TERM 'PRIVATE SECURITY' IN ESKOM

The term 'private security' in Eskom refers to the private security companies that have a legal contract with Eskom to secure and protect its business and critical infrastructure. These private security companies must be fully compliant with the requirements for registration in terms of section 21 and 23 of the PSIRA Act, 56 of 2001, before they can be permitted to provide a security service to Eskom.

The Private Security Industry Regulatory Authority (PSIRA) is a statutory regulatory body that sets the industry standards for the registration and training of security employees. In addition to the PSIRA registrations, these security companies must be registered in terms of Section 13 (1) of the Companies Act No 71 of 2008 ('Companies Act') as an incorporated

company in South Africa. The security officers deployed to Eskom sites must be registered with PSIRA, according to the respective security grade as required by Eskom.

While not all Eskom facilities hire private security companies which provide security guards with firearms (armed guards), there is a requirement at all the NKP sites, as well as a few non-NKP sites, for security guards to carry firearms. The private security companies providing Eskom with an armed service must be fully compliant with the Firearms Control Act (Act 60 of 2000) in additional to the PSIRA Act. The PSIRA Act requires PSIRA to keep a register of every service provider registered in terms of the PSIRA Act.

The oversight functions covering private security guards are shared by Group Security business partners and the divisional security units to ensure that the security guards, who need to carry any firearms, have valid firearm competency certificates (See Section 4.3) before any firearm can be issued. A further requirement is that all the security guards must attend two firearm training sessions per year. Although the Firearms Control Act, 60 of 2000 (Regulation 21), only requires one session per year, Eskom insists on two training sessions per year (see section 4.3).

Private security companies providing security services at a National Key Point (NKP) site must fully comply with the National Key Points Act, 1980. All the security guards must complete the necessary NKP training (Unit Standard 246693) before deployment to an Eskom NKP site.

5.3 BRIEF REMARKS ABOUT THE PRIVATE SECURITY INDUSTRY IN SOUTH AFRICA

Eastwood (2013) says there are nearly 9 000 companies and 400 000 registered, active private security guards, which amounts to more numbers than the police and army combined. Wilkinson (2015) mentions that by comparison, the South African Police Service employs 194 852 people, of whom 103 746 are employed in visible policing and 6 331 are employed in protection and security services. Swingler (2016) says that South African citizens are spending more money (R45 billion a year) on private security than they have ever done in the previous years. Swingler (2016) further mentions that this amount is a third more than the government spent on the police in 2016, which makes South Africa's private security industry the fourth largest in the world per capita.

Swingler (2016) says that there are 490 000 active private security officers in South Africa and working in armed response, cash-in-transit, and guarding. Swingler (2016) makes a comparison with the private security officers by mentioning that the SAPS employs 194 852 people and that the SANDF's total military force (excluding reserves) is 77 597. This means that the number of active private security officers in South Africa is nearly double the size of the SAPS and SANDF, combined. Wilkinson (2015) showed that in 2015, South Africa had 2.57 private security personnel for every police employee. In 2015, Wilkinson (2015) placed South Africa in fourth place, behind Guatemala (6.01), India (4.98) and Honduras (4.88), for having more security personnel than police officers.

Swingler (2016) believes that the fear of crime has led to increasingly militarised suburban armed response companies. Swingler (2016) mentions that people in South Africa are spending large sums on so-called 'tactical response' units. One South African security company markets itself as "the most feared and effective armed response company in the country", while another offers SWAT (special weapons and tactics) capabilities and advertises its services with a photograph of two of the company's officers holding LM5 carbines, the semi-automatic version of the South African police and military-issue R5 carbine (Swingler, 2016). The Private Security Regulatory Authority (PSIRA) is the body responsible for regulating the security industry in terms of the Private Security Industry Regulatory Act 56 of 2001 (see section 5.2).

5.4 ORGANOGRAM OF ESKOM'S REGIONAL SECURITY STRUCTURES FOR TRANSMISSION (TX) AND DISTRIBUTION (DX)

Figure 5.1 below shows an organogram of the Eskom security structure for the Transmission (TX) and Distribution (DX) environments.

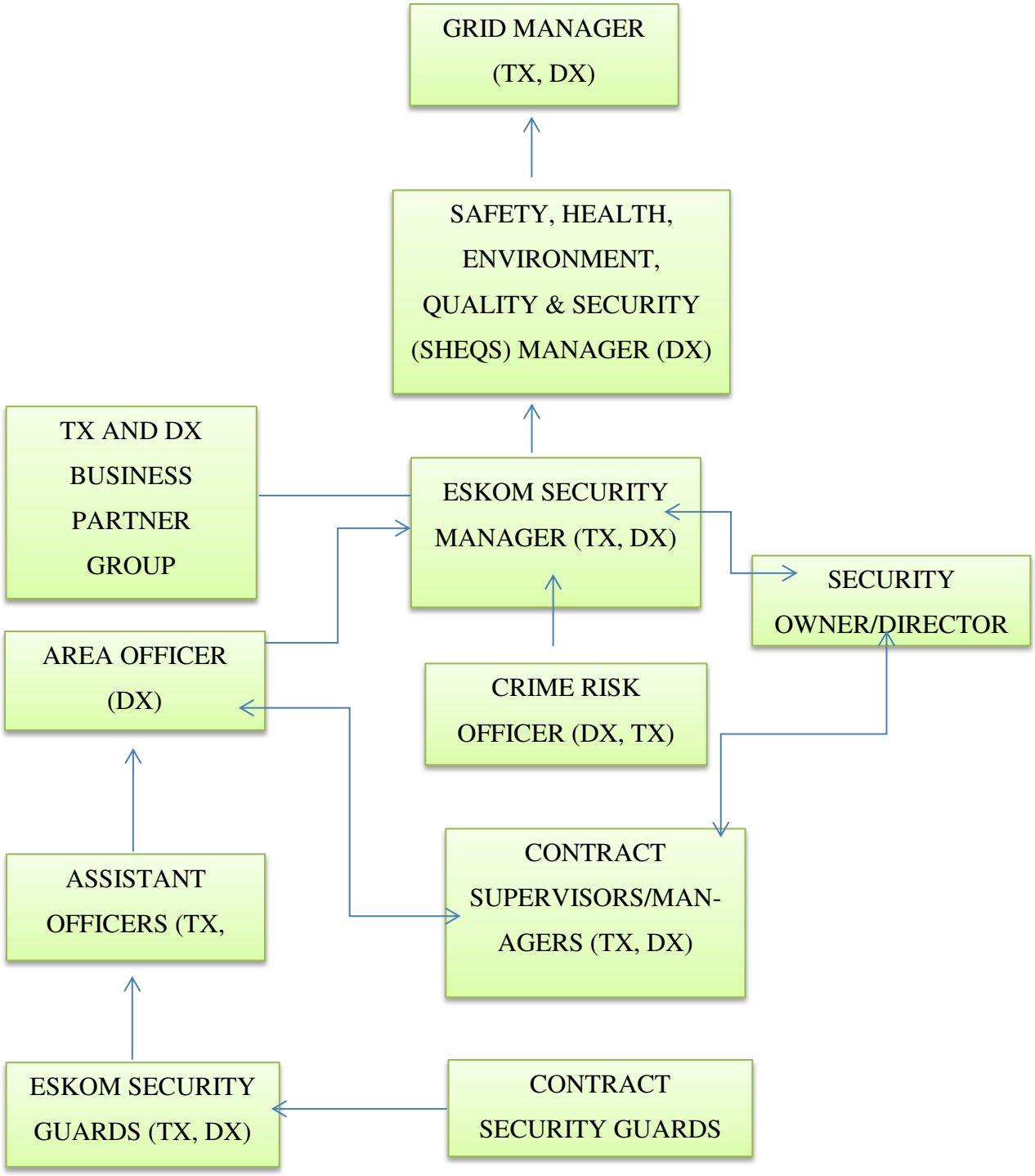


Figure 5.1: An organogram of the security structure for the Eskom Transmission and Distribution business units in the various regions

5.5 ORGANOGRAM OF ESKOM SECURITY STRUCTURES FOR GENERATION (GX)

Figure 5.2 below shows an organogram of the Eskom security structure for the Generation (GX) environment.

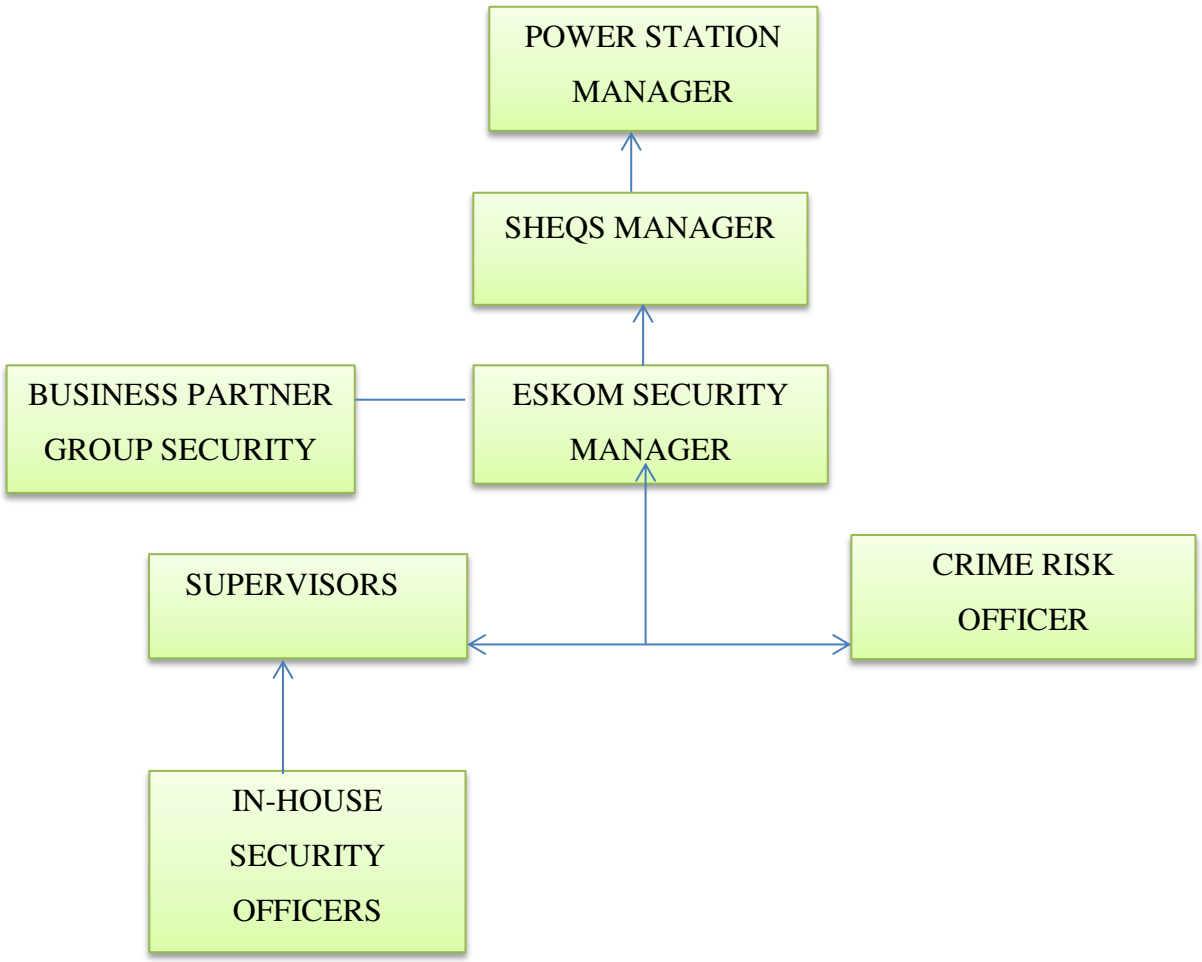


Figure 5.2: shows the organogram of the security structure for the Generation (GX) business unit

5.6 ROLE PLAYERS AND THEIR DUTIES TO REPORT CABLE THEFT

The researcher believes it is pertinent to provide an overview of the various roles played by the various reporting structures in security in reporting cable theft at Eskom. The following personnel / groups are involved:

The private security guard

The private security guard is responsible for the security services at the Eskom facility and has a duty to report any incident and break-in to his or her control centre. The security officer must notify the control room and the armed response unit of the incident.

The control room/centre

The control room/centre is responsible for communicating with the armed response units and the police, supervisor, security manager and, in certain cases, the Eskom site manager/supervisor and Eskom security personnel to notify them of the cable theft incident.

The contract security manager

The main role of the contract security manager is to communicate with Eskom on the incident, to provide leadership for improving the performance of the private security personnel, and to improve the quality of protection for the Eskom facilities.

Eskom security manager

The main role of the Eskom security manager is to communicate with Eskom's top management on the incident, to provide leadership for improving the performance of the private security personnel (including the contract security manager), and to improve the quality of protection for the Eskom facilities. The problem is that the feedback goes to people who have financial power, but do not have expert security knowledge to make informed security decisions.

The Eskom investigator

The role of the Eskom investigator is to register the case on the CURA system and investigate the cable theft incident. He or she is thereafter responsible for providing a report to the security manager with his or her findings and recommendations on the actions steps that must be taken to prevent further theft of Eskom property.

Eskom's crime analysts

The role of the Eskom crime analysts is to gather the relevant crime data from the CURA system on a monthly basis and distribute it in the form of an ENECC report to the relevant role players within Eskom.

5.6.1 Role players duties when cable theft incidents occur

Table 5-1 below depicts a route map for reporting cable theft at Eskom.

Table 5-1: Route map for reporting cable theft at Eskom

Role player's duties and who to contact when cable theft incidents occur	
Security Guard	Control room
Control room operator	Armed response company Police Supervisor Contract security manager Eskom security manager
Contract security manager	Eskom site manager Company owner
Eskom security manager	Crime risk officer Area officer
Eskom's investigator	Register the case on CURA, investigate and provide a report to the security manager, update the CURA system
Eskom's crime analysts	Retrieve information from CURA and compile ENECC report for the Eskom community

5.7 THE BASIC REQUIREMENTS FOR SECURITY COMPANIES THAT WISH TO RENDER A SERVICE TO ESKOM

The criteria for private security companies wishing to provide security services to Eskom are the following: they must be registered with The Private Security Industry Regulatory Authority (PSIRA), the Registrar of Companies and SARS; and be registered for Compensation of Occupational Injuries and Diseases (COID). Each of the managers,

directors, executives, members, partners or trustees must be registered with PSIRA and have a recognised grade B qualification (in terms of Section 23 of the PSIRA Act, 56 of 2000).

Eskom, in its written contracts with the security companies, expects these security companies to specifically comply with the following applicable laws: the Basic Conditions of Employment Act, 75 of 1997; SARS Act, 34 of 1997; Tax Administration Act, 2011; PSIRA Act, 56 of 2001; PSIRA Levies Act, 23 of 2002; National Key Point Act (NKP), 102 of 1980; The Code of Conduct for Security Service Providers, 2003, prescribed by the Private Security Industry Regulation Act, 56 of 2001; the Labour Relations Act, 66 of 1995 (South Africa, 1995, 1997, 2001(a), (b), 2003); Firearms Control Act, 60 of 2001; Unemployment Insurance Act, 63 of 2001; applicable Municipal bylaws; and the Minimum Information Security Standard (MISS).

New firearm training requirement: On the 6 March 2015, Lieutenant General Setloe, the Deputy National Commissioner of Policing for the South African Police Service, issued a notice to all police officials in respect of new quality assurance requirements, designed to combat fraudulent firearm training certificates being used by some applicants. Firearm training certificates will no longer be accepted if these training certificates are not accompanied by the PFTC's (Professional Firearm Trainers Council, a regulatory body for South African firearms instructors) statement of results (Ras, 2015b).

This means that no firearm training institution may issue a Firearm Training Certificate for the purposes of applying for a Competency Certificate or a firearm licence, if it is not accredited by the PFTC and if the certificates are not accompanied by a statement of results issued by the PFTC (Ras, 2015b).

5.8 WHY DO THE PRIVATE SECURITY GUARDS (PSG) NOT PREVENT CABLE THEFT AT ESKOM?

The researcher has identified possible reasons (see section 5.8.1 – 5.8.7) as to why the private security guards cannot prevent cable theft at Eskom. Certain issues were identified in questions, which led to the formulation of security-related statements (see section 5.8.1 – 5.8.7) which were put to fifty-five (55) participants, comprising Eskom employees, contract security supervisors, and contract security managers and directors/owners (see Table 5-2 below).

For the purposes of this study, the researcher decided to collate the responses from the 55 participants (see section 2.7.1-2.7.4) interviews, conversations and the focus group discussions (Cf. Chapters Five and Seven) into tables. This basically means that during the data analysis, the data was broken down into smaller, meaningful parts according to the set research objectives described in Chapter 1 (see section 1.9). Berg (2007:3) says that qualitative research refers to the meanings, concepts, definitions, characteristics, metaphors, symbols, and descriptions of things." The number, or numerical descriptions of things and their relationships are not the focus of this qualitative research, which utilises the focus of the "other" form of social science research: quantitative methods. The researcher utilised elementary data statistics to represent the percentages of participants that *"Agree", "Disagree"* or are *"Unsure"* with the security statements discussed. The data will be presented using tables.

The security-related statements that were put to participants, when conducting research for this thesis, were:

5.8.1 Security guards are not adequately trained to protect Eskom facilities and identify Eskom's cables

According to Jenkins (2015), one of the reasons that has increased the crime levels at Eskom facilities, and for private security being tremendously unsuccessful, is the fact that the security officials are not properly trained and equipped to protect Eskom. This interpretation of the concept of training presupposes that the security guards cannot work effectively unless they are given the appropriate training to produce the security services that must meet acceptable standards in terms of quality, as reflected in the security objectives of Eskom security.

Nkabinde (2014) says that the private security officers working at an Eskom facility are doing their work, but not effectively, as they should. He mentions that in some instances, cables are stolen while the security guards are on duty. Some of the security officers also have a negative attitude in the execution of their duties, while in some cases the guards help themselves to the cables.

Nkabinde further mentions that incidents which happen in the field where there are no guard/s deployed is understandable (as there is nobody monitoring those lines), but where

cables are stolen from the premises/yard where the security officers are deployed, it is unacceptable (Nkabinde, 2014).

The researcher further ascertained that the security officers working on Eskom facilities cannot identify Eskom cables. The researcher further discovered that the guards cannot tell the difference between Eskom copper cables and Eskom aluminium cables. The reason for this problem rests with Eskom security staff (Moonsamy, 2015; Krause, 2014).

Participant 21 mentioned:

"*… While we (security company managers) know it is our job to protect the assets on site, we also should be guided by Eskom to help us identify and protect the exposed material in a confined space ….*"

According to Moonsamy (2015) and Krause (2014), Eskom must determine what steps are necessary to protect Eskom property, and security should follow these instructions carefully. The guards should comply with the rules of access and protocols which should be provided by Eskom security upon induction of security when new contracts are put in place (Moonsamy, 2015; Krause, 2014).

The participants in the study reported that what mattered most was the right balance among the duties and tasks performed by the security guards while they are on duty at an Eskom facility. Security guards are expected to do their basic work, as well as be able to identify the products and materials that they are guarding. The information which emerged strongly from the interviews was that the central problem was that of combining security requirements of daily protection duties with non-security tasks of having to teach the security officers about Eskom's cables, their value and importance.

This study found that most security personnel of security companies are inducted during the commencement of a new contract and that clear instructions are given to the companies to protect Eskom assets, although in most cases, no training or instructions are given by Eskom personnel to the security guards and company management on the identification of what assets are on site and the value of such assets. This evidence points to a clear need for training and professional development.

Security guards, supervisors and all those who are functionally involved in the security operations need to receive training in areas such as identification of Eskom property, security

site procedures, security dress and equipment for the specific facilities, and so on. Indeed, for as long as human security is required to protect Eskom facilities, there will be need for training, and for as long as the training is needed, security officers' development should be as effective as possible.

Moonsamy (2015) and Krause (2014) say that one of the most challenging tasks that a security guard will have to deal with is the issue of the removal of Eskom materials from a work site. Eskom staff members routinely leave material (cable, steel, bolts, etc.) lying around the site, without confining it to a secure, and where possible fenced, area on site.

Highlighted in the study is the need for security officers to report exactly what they discover during routine patrols. In order for Eskom to improve the quality of the security officers reporting and competency skills, booklets of Eskom assets with the necessary training must be provided to them (see section 8.7).

Table 5-2: Security guards are not adequately skilled and trained to protect Eskom facilities and identify Eskom's cables

Theme	Agree	Disagree	Unsure
Security guards are not adequately skilled and trained to protect Eskom facilities and identify Eskom's cables	50 (90.91 %)	2 (3.64 %)	3 (3.64 %)

As shown in Table 5-3 above, 90.91 % (50 out of 55) of participants agree that security guards are not adequately trained to protect Eskom facilities or to identify Eskom's cables. However, 3.64 % (2 out of 55) of the participants disagree, with participant 40 saying *"We know what some of Eskom cables look like but we don't know its use or identification name"*, while 3.64 % (3 out of 55) of the participants were unsure or did not comment.

5.8.2 Lack of proper observation and reporting skills

Nkabinde (2015) and Booysen (2014) aver the guards do not prevent or detect intrusion early when the criminals are trying to gain entry and as a result the criminals are confronted when it is too late. Ogle (2014) believes that the guards often get comfortable in the guard room and do not patrol the site as they are required to do in terms of their job descriptions. Baccus

(2015) mentions that some guards lack concentration at night (and sometimes during the day) because they sleep every chance they get.

This evidence points to a clear need for training and professional development to improve the skills of security guards. Security guards need to be equipped with the necessary skills and they should incorporate these skills into their professional work activities so that the benefits of having professionally trained security personnel may follow and benefit Eskom.

One of the most important skills a security officer must possess is to observe and report information accurately, as he or she has observed it. Security officers must be extremely observant and detailed oriented (Maxwell, 2014; Nkabinde, 2014).

Krause (2014) found that often security guards possess the skill of observing through experience or common sense, but they lack proper reporting skills. They do not record all required information or fail to register the appropriate report with the control room. Nkabinde (2014) avers that the most important tools which security officers use are the daily activity reports, incident reports and access control information.

Security guards must record the pertinent information which Eskom needs to control access and to protect their assets entering or leaving the premises. Nkabinde (2014b) mentions that he noticed many of the company supervisors train the security officers by explaining to them that their job requires them to observe and report, but he adds that telling the security officers what to do is not good enough; they must be told what they should be looking for and what the risk factors to Eskom are. They should be trained to write relevant reports and taught about what information needs to be conveyed through those reports (Nkabinde, 2014).

In order for Eskom to improve the quality of security provided through private security contractors, it is important to assess the effectiveness of the security officers and their skills sets, and to align these with Eskom's requirements.

Table 5-3: Lack of proper observation and reporting skills

Theme	Agree	Disagree	Did not comment
Lack of proper observation and reporting skills	34 (61.82 %)	21 (38.18)	0

As shown in Table 5-4 above, 61.82 % (34 of 55) of the participants agree that the lack of proper observation and reporting skills is one of the reasons why private security guards cannot prevent cable theft from Eskom. However, 38.18 % (21 of 55) disagree, citing various reasons for their disagreements. Participant 9 said that *"They (security guards) are observant at all times but the Eskom sites are too big to look everywhere"*, while participant 3 said *"There should be a procedure put up in the guard room for reporting"*.

5.8.3 Security officers are distracted by their mobile phones while on duty

Characteristics of being observant are important because they enable the security guards to identify security risks earlier and to react sooner so as to prevent criminals from harming them or the facility they are protecting. This characteristic is also important for enhancing the security officers' understanding and recognition of this important security skill.

The above discussion about the characteristics of being observant has revealed that it is impossible to provide a comprehensive definition of this important security skill, although the study found that the biggest contributing factor to the security guards not being observant is the distraction of their mobile phones. The researcher has on a number of occasions observed private security personnel at a number of Eskom facilities in Gauteng, Free State and KwaZulu-Natal and found that many of the security officers were playing games on their mobile phones, talking on their mobile phones, and typing on the keypad, instead of observing the site for criminal activity.

The researcher, during site inspections at two different substations in KwaZulu-Natal (Mersey substation, 12 September 2014; Athene substation, 22 September 2014), observed security officers talking on their mobile phones while attending to visitors entering the main gates. The security officers were notified of their wrongful actions and sent for corrective in-house training by their respective company management representatives.

Table 5-4: Security officers are distracted by their mobile phones while on duty

Theme	Agree	Disagree	Did not comment
Security officers are distracted by their mobile phones while on duty	49 (89.09 %)	4 (7.27 %)	2 (3.64 %)

According to Table 5-5 above, 89.09 % (49 out of 55) of participants agree that the mobile phones cause distractions to the security officers while they are on duty, 7.27 % (4 out of 55) of the participants disagree, while 3.64 % (2 out of 55) of the participants did not comment.

5.8.4 Security officers sleep on duty (from 23h00 to 03h00)

The researcher discovered (Eskom investigation reports, 2014-2015) that Eskom's cable theft incidents (and criminal activity) occur at its facilities from between 23h00 to 04h00. The high crime incidence times at Eskom facilities are between 01h00 to 03h30.

The study discovered that 12-hour shift cycles have seen the levels of tiredness increase, concomitantly with the increasing number of hours worked by the security officers, and that this is more pronounced during the second half of a shift, especially between 00h00 and 06h00.

The researcher found through his experiences, and through this research study after site visits were conducted, that the most common problem experienced with the security officers at Eskom facilities is a high level of drowsiness when they are supposed to be wide awake and alert. Increased feelings of fatigue and drowsiness at work make it difficult for the security officers to maintain concentration during work hours.

The researcher found through his experiences and this research study that this increased level of fatigue is caused by the security companies' poor planning in terms of the allocation shift work and their having no contingency planning in place for frequent absenteeism. Additional work is required from security officers on their rest days who have to replace others that are absent from work.

From the above information, it becomes clear that it is essential that security managers must understand the concept of high crime incidence times in order for them to gain a clear picture of how they must manage, and how Eskom should benefit from the security programmes that they pursue, in order to ensure that their employees remain awake and alert during the high crime incidence times.

Table 5-5: Security officers sleep on duty (from 23:30 to 04:00)

Theme	Agree	Disagree	Did not comment
Guards sleeping on duty	49 (89.09 %)	3 (5.45 %)	3 (5.45 %)

According to Table 5-6 above, 89.09 % (49 out of 55) of participants agree that guards sleeping on duty is one of the reasons why they cannot prevent cable theft from Eskom. On the other hand, 5.45 % (3 out of 55) of the participants disagree, while 5.45 % (3 out of 55) of the participants did not comment.

5.8.5 Effective and dependable security patrols are not conducted consistently during the shifts (mostly at night)

Maxwell (2014) believes that the main purpose of a patrol is to maintain the security of the premises under the security officer's authority. Krause (2014) says that the preparation for a patrol should always begin with an understanding regarding the purpose of the patrol. The security officer needs to understand why patrols must be done and what equipment is to be used while on patrol.

Nkabinde (2015a) and Booysen (2014) believe that the main reason for the security guards not conducting the security patrols at Eskom facilities after hours is the lack of guard monitoring equipment to monitor their patrol activity. However, the researcher records that Eskom does have a few sites where guard monitoring systems are installed, although many of these systems are outdated.

Nkabinde (2015a) and Booysen (2014) aver that most security officers do not patrol the site. While most incidents occur at night (23h00 to 04h00), it is very difficult to establish accurate times for these incidents because guards discover the break-ins in the morning when they hand over or when the dayshift guards do the first patrol (usually at 04h30 or 05h30) (Nkabinde, 2015a; Booysen, 2014).

Nkabinde (2015a) and Booysen (2014) say that there is only one compulsory patrol, which is done during shift changes. This is done to prevent the security officers taking accountability for incidents which occurred during the shift being relieved.

The researcher, through his personal experience, agrees with the comments made by Nkabinde (2015a) and Booysen (2014). Security officers are often very reluctant to go out and patrol, despite being partnered with a colleague and being issued with firearms and brightly lit torches. This statement makes it very clear to any 'security person' that there is definite and deliberate action on the part of the security officers to record occurrence book (OB) entries that reflect 'All in order' as an indication of a physical patrol, although it was not physically done.

The researcher through this study, in collecting data by doing site inspections, found entries in the OBs which had been recorded in advance. The researcher, during this study, visited a number of Eskom substations in Gauteng (Central region report 02-03 October 2014) and ascertained that the recording of patrols in advance in the OB is an indication of deceit on the part of the security guards involved.

However, what is clear when analysing the deceit of recording dishonest, non-existent patrols, is the fact that any form of corrective action necessitates some specific form of intervention that is specifically directed at changing the mindset and behaviour of security officers. From a practical point of view, it is logical that any system change can only happen once Eskom decides to provide funding for new and advanced technology to monitor patrol activities and to intervene immediately when there is a breach in the system. It is now the time for the security services to play an honest role in the prevention and control of crime, which is more pressing than ever before (Fischer *et al.,* 2008: 41).

Effective management is central to all good security management practice, principally because the activities involved in developing and teaching security officers differ in key respects from conventional methods of training. The administrative structures within which the security officers operate have a significant influence on their ability to be effective. It is for this reason that the security managers need to structure their operations to carry out inspections on the manner and method in which the security officers patrol and to improve in areas where they find faults.

Table 5-6: Effective and dependable security patrols are not conducted consistently during the shifts (mainly at night)

Theme	Agree	Disagree	Unsure
Effective and dependable security patrols are not conducted consistently during the shifts (mainly at night)	36 (64.45 %)	10 (18.18 %)	9 (16.36 %)

According to Table 5-7 above, 64.45 % (36 out of 55) of participants agree that security guards do not patrol effectively and honestly, 18.18 % (10 out of 55) of the participants disagree, while 16.36 % (9 out of 55) of the participants were unsure or did not comment.

5.8.6 Inadequate protection for security officers causes them to feel unsafe and not committed to their jobs

The researcher here refers to security officers not having immediate access to armed response services, functional security equipment (torches, batons, handcuffs) and bullet proof vests.

Jenkins (2014) argues that the security support systems are inadequate because all private security officers should have access to a panic unit, linked to an armed response service that should be located in close proximity to where they are deployed. While obtaining information for this study, the researcher found that Jenkins has a valid argument because many of the security officers did not have access to panic buttons that are linked to a reliable armed response service, and that instead they make use of their private mobile phones to contact their control room operators to report on the site situation. The torches supplied by the private companies were inadequate and some were not functional.

The researcher believes that Eskom security management should evaluate the standard equipment requirements for private security companies in a more critical manner. A more critical evaluation will assist in improving the quality of all security service standards being provided to Eskom and will ensure that the security officers receive higher quality brands of security equipment and armed back-up response, which will make them feel more secure. Most of the remarks by the participants point out what many of the security companies are lacking, or not doing, in order to make their employees feel comfortable to do this risky job.

Meek (2014) says that if guards are not well protected and do not have access to reliable back-up support, then they will not prevent cable theft from Eskom.

Keeping security guards motivated and protected involves much work on the part of both the security companies and the security guards themselves. An effective security programme requires planning, organising and evaluating the development, and the use, of the various forms of communicating tools to evaluate progress. This is a challenging task for the security managers of private companies. Since the security guards are faced with many risks on a daily basis, the challenges to their management are many and require strong leadership and appropriate action.

Table 5-7: Inadequate protection for security officers to feel safe and committed to their jobs

Theme	Agree	Disagree	Unsure
Inadequate protection for security officers to feel safe and committed to their jobs	43 (78.18 %)	8 (14.55 %)	4 (7.27 %)

As indicated in Table 5-8 above, 90.91 % (50 out of 55) of participants agree that inadequate protection to feel safe and committed to their jobs is a real problem faced by the security officers, 3.64 % (2 out of 55) of the participants disagree, while 3.64 % (3 out of 55) of the participants were unsure or did not comment.

5.8.7 Vetting is not done consistently before deployment to Eskom

Eskom requires all private security officers to be vetted prior to them working at Eskom; however, this vetting does not happen regularly. Nevertheless, vetting is the most important task of the private security companies and this task of vetting must take place before deployment to Eskom, and in collaboration with the Eskom security manager. This means that the vetting exercise that is to be done by private security companies should be one hundred per cent in line with what is expected by Eskom and should be in accordance with the Eskom security contract.

What is very important to Eskom is that no security officers must have criminal records, because they are working in positions of trust. Nel (2014) is of the opinion that vetting is one area where security companies save money by using cheaper options of vetting exercises, i.e. by only getting police clearances via PSIRA applications and registration.

A more realistic and permanent solution would be for security companies to contract the vetting process out to accredited vetting companies and for Eskom to monitor this process strictly. Baccus (2015) believes that the low remuneration paid to security officers reflects the cut-throat competition among security firms, who submit the lowest possible bids to win Eskom contracts. Low margin contracts also mean lower profit margins and that less money is available for training and background checks for security guards (Baccus, 2015). These remarks definitely portray a need to change the perceived belief that 'cheap is best'.

In order for Eskom to improve the reliability and credibility of private security personnel, it is important to assess the effectiveness of the vetting compliance programmes and establish what needs to be done to improve it.

Table 5-8: Vetting is not done consistently before deployment to Eskom

Theme	Agree	Disagree	Unsure
Vetting is not done consistently before deployment to Eskom	29 (52.73 %)	20 (36.36 %)	6 (10.91 %)

According to Table 5-9 above, 52.73 % (29 out of 55) of participants agree that vetting is not done consistently before deployment to Eskom, 36.36 % (10 out of 55) of the participants disagree, while 10.91 % (6 out of 55) of the participants were unsure or did not comment.

5.9 PSG PIE SUMMARY CHART

This Pie Chart Summary indicates the percentage of participants (55) that agree with the reasons for why the Private Security Guards (PSG) do not prevent cable theft at Eskom (see section 5.8.1 – 5.8.7)

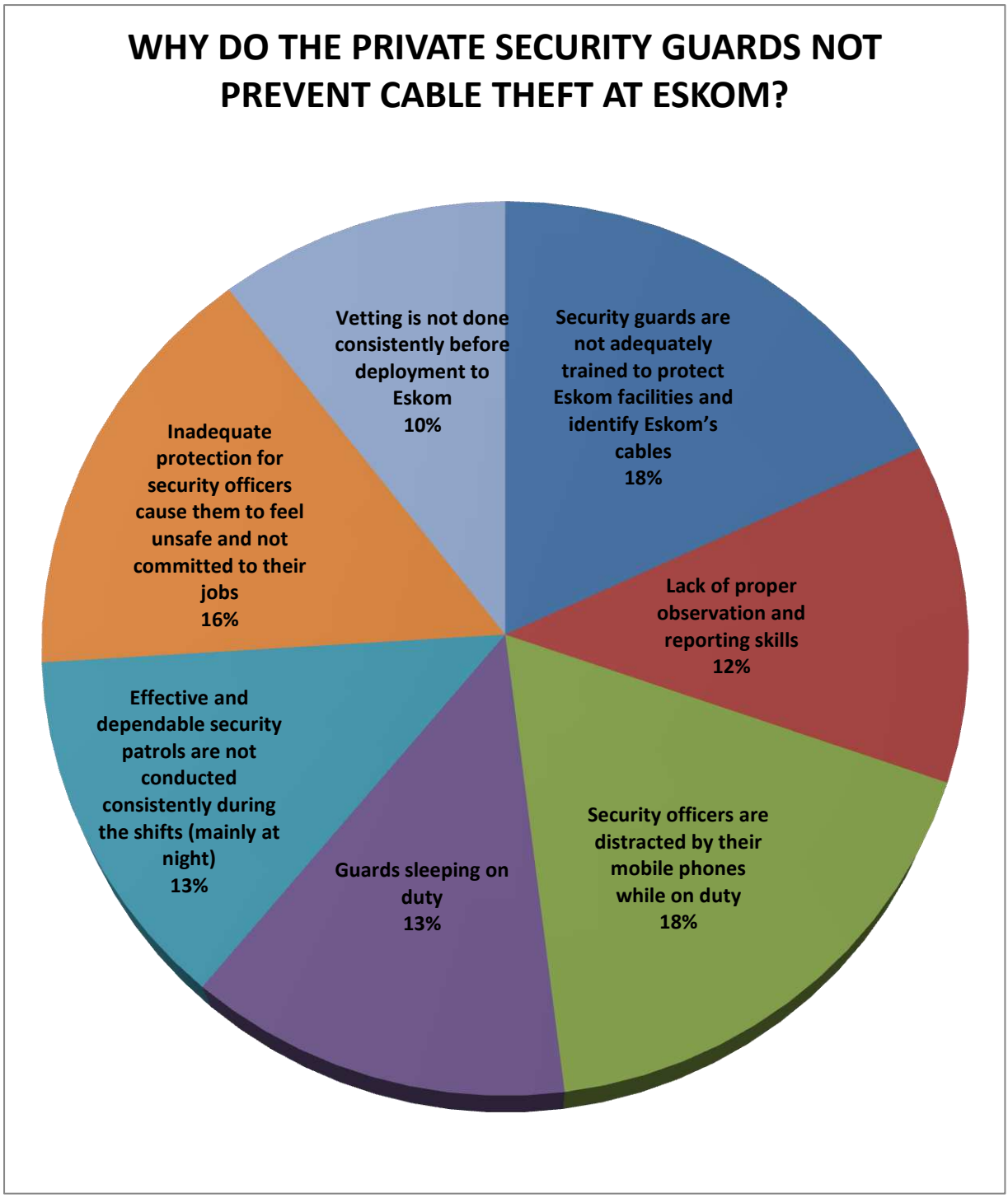


Figure 5.3: Pie Chart indicating the percentage of participants (55) that agree with the reasons for why the private security guards cannot prevent cable theft at Eskom

5.9.1 Explanation of the pie chart

In summary, the evidence of why private security guards seemingly cannot prevent cable theft at Eskom (see section 5.9), which is displayed on the pie chart shown in Figure 5.3 above, indicates (from highest to lowest) that the security guards are not adequately trained to

protect Eskom facilities and to identify Eskom cables (18 %); they are distracted by their mobile phones while on duty (18 %); followed by the inadequate protection which does not allow security officers to feel safe and committed to their jobs (16 %). The security officers are also not consistent during their patrol duty (13 %), which renders them ineffective and less reliable, mostly at night. It was also discovered that they sleep on duty during the night, instead of staying awake to protect the Eskom facility (13 %). The security officers further lack proper observational and reporting skills (12 %). The final issue raised was the fact that the vetting and screening procedures are not done consistently prior to the deployment of the security officers (10 %).

5.10 WHY DO THE SUPERVISORS NOT PREVENT CABLE THEFT AT ESKOM?

The researcher has identified the following possible reasons (see section 5.10.1 – 5.10.6) as to why the supervisors cannot prevent cable theft at Eskom. Certain issues were identified in questions, which led to the formulation of security-related statements which were put to fifty-five (55) participants, comprising Eskom employees, contract security supervisors and contract security managers and directors/owners (see Table 5-10 below).

The following statements were put to participants to investigate the issues described in the following subsections.

5.10.1 The contract supervisors are ineffective, unprofessional and unreliable

Jenkins (2015) mentions that the ineffective and unprofessional management of security guards is one of the biggest reasons why guards cannot perform according to Eskom's security standards. Jenkins (2015) and Baccus (2015) both agree that supervisors have an important role to play, if Eskom wants to prevent cable theft from its facilities. In this regard, during interview 23, participant 23 highlighted the following sentiments and stated:

'*… supervisors make invaluable contributions to the operation if they are committed and well-groomed into doing the job….*"

On the other hand, participant 30 said: *"... How can we show commitment when we are overworked with so many sites to visit in such a short period of time? ... it's impossible ...."*

What becomes clear, and was observed during this study, is that many of the supervisors doing inspections failed to step out of their vehicles to conduct the inspections; they merely complete the occurrence book (OB) while still seated in their vehicles.

The researcher believes that Eskom security management should evaluate the geographical areas assigned to the security companies in a more critical manner so as to make sure that contracts are awarded to companies that are located within close proximity to Eskom's infrastructure. It seems safe to say that supervisors have to drive many kilometres to inspect Eskom facilities, as well as other clients, in a 12-hour shift. It is important to point out that although it is a common practice for companies to tender for security contracts that are not within their areas of control, Eskom must discourage tenders from being awarded to such companies.

The central idea of awarding contracts to local companies will result in Eskom receiving a more professional service from supervisors because they will focus less on rushing to other, distant sites, and more specifically, they will focus on spending more time training and orientating their security officers at the local site (see recommendations in section 8.7).

Table 5-9: The contract supervisors are ineffective, unprofessional and unreliable

Theme	Agree	Disagree	Unsure
The contract supervisors are ineffective, unprofessional and unreliable	49 (89.09 %)	6 (10.91 %)	0

As shown in Table 5-10 above, 89.09 % (49 out of 55) of participants agree that contract supervisors are ineffective, unprofessional and unreliable. Only 10.91 % (6 out of 55) of the participants disagree with this theme.

5.10.2 Relationship problems between supervisors and security guards

For supervisors and security guards to maintain a professional and respectful relationship, it is necessary for them to develop and improve each other's confidence to work as a team. In order to give expression to this philosophical belief in a practical manner, and also to apply

this belief in practice, clear objectives must be developed and implemented by the security companies' human resource departments and implemented by the security managers.

Shearing and Stenning (1983) recognised certain issues with this relationship nearly three decades ago. They said that in order to assess the relationship between supervisors and security guards, one has to recognise and understand the context within which private security operates. Shearing and Stenning (1980) developed this argument by saying that in order to understand the relationship, it is a requirement that the structural context which forms the relationship must be reviewed.

The subject of motivation is of major importance in the security management arena, and more especially in improving relationships between supervisors and security guards. Prompt feedback is very important to security guards for increasing their understanding of company delays, which in most cases regard replacement uniforms and pay disputes. At every level of supervision and management, a variety of strategies needs to be incorporated to optimally assist security guards and thereby motivate them, thus strengthening the relationship between them and their supervisors.

Table 5-10: Relationship problems between supervisors and security guards

Theme	Agree	Disagree	Unsure
There are many relationship problems between supervisors and security guards	36 (65.45 %)	13 (23.64 %)	6 (10.91 %)

As shown in Table 5-11 above, 65.45 % (36 out of 55) of participants agree that there are many relationship problems between supervisors and security guards. On the other hand, 23.64 % (13 out of 55) of the participants disagree with this theme, with participant 42 saying that *"We have a good supervisor who treats us well"*, while participant 45 said that *"We have a good relationship with our supervisor who is always helpful"*. On the other hand, 10.91 % (6 out of 55) of the participants were unsure or did not comment.

5.10.3 Vetting is not done consistently before supervisors are deployed to supervise Eskom contracts

What is very important to Eskom is that no supervisors have criminal records, because they are working in positions of trust, and they have to work closely with the security guards.

Eskom requires that all supervisors be vetted prior to them working at Eskom. In other words, vetting is the most important task of the private security companies and this task of vetting must take place before deployment, and in collaboration with the Eskom security manager.

Table 5-11: Vetting is not done consistently before supervisors are deployed to supervise Eskom contracts

Theme	Agree	Disagree	Unsure
Vetting is not done consistently before supervisors are deployed to supervise Eskom contracts	34 (61.82 %)	13 (23.64)	8 (14.55 %)

According to Table 5-12 above, 61.82 % (34 out of 55) of participants agree that vetting is not done consistently before supervisors are deployed to supervise Eskom contracts. However, 23.64 % (13 out of 55) of the participants disagree, with participant 47 stating *"They took copies of my ID and fingerprints after I was employed as a supervisor"*, while participant 33 said *"if Eskom regularly inspected to ensure that all checks and balances were done, then maybe the security companies will do the vetting consistently".* Lastly, 14.55 % (8 out of 55) of the participants were unsure or did not comment.

5.10.4 Supervisors should do first line investigations only

The very difficult and challenging tasks involved in conducting investigations require a trained and qualified person to be an investigator, with at least a minimum national diploma qualification in investigations from an institution accredited by the South African Qualification Authority (SAQA). What is very important to Eskom is that after an incident has taken place, a full and detailed investigation is done by the private security company to establish the facts of the incident, whether any arrests were made, how the incident took place, and what needs to be done to prevent further incidents from taking place. This involves understanding the new risk profile and adapting by improving the security standard, and preventing the risk from increasing.

What became very clear during the collection of information for this study was that supervisors are required to conduct the entire investigation and supply a report with recommendations after a break-in incident has occurred, instead of qualified and experienced

people doing this job. The researcher discovered that many of the private security company supervisors have no formal qualification or experience for conducting thorough investigations and that the investigation reports lacked professionalism and credibility.

This objective again underlines the important role of the security companies to offer a professional security service to Eskom.

The researcher's opinion is that although a partnership is required between Eskom and the private security companies, the private security companies must make sure that professional and accurate investigations are done. Given a supervisor's heavy workload, it is safe to say that supervisors who carry out full investigations will find it difficult to determine specifically why break-ins occur and further, it will be unrealistic for them to always find facts during the investigations and to provide a professional report that can be used to prevent further thefts from Eskom.

Table 5-12: Supervisors should do first line investigations only

Theme	Agree	Disagree	Unsure
Supervisors should do first line investigations only	49 (89.09)	3 (5.45 %)	3 (5.45 %)

As shown in Table 5-13 above, 89.09 % (49 out of 55) of participants agree that supervisors should not be main investigators, and many of them agree that they should conduct only the first line investigations or first incident of crime, and then hand the investigation over to an experienced and qualified investigator who will not only provide a professional report, but also provide substantial recommendations to prevent further incidents of crime. Nevertheless, 5.45 % (3 out of 55) of the participants disagree, while 5.45 % (3 out of 55) of the participants were unsure or did not comment.

5.10.5 Insufficient support structures for supervisors to remain committed to their jobs

The "*insufficient support structures*" that the researcher is referring to here comprise management support in terms of providing action plans and reviewing mandates with the supervisor; leadership support in terms of assisting the supervisor with counselling the guards; and financial support. Financial support entails providing the resources required to improve security standards, providing resources for the supervisors' development training, as

well as advancing his or her career options, and providing further resources to increase the number of supervisors where supervisors have large geographical areas to cover.

Highlighted and recommended at various stages of this study, is the need for private security companies to take societal responsibility, including providing for the overall development of their supervisors. Jenkins (2015) says the security support systems are inadequate because the supervisors are often not given the necessary support by their company managers and directors. Jenkins (2015) believes that far too often, the supervisors need to wear many hats, other than that of a supervisor only. These include being an investigator, a security guard when there are staff shortages, a security manager and an armed response officer.

Table 5-13: Inadequate support structures for supervisors to remain committed to their jobs

Theme	Agree	Disagree	Unsure
Inadequate support structures for supervisors to remain committed to their jobs	33 (60 %)	14 (25.45 %)	8 (14.55 %)

According to Table 5-14 above, 90.91 % (33 out of 55) of participants agree that support structures, which are inadequate for encouraging supervisors to remain committed to their jobs, comprise a real problem faced by the supervisors. While 25.45 % (14 out of 55) of the participants disagree, 14.55 % (8 out of 55) of the participants were unsure or did not comment.

5.10.6 Supervisors lack the ability to create significant impact on the security officers

Supervisors must set the appropriate tone of behaviour through their individual work performance and impart this to the security officers they supervise. To enable security officers to feel a strong sense of loyalty to their supervisor, and for the supervisor to positively influence the retention of security guards, the supervisor must acquire the ability to a create significant impact on the security officers.

Supervisors are in a leadership role which is aimed at encouraging, supporting and motivating their team members. This important point underlines the fact that supervisors must have the commitment to actively engage with the security officers and to intervene in his or her work programme in order to create a significant impact so as to encourage them to perform better.

The interventions and leadership programmes mentioned by the researcher are based on Henri Fayol's well-known management principles for improving the qualities and leadership skills of a supervisor and for facilitating the supervisor to create a significant impact on his or her fellow security officers (https://www.mindtools.com/pages/article/henri-fayol.htm).

What is very important to Eskom is that the security companies contracted to Eskom must be the driving force behind the implementation of management principles to develop both the security manager and the supervisors.

Table 5-14: Supervisors lack the ability to make a significant impact on the security officers

Theme	Agree	Disagree	Unsure
Supervisors lack the ability to create significant impact on the security officers	34 (61.82 %)	12 (21.82 %)	9 (16.36)

As shown in Table 5-15 above, 61.82 % (34 out of 55) of participants agree that supervisors lack the ability to create significant impact on the security officers. On the other hand, 21.82 % (12 out of 55) of the participants disagree, while 16.36 % (9 out of 55) of the participants were unsure or did not comment.

5.11 PSS PIE CHART SUMMARY

This Pie Chart Summary indicates the percentage of participants (55) that agree with the reasons for why the Private Security Supervisors (PSS) cannot prevent cable theft at Eskom (see section 5.10.1 – 5.10.6)

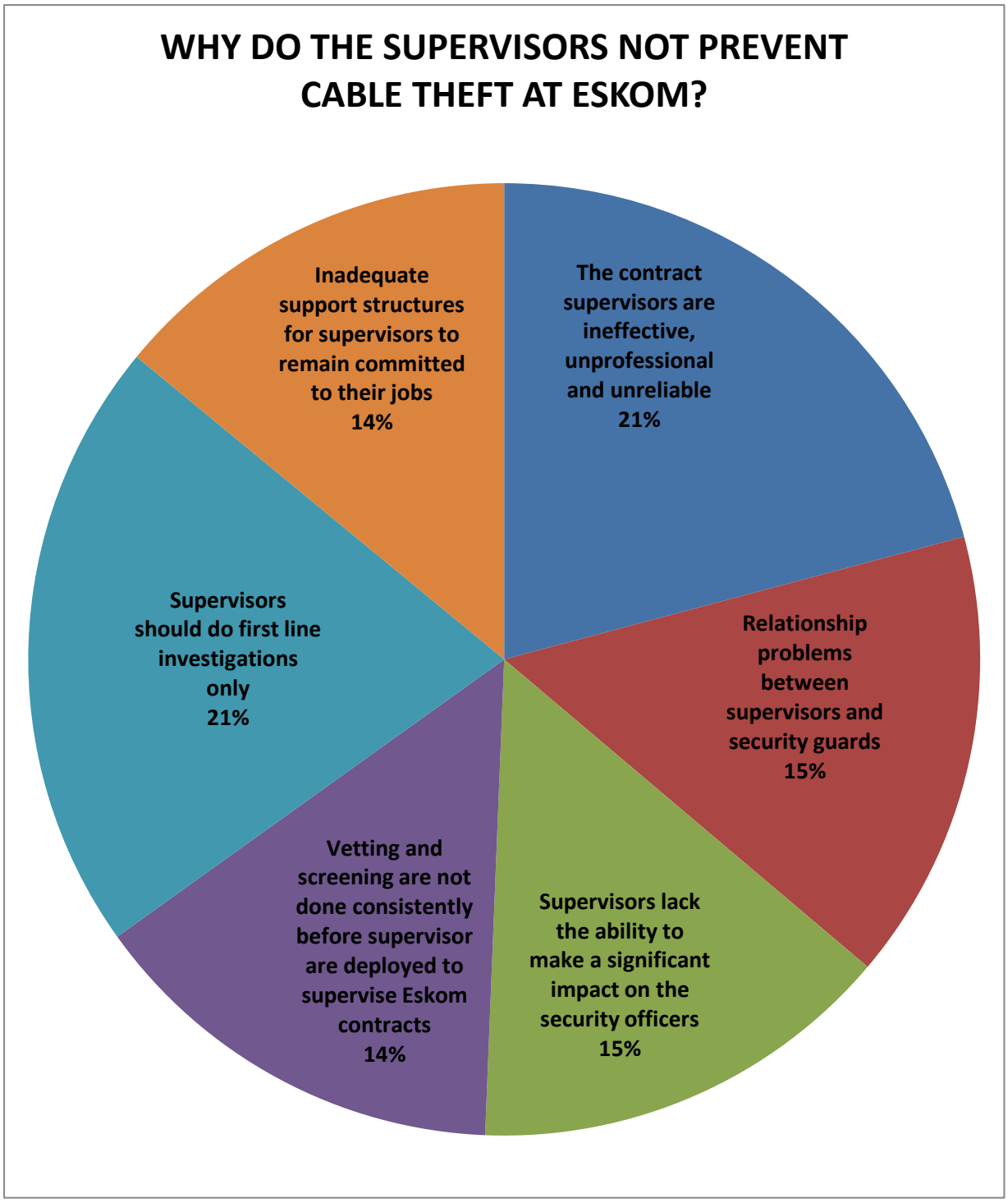


Figure 5.4: Pie Chart indicating the percentage of participants (55) that agree with the reasons for why the supervisors cannot prevent cable theft at Eskom

5.11.1 Explanation of the pie chart

In summary, the evidence of why the private security seemingly cannot prevent cable theft at Eskom (see section 5.11), which is displayed on the pie chart shown in Figure 5.4 above,

indicates (from highest to lowest) that supervisors are ineffective, unprofessional and unreliable (21 %). Many of the participants also felt that supervisors should do first line investigations only (21 %) and that they lack the ability to make a significant impact on the security officers (15 %). There is a serious relationship problem between supervisors and security guards (15 %). There are insufficient support structures in place by their companies for them (the supervisors) to feel safe and committed to their jobs (14 %). The final issue raised was the fact that vetting is not done consistently before supervisors are deployed to supervise Eskom contracts (14 %).

5.12 WHY DO THE PRIVATE SECURITY MANAGERS (PSM) AND COMPANY DIRECTORS/OWNERS NOT PREVENT CABLE THEFT AT ESKOM?

The researcher has identified possible reasons (see section 5.12.1 – 5.12.6) why the managers and company directors/owners of security companies cannot prevent cable theft at Eskom. Certain issues were identified in questions, which led to the formulation of security-related statements which were put to fifty-five (55) participants consisting of Eskom employees, contract security supervisors and contract security managers and directors/owners (see Tables 5-16 to 5-21 below).

These statements were put to participants to investigate the issues described in the following subsections.

5.12.1 The contractual commitment by security managers and company directors/owners of security companies is not shown consistently throughout the contract period

In order to comply with the contractual mandate to provide a reliable and competent security service to Eskom, private security managers and company owners have a great responsibility to uphold the contract requirements and obligations throughout the contract period. When it comes to compliance and consistency, and to fully adhering to the requirements of the security contract for the duration of the contract period, the point of departure or view point of Jenkins (2015) and Meek (2014) is that commitment is only shown at the start of the contract and at the end when the contract is renewed or at the re-tender stage. They say that it is at this stage where the company owners and managers will promise everything to win favour for considering them for the contract or renewal of their contract.

Eskom's security contracts are well-drafted legal documents which are signed by the appointed security service provider after it has been successful with its tender bid. What is not made clear, however, and which should be a challenge for Eskom security managers, is to make it compulsory for the security companies to provide a security manager exclusively to manage the Eskom security contract for the duration of the contract period.

The reality of increased profit margins and budget cuts affecting contractual compliance in the private security industry is well-known and as a result, many of the security companies do not make a security manager available to exclusively manage one client, but rather a security manager has to manage many clients. As a result of this reality, most of the security managers are overworked, dealing with various different contracts that they do not always understand, including the specific nature and requirements of Eskom. This is why the researcher believes that this is one of the reasons why they cannot prevent cable theft at Eskom. Jenkins (2015) believes that the managers show low to no commitment to Eskom contracts because they have other contracts to manage, apart from just Eskom (see recommendations in section 8.7).

Table 5-15: The contractual commitment by security managers and company directors/owners is not shown consistently throughout the contract period

Theme	Agree	Disagree	Unsure
The contractual commitment by security managers and company directors/owners is not shown consistently throughout the contract period	39 (70.91 %)	10 (18.18 %)	6 (10.91 %)

As shown in Table 5-16 above, 70.91 % (39 out of 55) of participants agree that security managers and company directors/owners lack commitment and do not consistently play their part in the contractual obligations. Some 18.18 % (10 out of 55) of the participants disagree, while 10.91 (6 out of 55) of the participants were unsure or did not comment.

5.12.2 All security managers and company owners/directors should be vetted before contracting to Eskom

It is common sense to note that security managers and company owners/directors occupy positions of trust. They will have access to Eskom's confidential information and will get to

know and understand Eskom's operations in great detail. This responsibility is gained partly in compliance with the security contract, but it will also be necessary for them to attend Eskom's strategic meetings for new construction and developments where private security will be required, and they will further attend to incidents where security has been breached. To enable them to conduct thorough investigations and make informed decisions, they would need access to Eskom's confidential information.

The vetting required for both a security manager and a company owner/director represents two sides of the same coin. Eskom must require that both these positions, which are entrusted with Eskom's confidential information, must be vetted before the contract commences.

Table 5-16: All security managers and company owners/directors should be vetted before contracting to Eskom

Theme	Agree	Disagree	Unsure
All security managers and company owners/directors should be vetted before contracting to Eskom	29 (52.73 %)	9 (16.36 %)	17 (30.91 %)

As indicated in Table 5-17 above, 52.73 % (29 out of 55) of participants agree that managers and company owners and directors should be vetted before contracting to Eskom. On the other hand, 16.36 % (9 out of 55) of the participants disagree, while 30.91 (17 out of 55) of the participants were unsure or did not comment.

5.12.3 Security managers are not adequately supported by company owners/directors

The support referred to here by the researcher is leadership support in terms of providing the security manager with the financial resources required to improve the security standards for the client and the company.

The researcher mentioned in section 5.12.1 above that the reality of increased profit margins and budget cuts affecting contractual compliance in the private security industry is well known and as a result, many of the security company owners focus on profits and allocate minimal budgets to the managers, and yet expect them to be effective in their positions. Baccus (2015) feels that managers are only as good as the support they receive from company directors.

Table 5-17: Security managers are not well supported by company owners/directors

Theme	Agree	Disagree	Unsure
Security managers are not well supported by company owners/directors	36 (65.45 %)	10 (18.18 %)	9 (16.36 %)

As reflected in Table 5-18 above, 65.45 % (36 out of 55) of participants agree that security managers are not well supported by company owners/directors. Participant 27 said that *"Managers are told by the directors to save costs and do more with less"*. However, 18.18 % (10 out of 55) of the participants disagree, with participant 26 saying that *"Managers are well supported but they lack experience to know what is required to run the operation effectively".* A similar proportion, 16.36 % (9 out of 55) of the participants, were unsure or did not comment.

5.12.4 Security managers fail to provide clear, honest and definitive leadership roles in their positions

In general, security managers are required to provide meaningful and sustainable programmes to prevent cable theft, which must lead to a decrease in cable thefts at Eskom and should not further exacerbate the problem. The researcher agrees with this statement because he has experienced it on different occasions, noting that the offerings of certain crime prevention programmes were not credible or sustainable because there was a shortage of resources experienced when these programmes were supposed to be implemented.

When there are limited resources allocated to crime prevention strategies, for example, where a security manager makes a commitment to provide a patrol vehicle in a high-crime area, but does not do so because of the lack of resources, of which he or she is fully aware, the argument can be made that in most cases this does compromise his or her integrity and honesty towards the client, as well as compromising the security of the affected area. Although this reality is definitely challenging and irritating, the making of false promises by certain security managers cannot be allowed to persist. Security managers must provide and implement clear, definitive and honest practices, at all times.

Table 5-18: Security managers fail to provide clear, honest and definitive leadership roles in their positions

Theme	Agree	Disagree	Unsure
Security managers fail to provide clear, honest and definitive leadership roles in their positions	47 (85.45 %)	6 (10.91 %)	2 (3.64 %)

As shown in Table 5-19 above, 85.45 % (47 out of 55) of participants agree that security managers fail to provide clear, honest and definitive leadership roles in their positions. Some of the participants that agreed are currently working as private security managers. Only 10.91 % (6 out of 55) of the participants disagree, while 3.64 % (2 out of 55) of the participants were unsure or did not comment.

5.12.5 Security managers are not innovative enough

It is clear to understand that doing things differently will bring about different results. The fact that Eskom continues to experience cable theft from its facilities, and at most times these are repeated incidents, is a real cause for concern. Applied within the context of this argument, security managers need to do things differently, for example, introducing new technology to manage the security officers, and using security aids, like CCTV, alarms, outdoor beams with real time monitoring and response planning, to prevent cable theft from Eskom.

In short, what this means in practice is that security companies are directly responsible for all criminal activities in all their contracted areas. All crime prevention programmes to combat cable theft must include innovation from security managers to do things differently and introduce better technology and standards.

Table 5-19: Security managers are not innovative enough

Security managers are not innovative enough	29 (52.73 %)	20 (36.36 %)	6 (10.91 %)

As indicated in Table 5-20 above, 52.73 % (29 out of 55) of participants are in agreement that security managers are not innovative enough to do things different. Some of the participants that agreed are currently working as private security managers. However, 36.36 % (20 out of

55) of the participants disagree, while 10.91 % (6 out of 55) of the participants were unsure or did not comment.

5.12.6 Security managers wear many hats during the contractual period

Everybody concerned has a role to play during the contract period between Eskom and the private security companies. It is a reality in the private security arena that in desperate times, the security manager "wears many hats". This means that often during the contract period, the security manager becomes the investigator, labour relations officer, supervisor, control room operator, director and sometimes a (relief) security officer. This means that he or she must do too many different things at the same time (must be multi-skilled).

As mentioned by the researcher in Section 5.12.1 above, the reality of increased profit margins and budget cuts affecting contractual compliance in the private security industry is well known. Sometimes, poor planning and controls means that the security manager must step in and take responsibility for the company's lack of planning. There is no universal blueprint for the design of exactly what the security manager must do, but one thing that is certain is that he must be consistent and committed in the portfolio of a security manager. In short, he or she must be a high performer.

Table 5-20: Security managers wear many hats during the contractual period

Theme	Agree	Disagree	Unsure
Security managers wear many hats during the contractual period	49 (89.09 %)	4 (7.27 %)	2 (3.64 %)

As shown in Table 5-21 above, 89.09 % (49 out of 55) of participants agree that security managers wear many hats during the contractual period. Only 7.27 % (4 out of 55) of the participants disagree, and 3.64 % (2 out of 55) of the participants were unsure or did not comment.

5.13 PSM AND COMPANY DIRECTORS/OWNERS PIE CHART SUMMARY

The following pie chart Summary indicates the percentage of participants (55) that agree with the reasons why the Private Security Managers (PSM) and security company directors/owners do not prevent cable theft at Eskom (see section 5.8.1 – 5.8.7)

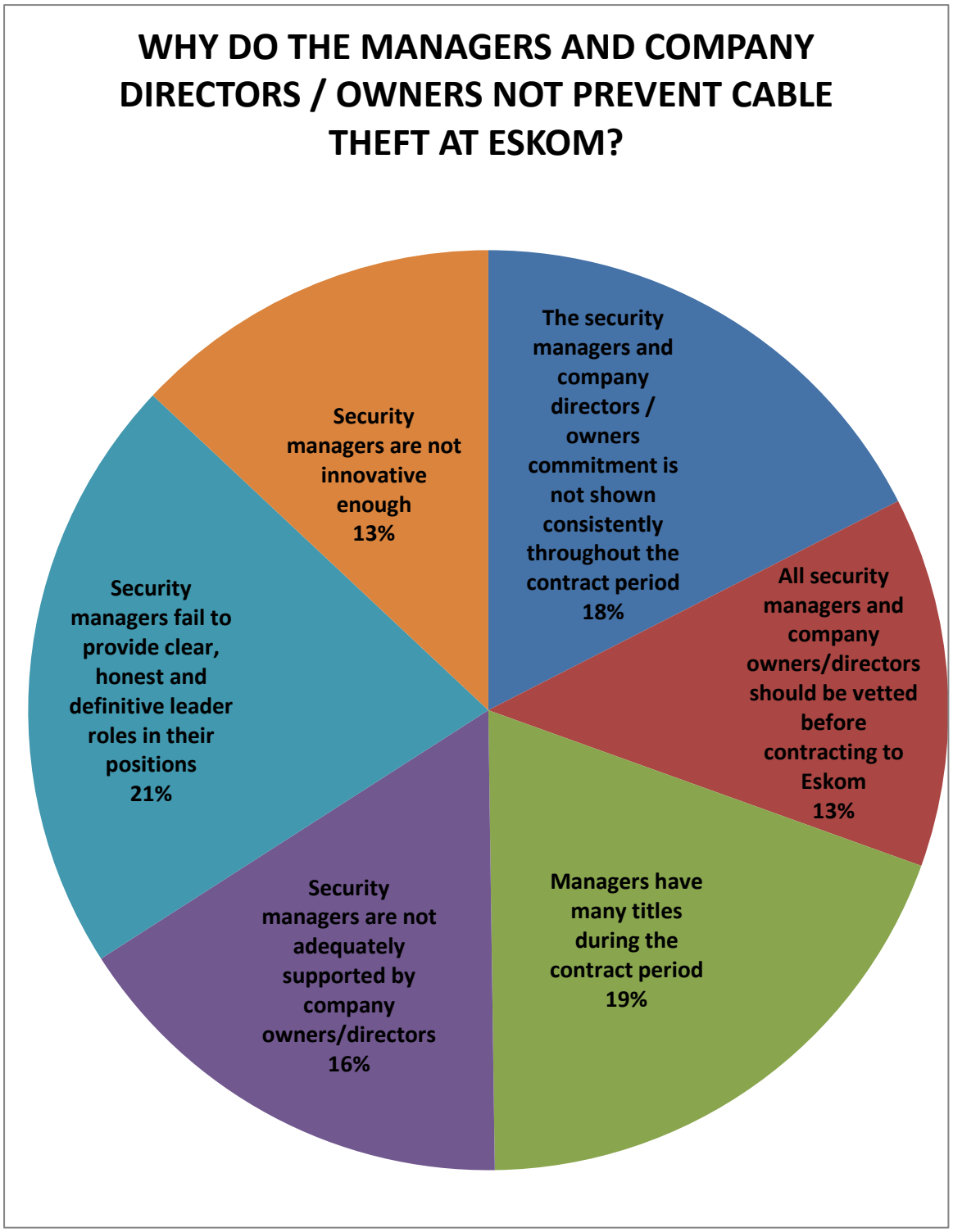


Figure 5.5: Pie Chart indicating the percentage of participants (55) that the reasons why the Private Security Managers (PSM) and security company directors/owners do not prevent cable theft at Eskom

5.13.1 Explanation of the pie chart

In summary, the evidence of why the managers and company directors/owners seemingly cannot prevent cable theft at Eskom (see section 5.13) displayed on the pie chart (from highest to lowest) is that security managers fail to provide clear, honest and definitive leadership roles in their positions (21 %). Many of the participants also agree that managers wear many hats during the contract period (19 %), followed by a lack of commitment shown by the managers and company owners/directors for the duration of the contract (18 %).

There also seems to be a problem in terms of the support shown to the security managers by company owners/directors (16 %). There seems to be a lack of innovation by security managers in developing new ideas and plans to prevent cable theft (13 %). Lastly, there is a need for vetting security managers and company owners/directors to be done before the contract commences, which is currently lacking (13 %).

5.14 WHAT ARE THE REAL REASONS WHY SECURITY CONTRACTED TO ESKOM CANNOT PREVENT CABLE THEFT?

The researcher has identified possible reasons (see sections 5.14.1–5.14.6) underlying the real problems as to why security businesses contracted to Eskom cannot prevent cable theft. Certain issues were identified in questions, which led to the formulation of security-related statements which were put to fifty-five (55) participants, comprising Eskom employees, contract security supervisors and contract security managers and directors/owners (see Tables 5-22 to 5-27 below).

The statements were put to participants to investigate the issues described in the following subsections.

5.14.1 The high turnover of security guards at Eskom facilities

It is a known fact that the security industry experiences a high turnover of security guards. This high turnover rate is the result of many factors, such as no work satisfaction, late salary payments, and unjustified penalties. This particular fact has made the researcher aware that there are security companies who do not fully comprehend the need to keep security officers committed in their jobs to prevent this high turnover rate.

According to Jenkins (2014), it is shocking to think that security companies, which should be driving employee satisfaction programmes to keep security officers content and motivated, are not aware of the importance of preventing the high turnover rate that undermines the cornerstone of any security contract. Du Preez (1991:157) makes a valid argument by saying that lowering the turnover rate in the security industry could aid in having better trained and efficient security officers.

The analysis of this problem of the high turnover rate indicates that the private security industry faces an uphill battle when it comes to reducing security guard turnover. This reality means that the costs related to turnover are extremely important and must be considered by security companies. Security companies must look at the financial costs related to the turnover rate, such as the costs involved in interviewing, training, uniforms, equipment, and providing boarding to new employees. Rather than focusing on this commonly accepted costs problem, security companies should focus on providing incentives to their guards to stay in their employment in order to be successful in achieving a lower turnover rate.

Table 5-21: The high turnover rate of security guards at Eskom facilities is a problem

Theme	Agree	Disagree	Unsure
The high turnover rate of security guards at Eskom facilities is a problem	43 (78.18 %)	8 (14.55 %)	4 (7.27 %)

As indicated in Table 5-22 above, 78.18 % (43 out of 55) of participants agree that the high turnover rate of security guards at Eskom facilities is a problem. Participant 4 said that *"The high turnover rate is a problem because the guards are not committed to staying on the job for long periods of time"*, while participant 8 mentioned that *"Guards are always in the hunt for more money"*. Only 14.55 % (8 out of 55) of the participants disagree, with participant 35 saying that *"If the company treat us right and look after us, we will not leave".* Finally, 7.27 % (4 out of 55) of the participants were unsure or did not comment.

5.14.2 Eskom lacks a standard training entry requirement for contracted private security employees to work at its facilities

Eskom relies on security companies to offer training programmes that promote the prevention of cable theft and to prepare their security officers to act when criminal activity takes place,

and hopefully prevent cable theft. Put differently, the security guards are graded according to their qualifications, experience, and training. They are trained to security industry standards.

Berg (2007) mentions that the guards are the frontline of contact with the public and, if not trained properly, may misuse their 'powers' and possibly violate the human rights of members of the public. Individual security officers may be answerable to their employers in terms, for instance, of removing 'undesirables' from outside a client's premises, but it is their responsibility to ensure that their actions do not violate anyone's rights. If they do not receive proper training and education in terms of the law and the rights of the citizen, they may be more likely to abuse those rights (Berg, 2007).

The reality is that, if Eskom wishes to improve the standard of security provided to its facilities, the security personnel would need to undergo training in security programmes designed for Eskom's standards, and then they would be able to perform according to Eskom's security standards. The participants continue to question the effectiveness of the security training that security guards receive at PSIRA-accredited training institutions, despite their success in producing thousands of security guards.

In addressing this approach, and in order to achieve a higher standard of security services, the researcher has designed a standard training entry requirement for private security employees to work at Eskom facilities (see section 7.9 below) as part of the recommendations for this study.

Table 5-22: Eskom lacks a standard training entry requirement for private security employees to work at its facilities

Theme	Agree	Disagree	Unsure
Eskom lacks a standard training entry requirement for private security employees to work at its facilities	49 (89.09 %)	2 (3.64 %)	4 (7.27 %)

As indicated in Table 5-23 above, 89.09 % (43 out of 55) of participants agree that an Eskom standard training entry for private security employees is required for them to work at an Eskom facility. A marginally small number 3.64 % (2 out of 55) disagreed, while 7.27 % (4 out of 55) were unsure or did not comment.

5.14.3 Eskom's private security contractors should use security patrol dogs at all its high crime facilities

According to the Private Security Industry Regulation Act, 2001 (Act No 56 of 2001), the use of security patrol dogs is permitted, although, in terms of Board Notice 15 of 1999, read with section 44(2) (c) of the Private Security Industry Regulation Act, 2001 (Act No 56 of 2001), it is provided that "*Security companies who uses dogs must, depending on the security service rendered with the particular dog, successfully complete the relevant dog handler courses as contemplated in the board notice from an accredited PSIRA training instructor and training provider*". The dogs must also be trained for the particular security service they are used for.

For example, in the case of substance detection, the dog must be able to positively identify and indicate a specific substance or specific group of substances, as required, and these training levels must be specified on a certificate in respect of the particular dog.

The Private Security Industry Regulator says that failure to comply with this notice (Board Notice 15 of 1999) will constitute improper conduct in terms of the Code of Conduct for Security Service Providers, 2003, as well as a criminal offence. The regulator further advises that security companies who use dogs must also apply for a licence at the relevant magistrate's court in terms of the Performing Animals Protection Act, 1935 (Act No 24 of 1935).

Table 5-23: Eskom's private security contractors should use security patrol dogs at all its high crime facilities

Theme	Agree	Disagree	Unsure
Eskom's private security contractors should use security patrol dogs at all its high crime facilities	55 (100 %)	0	0

As shown in Table 5-24 above, there is overwhelming support for the use of security patrol dogs, with 100 % (55 out of 55) of participants agreeing that Eskom's private security contractors should use security patrol dogs at all its high crime facilities.

5.14.4 Eskom's private security contractors must use patrol vehicles at all its high crime facilities

The Private Security Industry Regulation Act, 2001 (Act No 56 of 2001), allows for the use of vehicle patrols, but states that the security officers who make up the patrol teams must be trained for this work and compliance must be in line with the PSIRA Act.

The reality is that a vehicle patrol offers high visibility and mobility, and normally covers areas that are too great to be covered on foot. Without the intervention of patrol vehicles being factored into an integrated security plan for a high crime area, there is no doubt that cable theft crimes will be more challenging, when combatted using only security foot patrols.

Meek (2014) says that vehicle patrols are very effective because of the high visibility factor and of the fact that larger areas can be covered in a relatively shorter period of time. Krause (2014) and Meek (2014) recommend that patrol vehicles be fitted with tracking systems to ensure that the vehicles are patrolling their routes.

Table 5-24: Eskom's private security contractors must use patrol vehicles at all its high crime facilities

Theme	Agree	Disagree	Unsure
Eskom's private security contractors must use patrol vehicles at all its high crime facilities	36 (65.45 %)	10 (18.18 %)	9 (16.36 %)

As shown in Table 5-25 above, 65.45 % (36 out of 55) of participants agree that Eskom must use patrol vehicles at all its high crime facilities, while 18.18 % (10 out of 55) participants disagree, with participant 16 saying that *"This will only mean more money in the pockets of the security company because like the security guards, the vehicle patrols will not be managed effectively"*. Finally, 16.36 % (9 out of 55) participants were unsure or did not comment.

5.14.5 Eskom's private security managers must manage in line with the security contract agreement

What this means in reality is that an Eskom's private security manager's role is very challenging and demanding in making sure that cable theft is kept under control within

Eskom. These challenges are also accompanied by stress and pressure from the additional responsibilities in terms of making sure that the security company is performing in terms of the contract agreement.

It is the task of Eskom's internal security managers to see that Eskom's private security managers that have been contracted to prevent cable theft are doing their work properly, and if they do not adhere to that, they must be held accountable, in terms of the contractual agreement.

Table 5-25: Eskom's private security managers must manage in line with the security contract agreement

Theme	Agree	Disagree	Unsure
Eskom's private security managers must manage in line with the security contract agreement	39 (70.91 %)	10 (18.18 %)	6 (10.91 %)

As indicated in Table 5-26 above, 70.91 % (39 out of 55) of participants agree that Eskom's private security managers must manage in line with the security contract agreement, while 18.18 % (10 out of 55) participants disagree, and 10.91 % (6 out of 55) participants were unsure or did not comment.

5.14.6 Improper utilization of security manpower

The researcher has observed that there is an improper balance in security manpower at Eskom facilities. Some of the facilities have inadequate and insufficient manpower resources, while other sites have excessive manpower resources. There is no doubt that Eskom facilities with a lower security manpower numbers are more likely to experience more thefts than would a facility that has the appropriate number that is in line with the relevant risk analysis findings.

Some of the participants were probed further to understand why this may be a problem, and participant 52 stated:

"... This problem is a result of Eskom security people not interested in doing proper risk assessments to balance the appropriate number of guards needed at a facility ...."

Table 5-26: Improper utilisation of security manpower

Theme	Agree	Disagree	Unsure
Improper utilisation of security manpower	49 (89.09 %)	2 (3.64 %)	4 (7.27 %)

As shown in Table 5-27 above, 89.09 % (49 out of 55) of participants agree that there is an improper utilisation of security manpower at Eskom facilities, with most participants saying the numbers were insufficient. Only 3.64 % (2 out of 55) participants disagree, while 7.27 % (4 out of 55) participants were unsure or did not comment.

The researcher wants to point out that it is the task of Eskom's internal security management to tell the private security managers who are contracted to prevent copper theft, where and how many personnel, vehicles and dogs they need to deploy, where and when. This remains a real challenge at present because the utilisation of manpower in the wrong place at the wrong time could make Eskom sites vulnerable to possible cable thefts.

5.15 REAL REASONS PIE CHART SUMMARY

This pie chart indicates the percentage of participants (55) that agree with the real reasons why the security personnel contracted out to Eskom cannot prevent cable theft (see section 5.14.1 – 5.14.6).

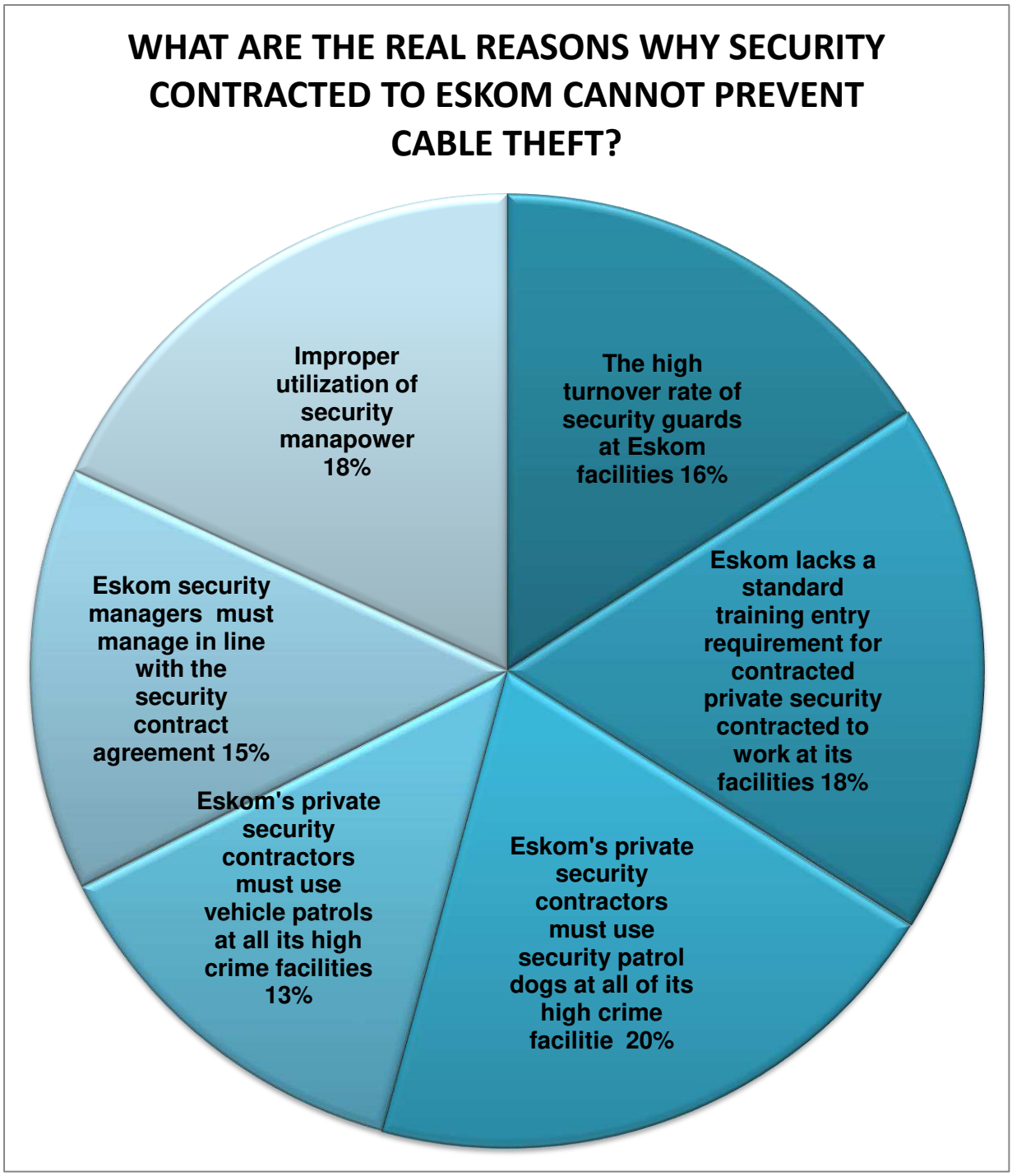


Figure 5.6: Pie Chart indicating the percentage of participants (55) that agree with the real problems why private security contracted to Eskom cannot prevent cable theft

5.15.1 Explanation of the pie graph

In summary, the evidence of the real problems why private security contracted to Eskom seemingly cannot prevent cable theft at Eskom (see section 5.15), displayed on the pie chart

(from highest to lowest), starts with the lack of security patrol dogs at its high risk sites (20 %), followed by the lack of an Eskom standard training entry requirement for private security employees deployed to an Eskom facility (18 %). There is an improper utilisation of security manpower at Eskom facilities (18 %). Next, there is a high turnover rate of security officers (16 %), and finally, there is a problem of Eskom private security managers managing security contracts without considering the real contents of the contractual agreements.

The researcher comes to the conclusion that Eskom's internal security managers are not doing their job and that this filters down through to the ground level.

5.16 OTHER GENERAL REMARKS MADE BY THE PARTICIPANTS FOR REDUCING CABLE THEFT

The reality is that cable theft cannot be completely eliminated from Eskom, or from other companies operating in South Africa. Cable theft serves a lucrative market and is very profitable to those willing to break the law and take the risk of getting caught in stealing it (Cf. Chapters One & Three). The researcher's experience gained over the years, especially during the time of the data gathering, together with the researcher's involvement in combatting cable theft, provides a basis for stating that it is reasonable to believe that cable theft crimes can be controlled and reduced at Eskom.

Eskom must improve its capabilities when appointing security companies that are to provide it with a sustainable, realistic, measurable and effective crime control strategy for protecting the cable at its facilities. The researcher, during his field research trips to Eskom facilities and while speaking to many of the security company employees, gained a fuller appreciation of the importance of this seemingly simple matter of appointing good security companies that understand the importance of employee satisfaction and crime reducing programmes and strategies.

The evaluations which are conducted on security companies before they are appointed, in addition to other legal requirements, should contribute to the procurement process by enabling the Eskom security panel to make more-informed decisions when appointing credible and compliant security companies.

The researcher believes that it is important to focus on some other remarks made by the participants on reducing cable theft (see sections 5.16.1–5.16.5 below).

The security-related statements were made by the 55 participants who had participated in this study.

5.16.1 Security companies must deploy armed response to all facilities and improve its response times to panic alarms

The purpose for Eskom including a compulsory armed response service in its security contracts is to make sure that the security officers are not left vulnerable in cases of emergencies and also to introduce them to a safety rights culture that is based on Eskom's safety standard practices, which ensure that human life is protected at all times.

What this means in practice is that all Eskom facilities which are protected by security guards must reflect a reality of having a reliable armed response service. However, this is not the case when it comes to all the facilities, and more especially the remote Eskom facilities. The researcher found during information gathering for this study that many discussions were being conducted by security managers, from both Eskom and private sector, concerning the armed response service and the importance of ensuring good response times. However, the researcher had discovered during site visits that many of the discussions were simply "meaningless discussions". Talking about something is fine, but what matters most is what is happening at the Eskom facilities and what security companies are doing to ensure the safety of its people.

The contractual obligations of the security companies are the same for all areas and sites, which simply implies that a reliable and efficient armed response service must be provided to all Eskom facilities, irrespective of their locations. If a security company is exempted from providing an armed response service to a remote facility because of its location, then security officers ought not to be deployed to that facility. Eskom's safety slogan is to the effect that no persons will operate in high risk areas without proper safety mechanisms, irrespective of the operating urgency or the importance of that facility.

Table 5-27: Security companies must deploy armed response to all facilities and improve its response times to panic alarms

Theme	Agree	Disagree	Unsure
Security companies must deploy armed response to all facilities and improve its	55 (100 %)	0	0

response times to panic alarms			

As shown in Table 5-28 above, there was overwhelming support for security companies to deploy armed response resources to all facilities and improve their response times to panic alarms. All, 100 % (55 out of 55), of participants agree with this theme.

5.16.2 Private security must reduce the opportunities for criminals to commit crime at Eskom facilities

There is no doubt that criminals have no difficulty in committing crimes at Eskom facilities. The ease with which they enter the facilities and commit crimes simply means that private security is not reducing the opportunities for criminals to enter and steal Eskom's cables.

Levy *et al*. (2014) state that there is a range of crime prevention strategies that can be used to reduce the opportunities for crime. These include increasing formal surveillance using electronic alarms, CCTV and security patrols. They further mention that increasing natural surveillance by removing obstacles to lines of sight, increasing controls over access and exit points, and concealing or removing targets, are other methods that can be used to reduce the opportunities for crime.

Sennewald (2011:29) feels that there is an increased need for the private security sector to educate employees on the necessity and objectives of security. There is no doubt in the mind of this researcher that one of the biggest challenges in the future for security companies is that, if they want to be more effective and retain their existing clients, they will have to design proactive crime prevention measures in order to effectively measure the performance of their security officers. So far, this researcher has not witnessed any attempt by security companies to prevent crime in any manner prescribed by Levy *et al*. (2014), at least, out of their own free will and at their own cost.

Table 5-28: Private security must reduce the opportunities for criminals to commit crime at Eskom facilities

Theme	Agree	Disagree	Unsure
Private security must reduce the opportunities for criminals to commit crime at Eskom	49 (89.09 %)	0	6 (10.91 %)

facilities			

As shown in Table 5-29 above, there was overwhelming support for private security to reduce the opportunities for criminals to commit crime at Eskom facilities, 89.09 (49 out of 55) participants being in favour of this measure, while 10.91 % (6 out of 55) were unsure or did not comment.

5.16.3 Private security companies must target the underlying causes of crime against Eskom

The high crime levels committed against Eskom pose a serious problem for its operating efficiency. Crime casts fear into the hearts of some security officers and this prevents them from working effectively, because they are fearful. Many private security guards have been killed while protecting Eskom facilities. Although much can be said why they were killed, this necessitates that security companies must transform and reorganise themselves to implement real crime prevention strategies to address copper theft. The researcher believes that the success of private companies will depend largely on the strategies they apply to target the causes of crime from Eskom. The use of intelligence and intelligent security systems will help private security companies evolve well into the next century.

Table 5-29: Private security companies must target the underlying causes of crime from Eskom

Theme	Agree	Disagree	Unsure
Private security companies must target the underlying causes of crime from Eskom	55 (100 %)	0	0

As reflected in Table 5-30 above, there was overwhelming support for private security companies to target the underlying causes of crime from Eskom. All 55 (100 %) of the participants were in favour of this theme.

5.16.4 Eskom management must improve its housekeeping procedures and lock up unused material

The main reason why Eskom must lock away unused material is to keep criminals from the temptation of stealing it. By not keeping the materials locked away, Eskom will run the risk

of delays on projects sites because replacement material is not easily available or accessible. Steenkamp (2002) says that secondary crime prevention measures strive to minimise the likelihood that specific criminal acts will be initiated at a particular time and in a particular place. Secondary crime prevention measures include all those of reducing opportunities for crime, which have been labelled opportunity-reduction strategies.

Creating physical barriers to would-be offenders increases the effort and risk involved in the commission of a crime, and this deters the would-be offender from committing crime against a specific target (Lab, 1997; Steenkamp, 2002).

The researcher found that although Eskom's cable is in most cases secured on site by outer perimeter fencing, the cables are still exposed to people working inside the premises (Cf. Annexures A14/A15/A16/A17/A18). He believes that if Eskom were to create lockable areas in which to secure its excess or unused cable, Eskom would further deter cable theft from its facilities.

Table 5-30: Eskom management must improve its housekeeping procedures and lock up unused material

Theme	Agree	Disagree	Unsure
Eskom management must improve its housekeeping procedures and lock up unused material	36 (65.45 %)	12 (21.82 %)	7 (12.73 %)

As indicated in Table 5-31 above, 65.45 % (36 out of 55) of participants agree that Eskom management must improve its housekeeping procedures and lock up unused material. Participant 21 said that *"Although the site has a fence, it is not adequate to protect the cables because it is high value and in demand"*[sic]. On the other hand, 21.82 % (12 out of 55) of the participants disagree, with participant 4 questioning *"Why do we (Eskom) still have to lock up cables when the security must do their job and protect the site?"* Lastly, 12.73 (7 out of 55) of the participants were unsure or did not comment.

5.16.5 Eskom security management must create early warning crime prevention programmes

The researcher believes that any crime prevention programme initiated and implemented early at high crime facilities would provide an immediate impact in deterring criminals from being willing to continue to target those facilities. What should be very clear in any mission statement on crime prevention problems is that emphasis should be placed in the programme on adding value by minimising further criminal activity. In any early crime prevention intervention programme, contingency budgets for security resources must be made available to render the programme successful. Appropriate training for security officers and people involved in the programme is also vital in order to raise the standards of crime prevention efforts of security.

Table 5-31: Eskom security management must create early crime prevention programmes

Theme	Agree	Disagree	Unsure
Eskom security management must create early warning crime prevention programmes	45 (85.45 %)	7 (12.73 %)	3 (5.45 %)

As shown in Table 5-32 above, 85.45 % (45 out of 55) of the participants believe that Eskom security management must create early warning crime prevention programmes. Only 12.73 % (7 out of 55) of the participants disagree, while 5.45 % (7 out of 55) of the participants were unsure or did not comment.

5.17 OTHER GENERAL REMARKS PIE CHART SUMMARIES

This pie chart indicates the other general remarks made by participants (55) on reducing cable theft (see section 5.16.1–5.16.5).

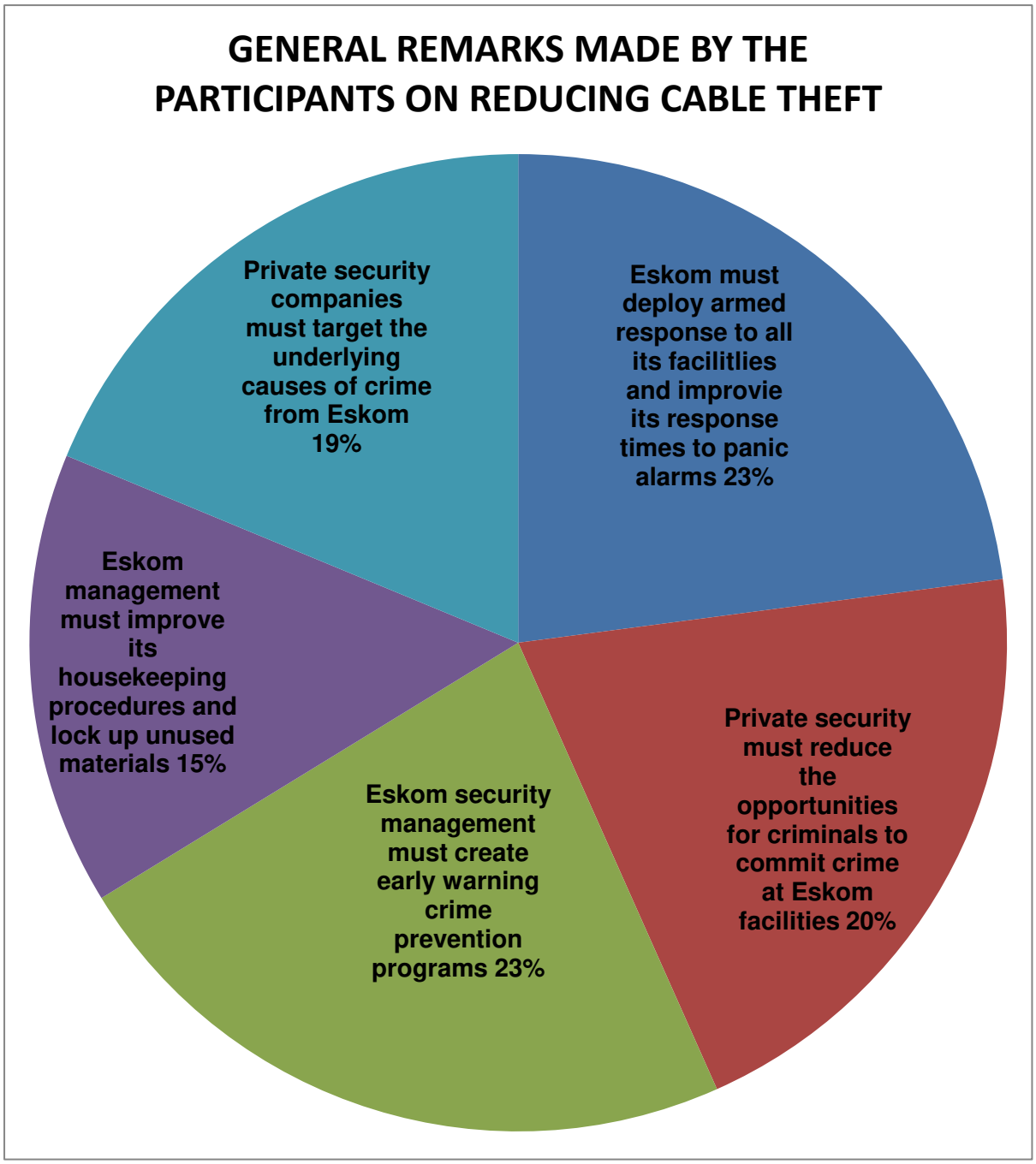


Figure 5.7: Pie Chart indicating the general remarks made by participants (55) on reducing cable theft

5.17.1 Explanation of the pie chart

In summary, the participants made various general remarks on reducing cable theft (see sections 5.16.1–5.16.6) which are displayed on the pie chart (from highest to lowest), as follows. Firstly, Eskom must deploy armed response services to all its facilities and improve the response time to panic alarms (23 %). Eskom must create early warning crime prevention

programmes (23 %). This is followed by the need for private security to reduce the opportunities for criminals to commit crime against Eskom (20 %). Finally, private security companies must target the underlying causes of crime (19 %) and Eskom must improve its housekeeping procedures and lock up unused materials (15 %).

5.18 SUMMARY

Chapter Five is, in a certain sense, one of the two most important chapters of this study. It contains an introduction (see section 5.1), after which attention was paid, inter alia, to the following points: the term 'private security' in Eskom (see section 5.2); brief remarks about the private security industry in South Africa (see section 5.3); an organogram of Eskom's regional security structures for Transmission (TX) and Distribution (DX) (see section 5.4); and an organogram of Eskom's security structures for Generation (GX) (see section 5.5).

The basic requirement for security companies that wish to render a service to Eskom was discussed (see section 5.7), as well as questions why the private security guards cannot prevent cable theft at Eskom (see section 5.8), why the supervisors cannot prevent cable theft at Eskom (see section 5.10) and why the managers and company directors/owners cannot prevent cable theft at Eskom (see section 5.12). Also discussed were the real problems why security contracted out to Eskom cannot prevent cable theft (see section 5.14), general remarks were made by the participants on reducing cable theft (see section 5.16) and lastly, this chapter concluded with a summary (see section 5.18).

In the next chapter, the researcher will discuss what action steps must be taken by the Eskom internal security management team and those responsible for the capturing of all relevant information related to cable theft.

CHAPTER SIX

ESKOM'S INTERNAL SECURITY MANAGEMENT TEAM AND THOSE RESPONSIBLE FOR THE CAPTURING OF ALL RELEVANT INFORMATION RELATED TO CABLE THEFT

6.1 INTRODUCTION

While Chapter Five focused mainly on private security and cable theft at Eskom, this chapter looks at the Eskom internal security management team and those responsible for the capturing of all relevant information related to cable theft. This is in line with research aim 1.8.6, set out in Chapter One (under section 1.8 "RESEARCH AIMS", above).

This chapter examines one question and sets out a discussion on the Eskom CURA system and on the Eskom Network Equipment Crime Committee (ENECC) report:

- Why can the internal security management team not stop cable theft at Eskom?
- The Eskom CURA system and cable theft is discussed, and;
- A study of the ENECC report is discussed to determine whether it prevents or worsens cable theft in Eskom.

In order to place the remarks that will be made in this chapter in the right security contexts, brief remarks will be made at the start of this chapter to put things in proper perspective (Cf. 6.2 and 6.3 below).

6.2 GROUP SECURITY'S ROLE WITHIN ESKOM'S SUSTAINABILITY DIVISION

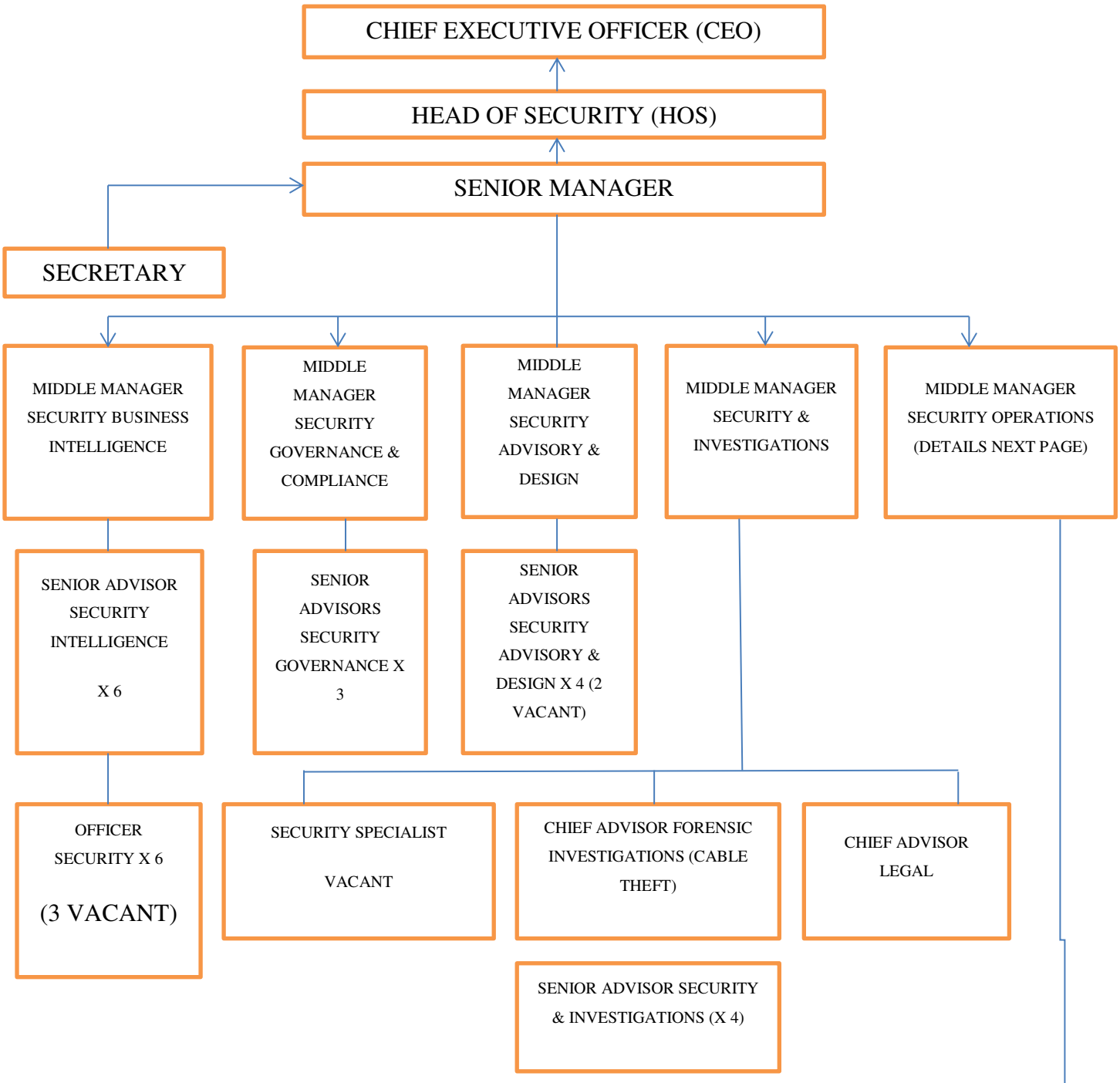
Security in Eskom plays the most important role in supporting Eskom's strategic imperatives, which are to provide Eskom, its employees, customers and suppliers a safe and secure environment and to support business sustainability. This is achieved by delivering an effective, economic, responsive and resilient integrated security network to Eskom (http://sustainability.eskom.co.za/sites/gs/Pages/Default.aspx).

The mandate of Eskom Group Security is to effectively shape security management; to provide strategic services to treat security risks, which impact on assets, information,

interests, people, systems and processes; to maintain security at agreed risk levels; and to provide assurance that security maintain high standards in Eskom (Eskom Group Security Mandate; http://sustainability.eskom.co.za/sites/gs/Pages/Default.aspx).

6.3 ORGANOGRAM OF GROUP SECURITY WITHIN ESKOM'S SUSTAINABILITY SYSTEMS DIVISION

Figure 6.1 below sets out an organogram which reflects the structure of Eskom's Group Security.



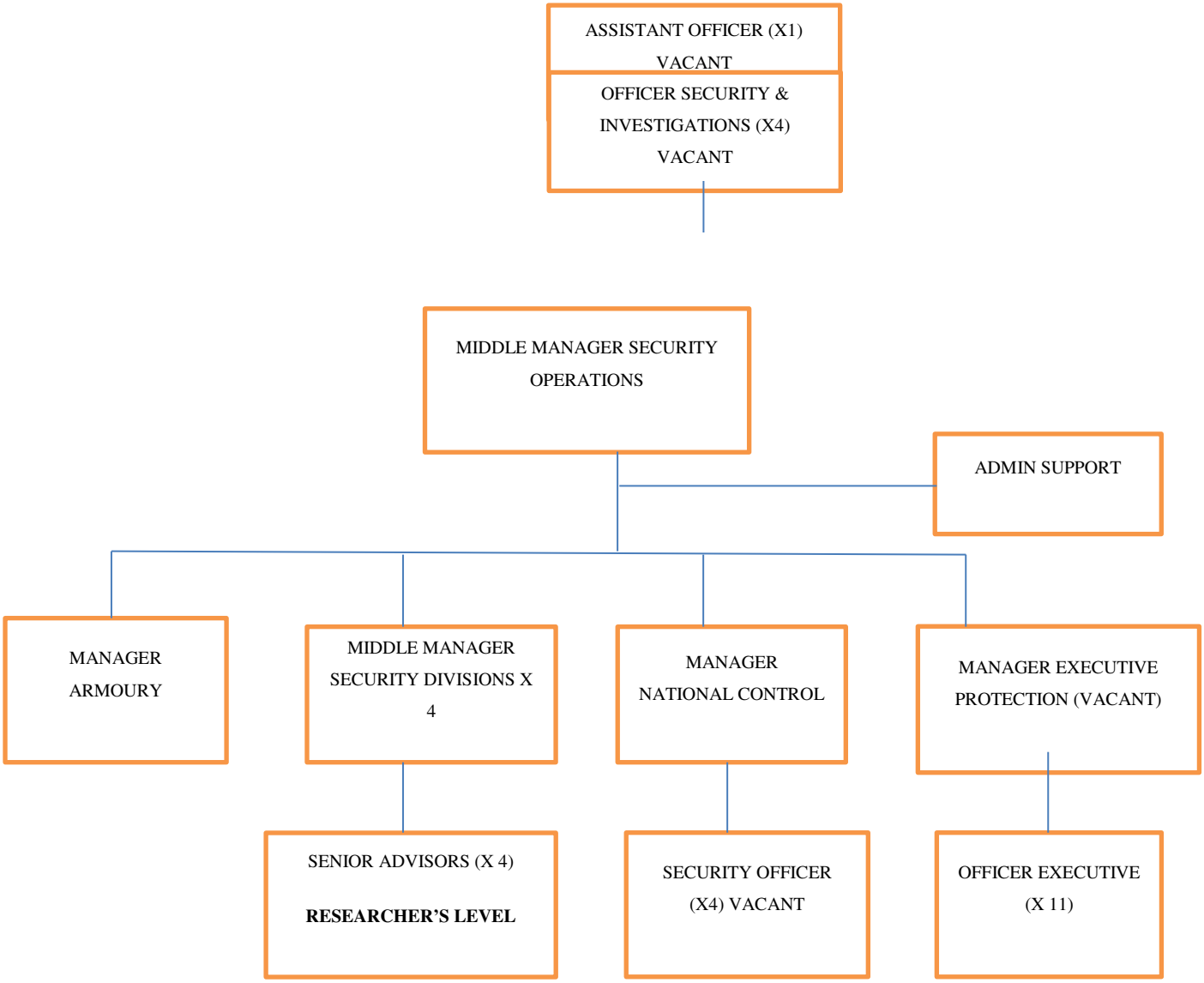


Figure 6.1: Organogram of Group Security within Eskom's Sustainability Systems Division

6.3.1 Discussion on the Organogram of Group Security within Eskom's Sustainability Systems Division

The current security structure is a very comprehensive structure. In reality, this means that security problems take longer to get resolved and to reach the Eskom's group security structure. It is important to note that Eskom's management is in the process of reviewing the security structure, which was scheduled to come into effect after 01 April 2016. The mechanisms and authorities for implementation of the new structure will more likely reside with multiple security structures, which is recommended and discussed further in Chapter Seven below (see section 7.5).

There have been new recent developments at Eskom and in the security structure. On the 5th July 2015, Major General (retired) TK Rakau was appointed as the Head of Security at Eskom, reporting directing to the Chief Executive Officer (CEO). The functions of Major General Rakau replace the previous operating structure, where the then Head of Security reported to the General Manager of Sustainability, who in turn reported to the Group Executive Sustainability.

6.4 WHY CAN THE INTERNAL SECURITY MANAGEMENT TEAM NOT STOP CABLE THEFT AT ESKOM?

The researcher has identified possible reasons (see sections 6.4.1–6.4.6) as to why the internal security management team cannot stop cable theft at Eskom. Certain issues were identified in questions, which led to the formulation of security-related statements which were put to fifty-five (55) participants, comprising Eskom employees, contract security supervisors and contract security managers and directors/owners (see Tables 6-1 to 6-6 below). Berg (2007:3) says that qualitative research refers to the meanings, concepts, definitions, characteristics, metaphors, symbols, and descriptions of things." The number, or numerical descriptions of things and their relationships are not the focus of this qualitative research, which utilises the focus of the "other" form of social science research: quantitative methods. The researcher utilised elementary data statistics to represent the percentages of participants that *"Agree", "Disagree"* or were *"Unsure"* with the security statements discussed. The data will be presented using tables.

As part of this investigative study, the following security-related statements were put to participants.

6.4.1 Eskom's security structures are not properly aligned

The organograms set out in Chapter Five (see sections 5.4 and 5.5 above), for Distribution, Transmission and Generation, operate independently from the above-mentioned organogram of Group Security (see section 6.3 above). Although the mandate of Eskom Group Security mentioned above (see section 6.2) is to effectively shape security management, to provide strategic services to treat security risks which impact on assets, information, interests, people, systems and processes, to maintain security at agreed risk levels, and to provide assurance that security is at a high standard, the only interaction between Group Security and the

regional security structures is based at an advisory level and not at an impact-making or decision-making level.

Security managers are deployed within Eskom and are found in all divisions of Eskom operations and at different levels within the organisation, ranging from M14 to E – Bands (Eskom's internal rank structures). They are responsible for managing security within their respective divisions at Eskom. The size and scope of their responsibility may differ, depending on the size of their divisions and the risks to their facilities.

The security managers for Distribution report to a Safety, Health, Environment Quality and Security (SHEQS) manager who in turn reports to the Grid Manager (Transmission security managers report direct to a grid manager), neither of whom is a security professional or a security expert, although both are experts in their fields of work. The Grid Managers assume responsibility for security in their regions, based on the title that was given to them as being asset owners. The Grid Manager is higher in rank and status than the SHEQS manager is.

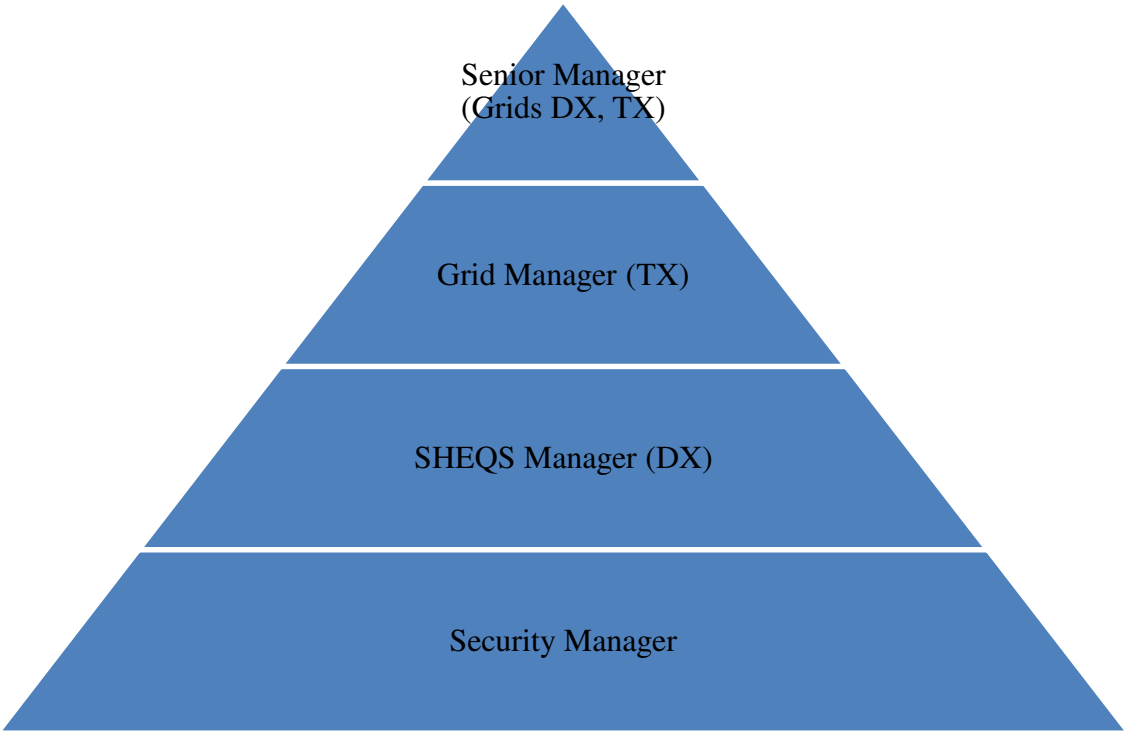


Figure 6.2: security managers reporting structure for Eskom's business units

Figure 6.2 above shows the reporting structure for security managers in Eskom's business units.

Table 6-1: Eskom's security structures are not properly aligned

Theme	Agree	Disagree	Did not comment
Eskom's security structures are not properly aligned	27 (49.09 %)	2 (3.64 %)	26 (47.27 %)

As shown in Table 6-1 above, 49.09 % (27 of 55) of the participants agree that Eskom's security structures are not properly aligned. However, 3.64 % (2 of 55) disagree, citing various reasons for their disagreements. Participant 20 said that *"It is easier to deal with the regional problems rather than going to head office for disagreements"*, while participant 25 said that *"I actually think that Eskom needs to realign its people rather than the structures"*. The majority of the people 47.27 % (26 out of 55) who did not respond were the contracted private security officers and inspectors employed by the private security companies.

6.4.2 Succession planning policies are not applied consistently in Eskom security divisions

Both lower-level and management-level employees need growth for them to remain motivated. In order for employees to produce acceptable and high quality work, they need to grow within the company. Highlighted in the study by many of participants was the fact that Eskom has a succession plan in place to replace near-to-exiting employees; however, this succession policy is almost non-existent within the security divisions.

Participant 8 mentioned that *"... although Eskom claims to have to have a succession planning programme in place, designed to identify talented individuals and prepare them for defined and specialised roles, we have not witnessed this ...."*

Participant 13 said, *"... Eskom security managers left the company and were then replaced by individuals who did not shadow them or were developed to succeed them. Some of these people came from outside the company, limiting our chances for promotion...."*

Participant 14 mentioned that "*… The same problem had occurred with the manager of the cable theft division with Eskom exiting the company after more than 25 years. The employee that departed without having a successor have unmatched technical knowledge and experience that is critical to the company's core mission in key areas such as preventing cable theft from Eskom ...."*

The research revealed that in the case of especially skilled employees working with cable theft incidents, finding and recruiting equivalent talent from outside the company would be extremely difficult, if not impossible: there simply are not many workers in the industry with similar expertise, which is why the researcher believes that it is extremely important for Eskom to ensure that proper succession planning is implemented within the security division (see section 8.7).

The research revealed that although the general mood within the security division was reasonable enough, the personnel in the division face challenges when positions are opened within their field of expertise. One interviewee (Participant 5) from Eskom security division had this to say:

"... when critical openings occur within the security divisions, Eskom must be ready to fill the positions with skilled, experienced internal candidates because they should have planned for such a transition – by ensuring that the individuals selected have been exposed to the proper training and career development opportunities. Eskom must be also ready to move selected employees strategically to fill the critical positions that open up ...."

The above statement shows that there is much to be done to help Eskom security personnel to get appointed to higher positions, and in line with their skill sets. There is a need to provide various support services to skilled Eskom security employees. Without good recruitment policies that benefit hard working and skilled personnel, the motivation of these people would be compromised.

Table 6-2: Succession planning policies are not applied consistently in Eskom security divisions

Theme	Agree	Disagree	Did not comment
Succession planning policies are not applied consistently in Eskom security divisions	17 (30.91 %)	0	38 (69.09 %)

As shown in Table 6-2 above, 30.91 % (17 of 55) of the participants agree that succession planning policies are not applied consistently in Eskom security divisions. The majority of the people, 69.09 % (38 out of 55), who did not respond were non-Eskom employees.

6.4.3 Eskom Security managers fail to consider recommendations made by private security companies to improve security measures to reduce losses

Meek (2014) mentions that the reason why security managers in parastatals and corporate companies fail to acknowledge the recommendations made by the private companies is simply that the private companies want to increase their profitability, rather than advance and improve their security measures to reduce losses. Reducing losses is considered to be an important aspect of the mandate of private security.

Private security companies are expected to identify risks and advise Eskom security of the ways in which these risks can be counter-measured. They are also expected to make recommendations. Similarly, Eskom management are expected to engage the private security companies in a discourse around what measures can be applied, and within what financial parameters.

Participant 54 mentioned:

"... sometimes the security companies have very good ideas, however, these ideas are very expensive and simply cannot be funded in the current financial climate ...."

Table 6-3: Eskom Security managers fail to consider recommendations made by private security companies to improve security measures to reduce losses

Theme	Agree	Disagree	Did not comment
Eskom Security managers fail to consider recommendations made by private security companies to improve security measures to reduce losses	34 (61.82 %)	11 (20 %)	10 (18.18 %)

As shown in Table 6-3 above, 61.82 % (34 of 55) of the participants agree that security managers fail to consider recommendations made by private security companies for improving security. Participant 19 said that "*Every time recommendations are made to the security manager, he says Eskom got no money"* participant 23 said that *"Eskom security divisions request that we do risk assessments and make recommendations, yet they don't even consider the recommendations".* On the other hand, 20 % (11 out of 55) participants disagree, citing various reasons for their disagreements. Many of the participants mentioned that the security companies made recommendations for more manpower to increase their revenue,

rather than for reskilling and retraining their own staff to become more effective. Lastly, 18.18 % (10 out of 55) participants did not comment.

6.4.4 Disjointed relationships between security managers and in-house security officials (Area officers, sections officers, security officers working for Eskom)

During a focus group meeting,[iv] the following comments were made (quoted verbatim):

"*… The security manager meets with the security company without involving us in the meetings ….*"

"… The security manager allows the security companies to do as they please and disregards our recommendations …."

"… The security companies don't listen or respect us because the security manager fails to take the necessary actions against them after we send him the inspection reports …."

"… The security guards remain on site despite us finding them sleeping on duty because the security manager does not give them penalties as per our recommendations …."

"… We don't know what the security contracts state because we are not shown the security contracts…. "

"… We are not allowed to work after hours and weekends to do spot checks on the security companies …."

"… Our job is nothing more than an inspector in a security company, the only difference is we get paid more to do less. We have the ability to do so much more and really get value from these companies, but our manager shoots everything we say down …. [sic]*"*

The challenges associated with disjointed relationships were almost common, among all lower-level security employees that the researcher focused on. The major problem associated with disjointed relationships was their dissatisfaction with the performance of their security managers. They were dissatisfied because their managers did not provide quality and precise direction in addressing major security concerns, and also because their managers failed to play a vital role in acknowledging their talents and implementing their recommendations for improving security within Eskom.

This resulted in qualified and educated employees (some of them university graduates holding B.Tech Degrees in Security Management from the University of South Africa – UNISA) being underutilised and demotivated. This also affected their sense of value within Eskom. Many of these employees can be seen as the foot soldiers in the security departments because they conduct inspections on the private security companies and report back to the security manager.

Table 6-4: Disjointed relationships between security managers and in-house security officials

Theme	Agree	Disagree	Did not comment
Disjointed relationships (lack of cohesions) between security managers and in-house security officials	26 (47.27 %)	9 (16.36 %)	20 (36.36 %)

As shown in Table 6-4 above, 47.27 % (26 of 55) of the participants agree that there is a lack of cohesion between security managers and in-house security officials as a result of their disjointed relationships. On the other hand, 16.36 % (9 out of 55) of participants disagree, citing various reasons for their disagreements, while 36.36 % (20 out of 55) participants did not comment.

6.4.5 Security contracts and oversight ownership are not structured evenly at Eskom

Eskom utilises a range of security services to protect Eskom assets, ranging from security guarding, monitoring, armed reaction, armed escorting, investigations, and security equipment installation companies. Fidelity Guards, G4S, IPSS, 2RM, Linda Security and Chubb Alarms are among the many security companies contracted to Eskom in South Africa.

The growing scientific evidence that Eskom security has produced allows the researcher to assess some preventative methods more intensively than others. Some of the evidence found during the researcher's working experience, and during this research, is strong enough to identify the fact that many security divisions in Eskom conduct ineffective management practices when managing private security companies contracted to Eskom, which is largely influenced by the unevenness in Eskom's security contracts.

The study found that the three biggest causes of this ineffectiveness are, firstly, the differences in contractual obligations and stipulations from one region and business unit to

another. Some of the regions include a penalty clause in their contracts, whereas others do not see a penalty clause as being an important tool for managing ineffective security services.

The second common problem is where the security managers fail to share the contract information with the assistant officers. The assistant officers are the people who actually manage the security contracts and provide feedback information to the security manager. The main question that should be asked here is, *"If the assistant officers do not have access to the security contracts that they supposedly have to manage, then what are they actually managing?"*

The third problem found during the research study is the failure of Eskom management to properly train the security staff on contract management. Eskom uses the New Engineering Contract (NEC) and, more particularly the Term Service Contract, as the basis for its security contracts. The Term Service Contract (TSC) is intended to be used for the appointment of a supplier for a specific period of time to manage and provide a service (https://www.neccontract.com/Products/Contracts/Term-Service-Contract).

The study discovered during the focus group discussion that many of the people working with the New Engineering Contract, and more particularly the Terms Service Contract, to facilitate the signature of the security contracts, have not been trained on how to implement the contract terms effectively so as to ensure that Eskom receives the best possible service from the security companies. The study further discovered that many of the security managers have also not received training to properly implement the NEC contract.

Table 6-5: Security contracts and oversight ownership are not structured evenly at Eskom

Theme	Agree	Disagree	Did not comment
Security contracts and oversight ownership are not structured evenly at Eskom	34 (61.82 %)	6 (10.91 %)	15 (27.27 %)

As shown in Table 6-5 above, 61.82 % (34 of 55) of the participants agree that security contracts and oversight ownership are not structured evenly at Eskom. Only 10.91 % (6 out of 55) participants disagree, citing various reasons for their disagreements, with inexperience and lack of training being some of the reoccurring reasons. Lastly, 27.27 % (15 out of 55) participants did not comment.

6.4.6 Criminals are adequately equipped and more determined

Many of Eskom facilities are guarded by unarmed security officers. A number of security officers have been killed while protecting Eskom's assets (Cf. Annexure A10), when criminals had entered Eskom premises unlawfully to steal copper cables (which is the most desired thing to steal, among other assets). The risk of violent attacks is a major challenge experienced by private security guards working at Eskom sites. It is not an understatement to say that many security officers working on Eskom premises have been killed, or killed themselves, in the line of duty.

These are some of those cases (Eskom fatality reports):

- On 8 February 2014, Mr Tsepo Justice Rakgotsoka (25 years old), who was employed by Sidas Security, was shot and killed at an Eskom substation in Rustenburg.

- On 2 May 2014, Mr Alfred Mosebetsi Skhebeza (35 years old), who was employed by FPM Business Solution as a security officer, was killed on duty at Delareyville CNC in the North West Province.

- On 27 August 2014, Mr Mahlabu Frans Ngobeni (39 years old), who was employed by Simango Business Services as a security guard, was killed while doing patrols at an Eskom building site in Sebayeng Township.

- On 27 August 2014, Mr Marata Dick Poopedi (37 years old), who was employed by Maximum Security as a security officer at Marble CNC in the Limpopo Operating Unit, was killed while on duty.

- On 29 September 2014, Mr Jimmy Bishop Makitla (32 years old), who was employed by Maximum Security as a security officer at Groblersdal zone in the Limpopo province, was killed while doing security patrols at the Eskom substations.

These deaths have made Eskom even more aware of the seriousness of cable theft and why it is important to make sure that adequate security measures are put in place to ensure that security officers have access to the correct support mechanisms for protecting their safety.

Table 6-6: Criminals are adequately equipped and more determined

Theme	Agree	Disagree	Did not comment

Criminals are adequately equipped and more determined	49 (89.09 %)	2 (3.64 %)	4 (7.27 %)

As shown in Table 6-6 above, 89.09 % (49 of 55) of the participants agree that criminals are adequately equipped and more determined. Participant 5 said that *"Criminals are often equipped with more dangerous weapons, like guns and bush knives, and the private guards face the risk of losing their lives by confronting the armed criminals. This situation has led to untimely deaths of many private security guards at Eskom".* The task of security guards becomes all that more difficult if the material they are contracted to secure is in great demand and left exposed to those that want to steal it (Meek, 2014; Nkabinde, 2014). Only 3.64 % (2 out of 55) participants disagree, while 7.27 % (4 out of 55) participants did not comment.

6.5 SUMMARY OF ESKOM INTERNAL SECURITY MANAGEMENT (EISM) PIE CHART

This pie chart indicates the percentage of participants (55) that agreed with the reasons why Eskom's internal security management team seemingly cannot stop cable theft (see section 6.4.1 – 6.4.6).



Figure 6.3: Pie Chart indicating the percentage of participants (55) that agreed with the reasons why Eskom internal security management team seemingly cannot stop cable theft

6.5.1 Explanation of the pie chart

In summary, the evidence of why the internal security management team seemingly cannot prevent cable theft at Eskom (see sections 6.4.1–6.4.6), displayed on the pie chart (from highest to lowest), indicates that the criminals are adequately equipped and are more determined (26 %). The security contracts and oversight ownership are not structured evenly

at Eskom (18 %). Eskom security managers fail to consider recommendations made by private security companies to improve security measures for reducing losses (18 %) and Eskom's security structures are not properly aligned (15 %), while disjointed relationships exist between management and lower level operational staff (14 %). Finally, the succession policy of Eskom is not applied consistently in Eskom security divisions (9 %).

6.6 WHAT ARE THE EXACT PROBLEMS WHY THE INTERNAL SECURITY MANAGEMENT TEAM STRUGGLE TO PREVENT CABLE THEFT AT ESKOM?

Welsh and Farrington (2010) are of the view that crime prevention has different meanings for different people. Programmes and policies designed by Eskom security to prevent crime can include joint operations between Eskom and private security as part of an operation to deal with cable theft, the contracting of private security to patrol a specific cable route, etcetera. Welsh and Farrington (2010) believe that these measures are crime control measures and that crime prevention refers to efforts to prevent crime, before the crime has been committed.

Cable theft is a crime which affects Eskom and this section will point out the exact problems which cause the internal security management team to struggle to prevent cable theft (see sections 6.6.1–6.6.7). Certain issues were identified in questions, which led to the formulation of security-related statements which were put to fifty-five (55) participants, comprising Eskom employees, contract security supervisors and contract security managers and directors/owners.

These statements were put to participants to investigate the issues described in the following subsections.

6.6.1 The absence of an accurate crime reporting culture relating to cable theft at Eskom

It is obvious that crime information regarding cable theft provides Eskom's security personnel with insight into this crime in terms of its progression, and what measures should be adopted to manage this specific crime. It is equally obvious that this information may provide relief to some people, through knowing something of the general status of this crime, although they may choose not to read the detailed information. For the researcher, it is

valuable information and provides an opportunity to evaluate the cable theft situation at Eskom and to further evaluate whether Eskom is providing the necessary resources to prevent and manage this crime. There is special significance in the title of this study, *Investigation towards the prevention of cable theft from Eskom*. The significance is that cable theft cannot be prevented if accurate reports are not recorded and evaluated by qualified security analysts.

Participant 10, who is also an analyst, said:

"*… I can only report to Eskom crime committee what has been reported on CURA and if security personnel responsible to report crime in their business units are not reporting the crimes then a true reflection of the crime activity within Eskom is not being captured* ....[sic]*"*

It should be noted that it is high time that Eskom employees should recognise that the crime reports constitute more than just an instrument for reporting crime, and that they also serve as an alarm to alert all concerned to the realisation that more needs to be done to prevent cable theft from Eskom. The most obvious and serious consequence of not reporting crimes, more particularly cable theft, is that Eskom may suffer unnecessarily by not knowing the exact loss of cable theft.

The cost to Eskom, and ultimately to South Africa, may be immense especially when compared with the small effort required to make a report that may result in enhanced protection of Eskom cables. Crime information is directed at safeguarding an organisation's assets against threats. Information is collected on incidents, threats and vulnerabilities that may illegally exploit the assets of an organisation and result in losses (Fischer *et al*., 2008: 149).

The security information culture in Eskom plays a key role in incident reporting, and all incidents that occur in Eskom are shared transparently with Eskom's employees and its contractors using Eskom's internal communication system, Intranet. Eskom management are faced with ever-increasing levels of complexity in managing the security of an organisation as large as Eskom and in preventing attacks that are increasingly sophisticated.

Garrett (2004) mentions that the vast majority of security breaches originate from human actions and lists a few potential reasons for this:

- People are poorly trained and have poor security awareness

- People are not motivated to perform at the required level
- People are malicious and deliberately expose the organisation to risk
- People are aware of the problem of security, but as managers and employees, they make poor decisions (Garrett, 2004).

Organisational culture, on the other hand, plays a key role in incident reporting. The key element here is that the organisational culture has to support a 'no blame' environment where people feel safe enough to report near misses or minor events that might otherwise go unnoticed (Talbot & Jakeman, 2009: 66; Govender, 2012).

Table 6-7: The absence of an accurate crime reporting culture relating to cable theft at Eskom

Theme	Agree	Disagree	Did not comment
The absence of an accurate crime reporting culture relating to cable theft at Eskom	17 (30.91 %)	0	38 (69.09 %)

As set out in Table 6-7 above, 30.91 % (17 of 55) of the participants agree that there is an absence of an accurate crime reporting culture relating to cable theft at Eskom. The majority of the people, 69.09 % (38 out of 55), that did not respond were non-Eskom employees. It is the absence of an 'information culture' in Eskom that indicates where the actual problems lie with the non-prevention of cable theft from Eskom.

6.6.2 Eskom appoints security companies that fail to establish strategic partnerships and develop crime prevention programmes to prevent cable theft during their contract term

There is a growing awareness among many of the participants, and other people interviewed for this research, that Eskom appoints security companies that fail to establish strategic partnerships and develop crime prevention programmes for preventing cable theft during their contract terms.

Being convinced by experience, the researcher found that a large percentage of security companies disregard transparency and honesty factors, and provide false and misleading company profiles when they submit company documents for security tenders. Many

companies purport to have a national footprint, strong infrastructure, specialised equipment and vehicles, skilled employees and the like.

Moodley (2014) believes that a strategic partnership works well to create security solutions. Companies must fully understand the business goals and thereafter combine their knowledge with Eskom's into actionable projects to prevent cable theft and other crimes. While the researcher believes this to be true, the private companies working for Eskom must also be willing participants in the contract.

Steenkamp (2002) says the scope of the duties of private security personnel is wide and varied. They prevent loss; they prevent crime; they protect persons, property and interests; and they protect and preserve environments to allow line function activities to go on.

Table 6-8: Eskom appoints security companies that fail to establish strategic partnerships and develop crime prevention programmes to prevent cable theft

Theme	Agree	Disagree	Did not comment
Eskom appoints security companies that fail to establish strategic partnerships and develop crime prevention programmes to prevent cable theft	36 (65.45 %)	10 (18.18 %)	9 (16.36 %)

As shown in Table 6-8 above, more than half of the participants (65.45 %, 36 of 55) agree that Eskom appoints security companies that fail to establish strategic partnerships and develop crime prevention programmes to prevent cable theft. Participant 52 said that *"We have been contracted to Eskom for more than 10 years and I am yet to see Eskom security managers form strategic partnerships to develop our managers."* Participant 51 said that *"We have been contracting nationally for Eskom for about 6 years and the only thing we get is warnings and threats to terminate our contract if we don't perform."*

Only 18.18 % (10 out of 55) of participants disagree, with participant 36 saying that *"Eskom spends hours every month in meetings with these companies to build relationships and partnerships, but some of these companies don't come to the party …"*, with participant 13 saying that *"We sometimes don't employ the right companies who understand strategies."* Lastly, 16.36 % (9 out of 55) of participants did not comment.

6.6.3 Security assessments in Eskom are not conducted meticulously and accurately to prevent repeated crimes

It is true that crime is not prevented alone by the private security companies contracted to Eskom. It requires collaborative efforts on the part of Eskom security as well. The number of repeated incidents continues to raise the crime statistics at Eskom. This is based on the voluminous body of literature that the researcher had used to come to this conclusion.

Following on the completion of a number of security assessments in Eskom, efforts to prevent repeat crimes have become a challenge, and in reality, these assessments are an important component in crime prevention. Security assessments are conducted to evaluate the security threats and risks and to provide solutions to crime prevention. An assessment is done not only when evaluating the risk profile of a facility, but an assessment is also done after security has been breached and a new profile then needs to be established.

Generally speaking, the most effective systems involve strong preventive instruments that are designed to suit the crime problem in high crime areas. This often requires a combination of multiple tactics, which usually include applying security upgrades. Furthermore, strong implementation is required, which is not easy to achieve, and reductions in repeat crimes do not necessarily coincide with an overall reduction in cable theft. In contrast, the least effective systems have weak preventive mechanisms (for example, recommendations are realistic but funding is not readily available) and poor implementation (for example, no action plan of execution, lack of security equipment).

It is high time that Eskom security personnel should conduct thorough security assessments, if they wish to realistically prevent crime and further repeated crime incidents. A realistic understanding of the actual risks will oblige security personnel to develop security countermeasures that mitigate risk and prevent repeated incidents. Gaps in knowledge on security assessment effectiveness, together with the need for Eskom management to take note of the gaps, are the subject of this section. The coverage here is by no means exhaustive. Rather, the researcher sets out to identify and discuss some of the most important issues for Eskom management to investigate and fix. This is certainly a matter which deserves more attention from management.

Bayne (2002) believes that any security assessment conducted endeavours to answer the following questions:

- What needs to be protected?
- Who/What are the threats and vulnerabilities?
- What are the implications if assets were damaged or lost?
- What is the value to the organisation?
- What can be done to minimise exposure to the loss or damage? (Bayne, 2002).

The security assessment approach recognises that crime could have a profound effect in terms of further losses to Eskom, should this process not be completed accurately and diligently. Therefore, the security assessment process must seek to address the weaknesses in security so that further criminal acts can be prevented.

Table 6-9: Security assessments in Eskom are not conducted meticulously and accurately so as to prevent repeated crimes

Theme	Agree	Disagree	Did not comment
Security assessments in Eskom are not conducted meticulously and accurately so as to prevent repeated crimes	47 (85.45 %)	6 (10.91 %)	3 (5.45 %)

As shown in Table 6-9 above, more than half of the participants (85.45 %, 36 of 55) agree that security assessments in Eskom are not conducted meticulously and accurately. Participant 17 said that *"I have seen many cases where the Eskom guys copy and paste the information of past assessment documents in the present documents; they say the risks are the same so they don't need to repeat the procedure."* participant 19 said that *"The problem with Eskom management is that they want things to be done professionally but they introduce new ways of doing things without giving us training. I saw a new assessment document but I don't know how it needs to put into practice."*

Only 10.91 % (6 out of 55) disagree, with participant 2 saying that *"I don't know what other regions are doing, but we make sure that we do the assessments professionally"*, with another participant (4) saying that *"We check the assessment documents and compare stats to ensure the information is current."* Lastly, 5.45 % (5 out of 55) of participants did not comment.

6.6.4 The need for Eskom investigators to forge closer relationships with the police investigators and justice department

A South African Law Commission (SALC) criminal case outcome research report (18) Project 82 (http://www.justice.gov.za/salrc/rpapers/rp18.pdf), has noted the importance of measuring the effectiveness of the criminal justice system as a whole, rather than artificially isolating its constituent elements. For this reason, they mention that it is useful to measure the number of convictions compared with the number of cases reported to the police to get a sense of how effectively the police and prosecution authority work together to hold perpetrators of crime accountable for their actions.

The report says that the ratio of convictions to acquittals is influenced by a number of factors, including:

- The quality of the police investigation;
- The experience of the prosecutors and their ability to effectively present the State's case, and;
- The extent of cooperation by witnesses, including the complainant, with the State.

Eskom investigators must not be concerned exclusively with only the completion and handing over of investigations, but should rather work closely with the police and public prosecutors to run the full extent of the court case to secure convictions. They must concern themselves with methods that have been successful in previous prosecutions and forge a closer relationship with the police and justice department.

The Department of Justice (DOJ) had recommended that SAPS and the Directorate for Priority Crime Investigation (DPCI) provide training to enhance the prevention, investigation, and prosecution of cases relating to non-ferrous metals thefts. They say that although police would often affect arrests, the courts tended not to give priority to these crimes, and this often led to cases being withdrawn. The DOJ mentioned that it was important to have a common understanding of the seriousness of the crime between the victims, police, prosecutors and magistrates (http://www.pmg.org.za/report/20120228-departments-energy-public-enterprises-justice-salga-transnet-and-eskom).

Mistry (1997) believes that inadequate training hampers the ability of prosecutors to do their work properly. She said that the current university education did not prepare prospective prosecutors for the practical side of their work.

The researcher believes that it is illustrative to mention the case of Fana Ben Msimanga [Msimanga v S (A119/12) [2013] ZAFSHC 26 (4 February 2013)], Case no: A119/12]. The appellant, Mr Msimanga, was convicted of theft of copper-conducting cable by the regional magistrate at Viljoenskroon and sentenced to nine (9) year's imprisonment. Eskom (and other victims of cable theft crime) would benefit tremendously if all the cable theft trials were carried out like that of Fana Ben Msimanga.

In line with this discussion and the above-mentioned case example, the researcher believes that the effective performance of the investigators (both private and in-house) should be measured by the number of cases that are taken to court and the number of convictions achieved in those cases. It is particularly important for Eskom that people involved in cable theft are convicted and appropriately punished in terms of the judicial process of South Africa.

Table 6-10: The need for Eskom investigators to forge closer relationships with the police investigators and justice department

Theme	Agree	Disagree	Did not comment
There is a need for Eskom investigators to forge closer relationships with the police investigators and justice department	34 (61.82 %)	11 (20 %)	10 (18.18)

As can be seen in Table 6-10 above, more than half of the participants (61.82 %, 34 of 55) agree that there is a need for Eskom investigators to forge closer relationships with the police investigators and justice department in order to secure harsher sentences for criminals convicted of stealing Eskom cables. Participant 54 said that *"If the prosecutors are not told of the direct and indirect losses, then the cases are not taken seriously,"* participant 5 said that *"Prosecutors don't know the challenges we experience with cable theft, therefore they must be educated to give harsher sentences."*

However, 20 % (11 out of 55) disagree, with participant 7 saying that *"It does not take an expert to influence harsher sentences for cable theft because prosecutors are educated and*

should know cable theft effects everyone". Lastly, 18.18 % (10 out of 55) of participants did not comment.

6.6.5 Eskom security officials cannot identify the cable after it is stolen, which increases the problem of cable theft

Another matter deserving of more attention is the urgent need for Eskom to mark its cables to make it easy to identify them after they are stolen. The literature study (see section 3.3.3 above) found that the inability to properly identify stolen copper cables remains one of the main reasons why copper cables were so easily reintroduced in the recycling industry. Eskom security is regularly facing these challenges (Nkabinde, 2014).

While plans are already in place at both Eskom and other users of cable to mark their cables, there is still a long way to go in getting all the cables marked. The researcher believes that retro-marking the existing cables would be a difficult, if not impossible, task.

This marking process would help to prove, in court, that the suspect was illegally in possession of a particular piece of cable, which had been installed at a specific place, for a specific service provider (Ogle, 2014; Booysen, 2014; Traceable solutions, 2012, http://www.tracesol.co.za/about/articles/traceability-solutions-joins-the-fight-again-copper-cable-theft).

Table 6-11: Eskom security officials cannot identify the cable after it is stolen, which increases the problem of cable theft

Theme	Agree	Disagree	Did not comment
Eskom security officials cannot identify the cable after it is stolen, which increases the problem of cable theft	34 (61.82 %)	6 (10.91 %)	3 (5.45 %)

As shown in Table 6-11 above, more than half of the participants (61.82 %, 34 of 55) agree that Eskom security officials cannot identify the cable after it is stolen, and this increases the problem of cable theft. Only 6 participants (10.91 %) disagree, while 3 (5.45 %) did not comment.

6.6.6 Eskom security must support the use of intelligent security systems to manage private security guards and supervisors

While the prevention of cable theft is by far the predominant focus of this study, there are many other issues that can be measured and have direct bearing on the effectiveness of Eskom security and the private security to prevent crime and cable theft. Additionally, if Eskom wishes to receive a higher level and quality of security that integrates current technology, then proper management, research and oversight of its security systems should receive serious attention, nationally.

It can be said that there are many potential benefits associated with the use of intelligent security systems. The intelligent systems referred to here are real time guard monitoring systems, CCTV, etcetera. The potential benefit of using intelligent systems in reducing crime through deterring security officers from becoming complacent may be much lower on Eskom's list of priorities than the physical prevention methods, which include regular patrols in high crime zones by the private security officers at its facilities.

Eskom security and the private security supervisor's safety is another potential benefit associated with CCTV. This has been experienced through the installation of CCTV cameras in inspection vehicles and on clothing to record the events of site visits, for example.

Table 6-12: Eskom security must support the use of intelligent security systems to manage private security guards and supervisors

Theme	Agree	Disagree	Did not comment
Eskom security must support the use of intelligent security systems to manage private security guards and supervisors	49 (89.09 %)	2 (3.64 %)	4 (7.27 %)

As shown in Table 6-12 above, more than half of the participants (89.09 %, 49 of 55) agree that Eskom security must use intelligent security systems to manage private security guards and supervisors. Participant 3 said that *"If they spent so much money on security guards then surely you can spend a bit more on intelligence security systems to monitor and protect those guards."*

6.6.7 Eskom in-house security officials need to work shifts to provide proper oversight management for security providers

Most evaluations of crime prevention programmes at Eskom are area or regional based. Advancing knowledge about the effectiveness of crime prevention programmes should begin with attention being given to the methodological rigour of the evaluation of private security and their ability to prevent crime during the 24-hour cycle which Eskom demands and pays for.

Many of the participants believe that it is desirable for future evaluations to compare the shift work of private security with that of the Eskom security personnel who provide oversight management for security providers to Eskom. It is also desirable in future evaluations to compare cost–benefit analyses to assess the financial costs of paying overtime to Eskom security to conduct oversight facility visits. The participants believed that in the interests of maximising the effectiveness of Eskom security and reducing operational costs, they need to be working on a shift basis aligned with private security, and not the current office hours routine.

Table 6-13: Eskom in-house security officials need to work shifts to provide proper oversight management for security contractors

Theme	Agree	Disagree	Did not comment
Eskom in-house security officials need to work shifts to provide proper oversight management for security contractors	49 (89.09 %)	3 (5.45 %)	3 (5.45 %)

As indicated in Table 6-13 above, more than half of the participants (89.09 %, 49 of 55) agree that Eskom in-house security officials need to work shifts to provide proper oversight management for security contractors. Participant 29 said that *"If the security operations are on a 24-hour mandate, then why do we only work 07h30 to 16h00, Mon – Fri. We need to do inspections and spot checks to have the element of surprise."* Participant 44 said that *"We never see the Eskom security people after hours. They don't come and check on us, so most of the guards relax and sometimes sleep and don't patrol because of this."*

6.7 PIE CHART SUMMARY OF WHY THE INTERNAL SECURITY MANAGEMENT STRUGGLE TO PREVENT CABLE THEFT

This pie chart indicates what the exact problems are as to why the internal security management team struggle to prevent cable theft at Eskom (see section 6.6.1 – 6.6.7).

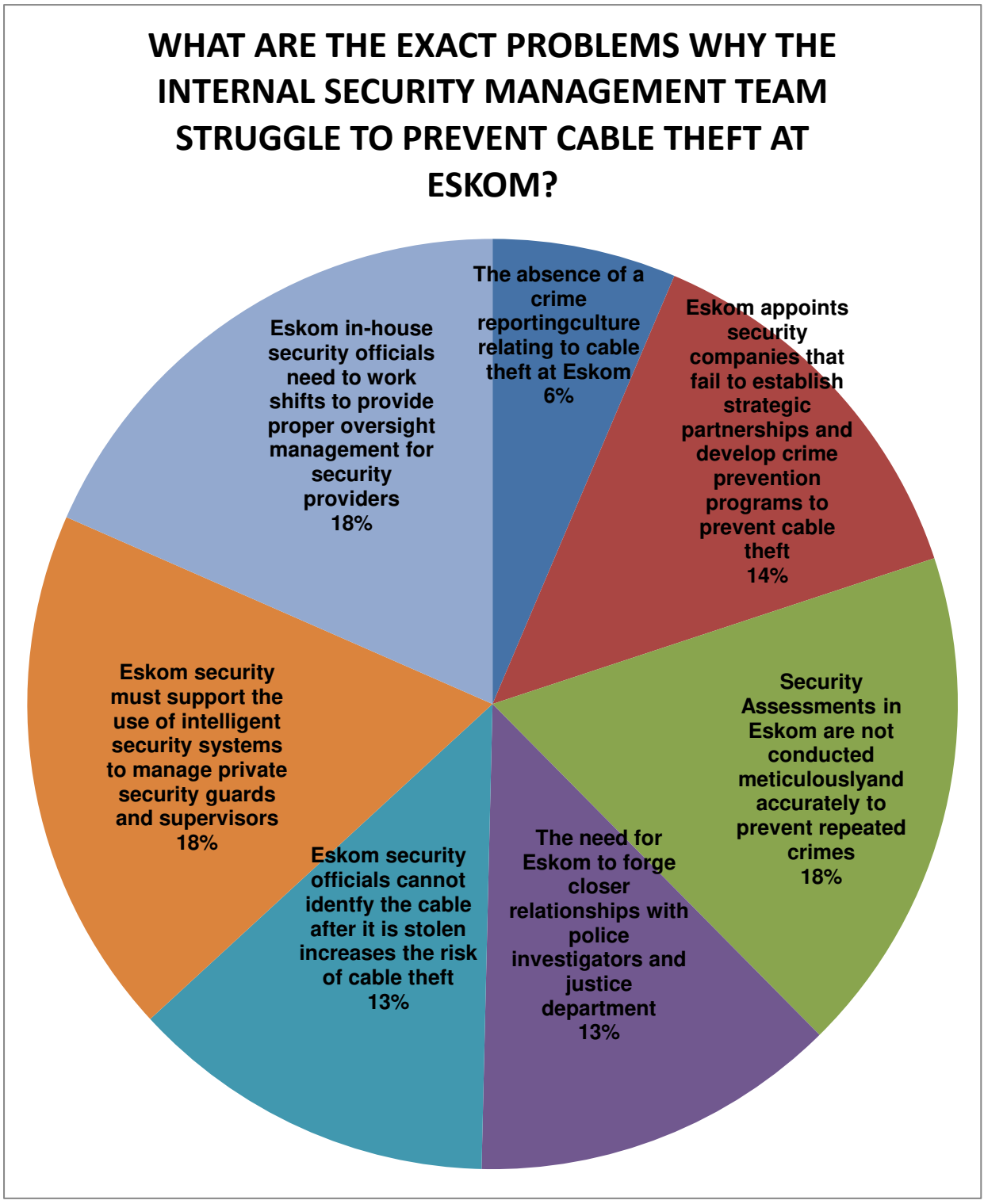


Figure 6.4: Pie Chart indicating the percentage of participants (55) that agreed with what the exact problems are as to why the internal security management team struggle to prevent cable theft at Eskom

6.7.1 Explanation of the pie chart

In summary, the evidence of what the exact problems are as to why the internal security management team seemingly cannot prevent cable theft at Eskom (see section 6.7), which is displayed on the pie chart shown in Figure 6.4 above, indicates (from highest to lowest) that security assessments are not conducted meticulously and accurately enough to prevent repeated crimes (18 %). Eskom security must use intelligent security systems to manage private security guards and supervisors (18 %); and Eskom in-house security officials need to work shifts to provide proper oversight management for security contractors (18 %).

There is a concern that Eskom appoints security companies that fail to establish strategic partnerships and develop crime prevention programmes for preventing cable theft (18 %). There is a need for Eskom investigators to forge closer working relationships with the police and Justice Department (13 %). The fact that Eskom security personnel cannot identify Eskom cable after it is stolen increases the risk of cable theft (13 %). Finally, there is a concern with the absence of an accurate crime reporting culture relating to cable theft at Eskom (6 %).

6.8 ESKOM'S CURA SYSTEM AND CABLE THEFT

Crime prevention has today, more than ever before, entered a new, more pressing phase in the need to have accurate and relevant crime data which holds greater relevance for crime prevention policy and practice. Certainly, in Eskom crime data stands as an important component of the overall crime prevention strategy to reduce crime, and more importantly, cable theft.

In order to implement effective proactive, predictive and/or intelligence-led strategies, Eskom must have excellent data. The more accurate, complete, timely and available the crime data is which is collected and kept at Eskom, the better it will be for Eskom security managers, who are tasked with preventing cable theft, in doing their job.

The data relating to cable theft incidents occurring at Eskom-guarded facilities is useful for compiling crime statistics, because it represents an official record of crime occurring where Eskom is paying their security guards to protect its assets. All divisions and regions that experience crime incidents, including cable theft crimes, collect information and record it on CURA in the allocated information blocks that are pre-set on the system.

The need to have credible data has brought greater attention to the need for higher quality data capturing and dissemination evaluations, as well as the need for more rigorous, systematic methods to synthesise the data and examine data policy implications. Related to this development is the growing evidence base of the effectiveness of the wide range of crime prevention models applied at Eskom.

Also of importance to crime preventions standing is the widely held view of the need to strike a greater balance between accurate and consistent crime reporting. This has become more urgent in recent years with the accumulation of inaccurate reports, compounded by years of weak policies for properly enforcing the need for Eskom personnel to report consistently. This need to provide accurate and consistent reports seems well poised to help change this state of affairs and make a major contribution to crime reduction at Eskom.

Participant 4 (interview 4) had this to say about CURA:

"… *CURA is not the best system, but it is the only system currently being used at Eskom ….*"

Participant 14 (interview 14) mentioned the following problems with the CURA system:

"… *the CURA system has many defaults and sometimes don't reflect the same information we put in it. We have experienced information going missing and does not reflect accurately. The information is not shared transparently to all regions. Training is only on request and not on a regular basis. The system is not effective and needs more blocks to include more information. The reporting is too long and cumbersome which is why managers don't report regularly. There is a lot of repetition to report one case ….*"

Jenkins (2015) believes that the CURA system is just a statistical technique used for reporting crime stats to management. He also says that, due to the lack of connection to crime systems, it is not used in the prevention of crime. Jenkins (2015) further states that, to date, the statistics available from CURA have not been used for the deployment of personnel in high risk areas.

Generally speaking, an incident is recorded once it has come to the attention of Eskom analysts, and it must then become a source of up-to-date information that can be broken down by day, month, year and so on. This information enables cable theft data to be used for comparative purposes and to track trends in the incidence of thefts in certain areas of the business.

What is also interesting to note, and deserves urgent attention, is one other reason for the inaccurate reporting of statistics: there are people recording information on Eskom's CURA system who have not received formal training to work on this system (Nkabinde, 2014c; Ogle, 2014b). The researcher believes that continuous and relevant training for security personnel working on the CURA system is a perfect way of ensuring that the system is being effectively utilised, and that Eskom would benefit from having accurate and reliable information.

6.9 ESKOM'S NETWORK EQUIPMENT CRIME COMMITTEE (ENECC) REPORT: DOES IT PREVENT OR EXACERBATE CABLE THEFT?

According to Govender (2012), a culture of security is, inter alia, the logical conclusion of a well-driven security awareness programme. Once people become aware of incidents, threats and vulnerabilities affecting the assets of an organisation, it will then be in their nature to react to it.

Understanding crime has the primary benefit of assisting in making good security decisions, which are effective in preventing real risks in a cost effective manner. It is an important step in the total process of understanding crime and that is achieved through crime awareness. The researcher is of the opinion that all Eskom crime reports should identify and highlight concentrations of where crime is taking place and where the need exists to focus on crime prevention efforts. The researcher believes that this analysis can help forecast future crime problems, with the aim of developing pre-emptive strategies for Eskom.

Eskom Group Security sends out a monthly crime report, entitled "ENECC Report". This ENECC (Eskom Network Equipment Crime Committee) Report is sent to Eskom security experts, senior management and Eskom executive committee members that have been working in the Eskom security fraternity for more than 20 years, and some even longer.

This section is intended to highlight a few shortcomings identified in the ENECC Report (see section 7.11), which can be identified by the following areas of enquiry:

- What reason was recorded for the increase or decrease in crimes of cable theft.
- Whether any of the people arrested for cable theft were convicted after the court proceedings and what punishment was handed down.

- Whether Eskom had any control over the losses that it experienced with cable theft.
- The summary of the performance of the private security contractors should not be limited to the two companies mentioned in the report, but that it should extend to all the private security companies contracted to Eskom.
- A table indicating Eskom's national cable theft hot spot areas.

It is true that crime is prevented by optimising security. Optimising security must be driven by data to establish good security programmes for reducing crime.

Nkabinde (2014) says that the cable theft information must stand out in any report, because of the negative impact it has on service delivery and the high losses that Eskom suffers. The opportunities for identifying poorly performing security companies will be immediately noticed and action can be taken immediately by the CCC.

Carstens (2015) confirms that the ENECC Report does not prevent or promote cable theft and believes that it is basically an information sharing report. The researcher would like to contribute to Carsten's (2015) statement by mentioning that if it does not prevent cable theft, then it should be reviewed. The main function of the ENECC Report must be to prevent cable theft and not allow it to get worse.

The ENECC crime report is by inference placed in its proper setting as an important instrument that Eskom uses to highlight the crime incidents at Eskom. The prevention and control of crime should, therefore, also be the focus of this report. If Eskom management identify security threats early, an immediately security plan can be established to manage this problem.

To answer the question: *Does the ENECC report prevent or exacerbate cable theft?*

Effective and reliable information is central to all good crime prevention plans, principally because the necessary resources can be directed to specific crime problems observed in crime reports. The researcher is therefore of the view that the ENECC Report currently exacerbates cable theft because if management is not aware of where the cable theft is occurring and of which security company is tasked to prevent cable theft and is thus failing in its obligation to Eskom, then it means that no action can be taken to prevent cable theft or to minimise losses to Eskom.

Participant 4 had the following to say about the ENECC report:

"… the information in the ENECC report is helpful to an extent, but I cannot use it to combat cable theft. I don't see exactly where the cable theft is occurring (Eskom guarded site or open network). The strategy is practical that they apply in the ENECC report ….[sic]*"*

6.10 WHAT DID SOME OF THE PARTICIPANTS SAY WHEN ASKED THE FOLLOWING RESEARCH QUESTION: *IF THE PRESIDENT OF SOUTH AFRICA INSTRUCTS YOU TO IMMEDIATELY STOP CABLE THEFT AT ESKOM, WHAT WILL YOU DO WITHIN ONE MONTH*?

The participants gave the following responses to the above-mentioned question:

"… One month will not be enough to do anything substantial. You might be able to focus on your hotspots areas but then additional resources will be required. However, given unlimited resources you might be able to achieve an impact but that will require a longer period than a month. But stop it entirely – never…." (Participant 7, interview 7).

Researcher's comment: South Africa has many law enforcement agencies that could be called on and their resources integrated to minimise this problem, without having to be given unlimited resources. Unlimited resources are not possible.

"… Upgrade the security at substations to ensure sites are protected, Increase frequency of line inspections, Address offset of product by increasing proactive inspections at scrap dealers and ports, Ensure that consequence of crime carry major penalties …." (Participant 52, interview 52).

Researcher's comment: This recommendation would be too expensive to implement; rather, a wake-up call to security companies is required, to the effect that Eskom will terminate their contracts if this problem is not appropriately dealt with.

"… declare an emergency and deploy and increase security measures, increase private security and technology measures like we did in the world cup where we have zero increases. I would employ more effective techniques like dogs, armed guards, and patrol vehicles …." (Participant 15, interview 15).

Researcher's comment: This is a long-term solution.

"…. Currently under the law, those charged with theft of our cables are charged with common theft. I will ensure that the laws toughening up of the legislation to make the crime of cable theft become an economic sabotage problem and the courts must pass harsher sentences on those convicted for cable theft …." (Participant 41, interview 41).

Researcher's comment: The Criminal Law Amendment Act, 1997, was passed on 29 October 2015. This was done to regulate the imposition of discretionary minimum sentences for essential infrastructure-related offences; to create a new offence relating to essential infrastructure; and to provide for matters connected with infrastructure-related offences. The researcher views this as a step in the right direction, although it will take a few months to effectively implement.

"… I will convince all citizens to demonstrate civic pride and a sense of co-ownership of the country's resources and assets and reward them adequately for handing over criminals and people involved in cable theft without fear of being intimidated or victimised …." (Participant 37, interview 37).

Researcher's comment: This is a long-term solution'

"… I will set up a specialised team within the Hawks to investigate scrap dealers and syndicates …." (Participant 42, interview 42).

Researcher's comment: This recommendation is reactive.

The information obtained from interviews, and stated above, revealed the many different views given by the participants on how they would stop cable theft within a month, if requested by the president. It is clear from the above extracts that these participants believed that something was possible and could be done within a month to stop cable theft.

6.11 FURTHER INFORMATION SUPPLIED BY THE PARTICIPANTS RELATED TO CABLE THEFT

The participants provided the following additional information related to cable theft:

"… Lack of properly skilled and motivated resources, Disinterest of some management employees, Lack of pride in their work, Lack of dedication …." (Participant 12, interview 12).

"…. although the scale of the problem has been recognised for years, measures to prevent cable theft have comprehensively failed. It is time now for the Police and law enforcement

agencies to focus on the points of trade, the scrap dealers and other businesses where stolen cable is cashed in and processed. I believe we will stand a better chance of cutting off the flow ...." (Participant 14, interview 14).

"... The security guards working on Eskom facilities must be vetted consistently before deployment and be polygraphed every six months to make sure they are not involved in cable theft. Eskom security must manage these security companies very strictly and only appoint them if they can prevent cable theft from Eskom ...." (Participant 18, interview 18).

"... Eskom must fast track the issue of marking its cables and also find a solution to mark the cables that are existing on the network. The security companies must be held financially accountable for all cable theft losses which occur while they are on duty to protect Eskom ...." (Participant 25, interview 25).

"... Copper should be classified as a precious metal, which will allow the courts to pass heavy sentences on thieves ...." (Participant 53, interview 53).

The information obtained from interviews, and stated above, revealed the many different views given by the participants on cable theft. It is clear from the above extracts that these participants are concerned with the problem of cable theft and gave suggestions of what they believe are solutions on how to stop cable theft.

6.12 SUMMARY

Chapter Six is, in a certain sense, one of the two most important chapters of this study. It contains an introduction (see section 6.1), and attention was then paid, inter alia, to the following issues: group security's role within Eskom's sustainability division (see section 6.2), an organogram of group security within Eskom's sustainability systems division (see section 6.3), the issue of why the internal security management team cannot stop theft at Eskom (see section 6.4), what the exact problems are which cause the internal security management team to struggle to prevent cable theft at Eskom (see section 6.5).

Also examined were Eskom's CURA system and cable theft (see section 6.8); the Eskom Network Equipment Crime Committee (ENECC) Report, and whether it prevents or exacerbates cable theft (see section 6.9); what some of the participants said when asked the research question: "If the President of South Africa instructs you to immediately stop cable theft at Eskom, what will you do within one month?" (see section 6.10); and certain further

information supplied by the participants related to cable theft (see section 6.11). The chapter concludes with a summary (see section 6.12).

Chapter Seven discusses the action steps necessary to prevent copper theft from Eskom.

CHAPTER SEVEN
ACTION STEPS TOWARDS THE PREVENTION OF CABLE THEFT FROM ESKOM

7.1 INTRODUCTION

While Chapter Six focused mainly on Eskom's internal security management team and those responsible for the capturing of all relevant information related to cable theft, this chapter examines what action steps must be taken to prevent cable theft at Eskom. This is in line with research aim 1.8.7 found in Chapter One (under the heading "Research Aims").

In this chapter, there are three questions and four discussion points for consideration:

- What must the Eskom internal security management team and those responsible for the capturing of all relevant information related to cable theft do to prevent it?
- What must the Eskom internal security management team demand from its in-house security personnel?
- What must the Eskom in-house security personnel demand from the contracted private security companies to prevent cable theft?
- Proposed: Eskom security structure
- Proposed: A newly designed training standard for all private security contracts at the Eskom facility
- The Eskom CURA system
- The structure of the ENECC report.

The views of the interviewees and information obtained from the observations and other relevant documents constitute the focal point of this chapter. The researcher is of the view that the prevention strategies presented in this chapter are based on the best available evidence, as informed by the research study. These strategies must be used to prevent cable theft from Eskom.

7.2 INFLUENCING THE JUDICIAL PROCESS

It is important to assess the effectiveness of the judicial process for cable theft crimes and to influence it to benefit Eskom. The crime statistics reflect the crime situation and its effect on Eskom; however, little is known about the effectiveness of judicial processes and why the outcomes of cable theft crimes are not influencing and deterring criminals from stealing cables.

The focus on the judicial process is not meant to diminish the importance of the efforts made to reduce cable theft crimes in the courts. Instead, the focus of this section allows for a more comprehensive examination of the judicial process and cable theft in order to do better crime prevention. The focus is also driven by the growing number of cases that go to court, but are not successfully prosecuted.

Before a case can be presented in court, the prosecutors need to have a comprehensive understanding of the matter before they can prepare for the trial. This comprehensive understanding helps the prosecution to evaluate the risks and losses that Eskom experiences with cable theft. It is with this context that Eskom legal experts should be part of the investigation process in cable theft investigations, and further, be part of the court processes. They need to advise the investigators of the relevant legal requirements, provide legal opinions on cases, and give evidence as expert witnesses on the losses that Eskom experiences with cable theft. According to Mistry (1997), inadequate training hampers the ability of prosecutors to do their work properly. University education does not prepare prospective prosecutors for the practical side of their work.

Nel (2012) believes that cable theft cases are not being successfully prosecuted because the investigators do not possess legal expertise and cannot talk the same legal language as the prosecutors, and feels that Eskom legal experts can help investigators motivate that higher sentences be handed down to criminals that steal Eskom cables.

The Criminal Law Amendment Act, 1997, was passed on 29 October 2015. This was promulgated to regulate the imposition of discretionary minimum sentences for essential infrastructure-related offences; to create a new offence relating to essential infrastructure; and to provide for matters connected with infrastructure-related offences. The researcher views this has a step in the right direction, although notes that it will take a few months for the Act to be effectively implemented.

Legal experts should provide a uniform understanding of how to implement the Second-Hand Goods Act (No 6 of 2009), so as to strengthen the hand of Eskom investigators in dealing with cable theft investigations and court proceedings. Ras (2015) believes that if Eskom losses could be prevented, Eskom could progress and would be able to provide unserved parts of South Africa with much-needed electricity.

In the light of this belief, Ras (2015) mentions that if the actual losses were provided in court to educate the courts of the financial implications of cable theft for Eskom and the country, then the courts would consider this information as aggravated circumstances and would hand down longer prison terms to deter other people from stealing cables.

7.3 INFLUENCING LAW ENFORCEMENT AGENCIES

The increasing pressure from both the private and public sector for Eskom to maintain better control over the power cuts in South Africa means that security must be incorporated early and comprehensively in the security planning and protection processes. When cable theft is addressed effectively as a whole, it will be possible to reduce the operating cost and increase the effectiveness of Eskom. It is this progress, and the inclusive philosophy that activates it, that makes it appropriate to discuss the role of law enforcement as part of the security programme to prevent cable theft.

Eskom needs to engage the law enforcement agencies more vigorously to help in the fight against cable theft. What is obvious is that they would require education and training on the facts of Eskom's cables. Noah (2012) agreed that law enforcement agencies need to increase the efforts to arrest and prosecute cable thieves, and further noted that Eskom had to work with communities and law enforcement agencies to raise awareness and thus make them realise that they are part of the crime solution (http://www.pmg.org.za/report/20120228-departments-energy-public-enterprises-justice-salga-transnet-and-esko).

Binderman (2012) believes that systematically training police officers on the ground will result in stopping nonferrous metal theft. Booysen (2014) recommends that the development of a training manual will assist the South African Police Service (SAPS) in combating nonferrous metal theft more effectively (http://www.engineeringnews.co.za/article/saps-to-tackle-copper-cable-theft-2013-07-12).

7.4 WHAT MUST ESKOM'S INTERNAL SECURITY MANAGEMENT TEAM AND THOSE RESPONSIBLE FOR THE CAPTURING OFF ALL RELEVANT INFORMATION RELATED TO CABLE THEFT DO TO PREVENT IT?

This section specifically focuses on what is required by Eskom's internal security management team, and those responsible for the capturing off all relevant information related to cable theft, in order to prevent it. In order to better comprehend some of the problems preventing Eskom's security from achieving its objectives, it is necessary to first pay attention to the issues that it is faced with.

An effective security management division, including those responsible for capturing information, requires not only having competent staff, but also well-designed and efficient administrative and reporting systems. Management skills are, therefore, necessary for an effective oversight management function of the security division, especially for those that manage the private security and in-house officials.

7.4.1 Improve relationships between security managers and in-house security officials

Given the overall objective of this study, and in line with finding solutions to prevent cable theft at Eskom, it was reasonable for the researcher to engage the participants in a critical dialogical reflection to determine what the problems are (see subsection 6.4.4). That question was particularly relevant to the participants because a joint effort and collaboration is required to prevent cable theft.

During the interviews, the majority of these participants openly and confidently discussed relationship problems in their respective security departments. While holding the view that "*Security managers have the final word on decisions*", many of these participants emphasised that their growth in the company was being stifled and that they are definitely divided in the way they operate and treat each other. Many of the participants were happy to contribute to the prevention of cable theft and security programmes, but felt rather constrained in their jobs.

Generally, throughout the various stages of this research, the participants revealed strong determination to work diligently and tirelessly in ensuring that private security is working in line with the terms of their contractual obligation. They maintained a high service level output, but highlighted numerous constraining conditions that impaired their efforts. Some of

these conditions included the lack of resources needed to work overtime and the lack of cooperation from managers to support these operations.

7.4.2 Eskom's security management must realign its security contracts, form strategic partnerships with private security companies, and develop effective crime prevention programmes to prevent cable theft

Given the overall objective of this study, and in line with finding solutions to prevent cable theft at Eskom, it was reasonable for the researcher to engage the participants in a critical manner to understand why Eskom continues to contract with private security companies that fail to protect its cable from theft at its facilities (see subsection 6.6.2). Likewise, the participants from Eskom security and the private security sector acknowledged the fact that many problems hamper progress, with both parties experiencing several conditions that constrained them in achieving their objectives to prevent cable theft.

Some of these conditions included the unilateral decisions taken by Eskom's security department towards the private security companies, the appointment of security companies that are not based in the region where the security service is required, and the unreasonable demands made on private security companies that do not form part of their security contract obligations.

The researcher can better appreciate the above position of both parties because, generally, throughout the stages of this research, the researcher found that many of the Eskom contracts were misaligned and varied significantly from each other.

Many of the Eskom non-security personnel participants participating in the study argued that the security structures of Eskom do not offer them, as non-security specialists, a platform to push their agendas and resolve their pressing challenges of substandard investigations and security measures. Eskom was described as an established organisation which spends millions of rands to protect its assets, but does not understand why these millions are not yielding positive results. The participants revealed that some of Eskom's security personnel lack the necessary resources and skills to use the security structure platforms so as to influence changes in the security environment.

7.4.3 Security assessments for Eskom facilities must be improved through further training, education, monitoring and accountability

The security assessments that Eskom security personnel undertake need to have linkages to their training and development for them to fully understand why it is that these assessments are being done, and in turn contribute to determining the risk profile of an Eskom facility. In contrast with the belief of many of the participants that it is the private security contractors that are not preventing cable theft, the findings of this study point to the fact that security assessments are being done by experienced Eskom security personnel, but with limited experience on how to actually conduct a proper security risk assessment (see subsection 6.6.3). A thorough threat assessment, if comprehensive and accurate, will lead to the implementation of effective security risk control measures (Fischer *et al*., 2008: 149).

For instance, Participant 5 who participated in the study discussed the security assessments and concluded:

"*… The problem with Eskom management is that they want things to be done professionally but they introduce new ways of doing things without giving us training. I saw a new TRA document but I don't know how it needs to put into practice ….*" (Interview 5).

Generally, throughout the stages of this research, the researcher discovered a lack of proper housekeeping practices at Eskom facilities and feels that security assessments must do more than just identify the face value risks, they must also advise Eskom management to lock up assets and materials that are not in use (see subsection 6.5.5).

In keeping within the context of increased measures needed to prevent cable theft, Eskom security personnel must improve their learning and research capabilities in order to access and utilise relevant and innovative technology to achieve success with combatting cable theft (see subsection 6.6.6).

7.4.4 Management needs to improve its awareness culture among employees on the issue of cable theft

As highlighted in Chapter Six (see subsection 6.6.1), most participants were convinced that if improvements were made to Eskom awareness programmes, it would create a basis to highlight the problem of cable theft.

For instance, participant 9 who participated in the study discussed the security awareness and concluded that:

"... If cable theft is such a huge problem in Eskom then why don't Eskom make the employees aware of where these problems happen and request its employees to also participate in cable theft prevention methods. It could very well be that some of our own family members are involved and we can maybe encourage them to stop stealing Eskom cables because it will affect our jobs if the company continues to lose money ...." (Interview 9).

Generally, it is the absence of measures for creating awareness on cable theft in Eskom which gives rise to why Eskom employees say they have limited or no information on cable theft. Following the lack of or limited information, it is important to note that the Eskom security division is well placed to send out regular communications to employees, highlighting to them the losses experienced by Eskom through cable theft. This information can help them to educate people and create a culture of reporting cable theft crimes in their respective communities.

7.4.5 Eskom security personnel must report crime incidents accurately and diligently on the CURA system

As highlighted in Chapter Six (see subsection 6.6.1), most participants were convinced that Eskom security personnel need to report crime incidents accurately and diligently on the CURA system. Accurate and diligent reporting guarantees that Eskom's top management is kept fully aware of what the actual losses to Eskom are. This information enables management to engage security in open and trusted ways.

In fact, Eskom would then have a better opportunity of knowing the extent of its actual losses when it reports its financial year end results. Accordingly, the information recorded and reported must guide and advise multiple sections and employees within Eskom to transparently and fairly protect each one's meaningful interests and obligations as Eskom employees.

In contrast, however, most people reading these reports experience a lack of, or limited, transaction in their dealings with fellow employees in Eskom. This results in no action being taken or in objections being raised towards these inaccurate reports.

Generally, throughout the stages of this research, the researcher was surprised to discover how much depth the recorded information lacked, for example as to the exact location of where the crimes took place, whether these incidents were repeated, the suspect's details and descriptions, the security company guarding the facility, the presence of armed or unarmed guards, the modus operandi, and so forth. It is fair to say that this an opportunity missed by Eskom management to successfully prevent cable theft.

In conclusion to this section, the researcher notes that it is the absence of an 'information culture' in Eskom which suggests where the actual problems lie in not preventing cable theft. Following the lack of, or limited information, it is important to note that the Eskom security division would be enabled to function effectively if management were to send out a strong message that it would sanction those that fail to report accurately and diligently on cable theft. Eskom management must not be deprived of opportunities to effect positive changes and improve on the cable theft situation.

7.4.6 Cable theft experts are needed to testify in court if criminals are to receive lengthy jail terms

Given the overall objective of this study, and in line with finding solutions to prevent cable theft at Eskom, it was reasonable for the researcher to engage the participants in a critical manner to understand why cable theft cases are not prosecuted successfully and criminals are not receiving lengthy jail terms to deter them from continuing to steal Eskom cables (see subsection 6.6.4).

Likewise, the participants from Eskom security and the private security sector acknowledged the fact that many relationship problems exist between the Eskom investigators, police investigators and the prosecutors. The perception that prosecutors are not trained to understand Eskom's crime situation and losses through cable theft is true. It is the responsibility of Eskom management to make sure that our courts and prosecutors know and fully understand the extent of the losses that Eskom suffers. This is possible to achieve if Eskom security personnel were to forge closer working relationships with the police investigators and prosecutors.

Generally, it is important for the courts to know and understand the direct and indirect losses attributable to cable theft; how it impacts on the country, how essential services, and which essential services, are impacted upon; how cable theft negatively affects the financial status

of Eskom; what the current financial problems are that Eskom is experiencing due to the lack of funds; and so forth.

7.5 WHAT MUST ESKOM'S INTERNAL SECURITY MANAGEMENT TEAM DEMAND FROM ITS IN-HOUSE SECURITY OFFICIALS

It is vital that Eskom's management team must expect from all Eskom's in-house security personnel will take the prevention of copper theft very seriously and move to prevent it with everything that they have.

The transformation for security should begin with a clear starting point, which the researcher believes should be the demands from Eskom internal security management team on its in-house security officials' approach to prevent cable theft. Security management, and the oversight functions towards the private security personnel, are the responsibility of the Eskom in-house officials.

Because of the limited freedom permitted to them, and the lack of management support for utilising their available skills to their advantage, the in-house security officials remain marginalised in most security departments within Eskom. They are left out of most decision-making processes, and continue to experience limited freedom to make decisions and keep the private security personnel on their toes.

Specific security management functional issues need to be understood within their own contexts. A better understanding of security management functional issues will dispel confusion and misunderstanding concerning the security division's existing functional processes. A discussion of the different management-related functions will help foster an understanding of the operational competency areas of the security environment within Eskom.

In general, within the context of this shared responsibility for improving private security protection capabilities, the fact that most in-house security officials fail to prevent copper theft is attributable to the lack of support and transparency by security managers.

Many of the participants reported that the constraints facing most in-house security officials have a negative influence on their personal status, as they increasingly experience low self-esteem when they execute their duties, and because of this, fail to negotiate confidently with

the private security companies towards getting the companies to perform efficiently to prevent copper theft from taking place.

Eskom internal management must make the in-house security officials aware of specific activities of the operations and how private security companies should be managed and what is required from them to prevent copper theft. The basic contractual demands will only be achieved if Eskom in-house security officials manage the security companies in a structured manner.

The Eskom internal management team must demand the following from its in-house security officials:

7.5.1 Proposed security management structured plan for supervising and managing private security contracts

In this subsection, the researcher sought to analyse and systematise the evidence from the study participants to establish why the security departments in Eskom cannot manage the private security resources in an effective manner so that they prevent cable theft. A thorough scrutiny of the evidence uncovered an understanding of some of the problems, which was instrumental in assessing whether or not a structured plan exists between the security manager and the in-house officials on how to manage the private security resources allocated to prevent copper theft.

Many of the participants underlined the fact that the problems they experience were linked directly to the lack of proper consultation by, and guidance from, the security managers, which resulted in them being constrained from performing their functions efficiently. Many of them felt that a proper plan of action with sufficient management support, if it were to be put in place, would encourage them to plan properly manage the security companies effectively so they can stop copper thefts from happening.

The researcher believes that the oversight security management plan must become part of the day-to-day operations of the in-house security officials. If the internal management teams wish to ensure that security companies are being managed effectively and regularly so they can prevent cable theft, then they have to change their operational plan to integrate the oversight security management plan and keep up with current security management developments.

7.5.2 Private security companies must deploy competent and reliable personnel to Eskom facilities

As highlighted previously (see subsection 7.5.1), Eskom's in-house security officials experience limited freedom, constraining conditions, and are being deprived of management support, partly because the Eskom security managers who are expected to support them and work in cohesion to manage this important transaction are, whether by default or lack of skills, failing to redress those diverse constraints and deprivation. The private security companies are then left to do their own planning because they in turn take advantage of these disjointed relationship problems and deploy incompetent and unreliable security officials to Eskom facilities.

For instance, some of the participants who participated in the study discussed the non-deployment of competent security personnel and concluded:

"... The lack of professional management skills and oversight management is the reason why security companies do their thing at Eskom ...." (Participant 20, interview 20).

"... The Eskom security inspectors are not given adequate support from their superiors ...." (Participant 13, interview 13).

From the above information, it becomes clear that it is essential that private security managers and Eskom in-house security officials should understand the concept of competence in order for them to have a clear picture of what they manage and how Eskom can benefit from competent private security personnel. Finally, the Eskom internal management team must demand an exemplary and professional service from its in-house security officials and the private security contracted officials.

7.5.3 In-house security officials must encourage line management to report non-performance issues of private security companies and employees

The daily oversight security management function is the responsibility of line management. Given their lack of expertise in private security management matters, it would make sense for them to seek intervention from Eskom security immediately when they experience non-performance and non-compliance by private security personnel.

If these experienced Eskom line managers cannot help in redressing the security compliance challenges on a daily basis, *who else could?* It is therefore important that in-house security officials encourage line management to immediately report these non-performance issues to them.

7.6 WHAT MUST ESKOM'S IN-HOUSE SECURITY OFFICIALS DEMAND FROM PRIVATE SECURITY COMPANIES TO PREVENT CABLE THEFT FROM ESKOM

Private security companies, while having relevant competence and resources, have not been doing much to improve or reduce the losses experienced by Eskom through cable theft. The conditions in the current situation make it profitable for them to contract to Eskom, but unprofitable for Eskom since Eskom suffers financially. With regard to the private security companies contributing to improving the situation at Eskom facilities in terms of cable theft, prevention has mostly remained indifferent.

Generally, throughout the stages of this research, the researcher found that one of the biggest differences between good quality security services and substandard quality security services is the extent of authority and accountability that Eskom in-house security officials have, and must take, to make efficient operational changes to the current methods of operating.

Eskom security divisions have many in-house security officials to provide oversight for achieving the required outcomes and managing the complexity and risks of Eskom facilities. This is one of the reasons why the role of the in-house security officials has emerged strongly in the study as a critical competency which is necessary in Eskom's security divisions.

This is also why the in-house officials themselves need to start focusing less on what makes them different from other Eskom employees, and more on recognising that there is a common and consistent core of activities that underlie their role and professionalism within the divisions.

To remedy the finding of this study that security guards are not adequately trained to protect Eskom facilities and identify Eskom's cable (see subsection 5.8.1), Eskom in-house security officials must demand the following improvements from the private security companies for security guards, which are set out in Table 7-1.

Table 7-1: Improvements required from the private security companies for security guards

Improvements	**Cf.**	**Study findings for those participants (out of 55) that agree**
Security guards must be adequately skilled and trained to protect Eskom facilities and identify Eskom's cables (and other assets)	5.8.1	50 (90.91 %)
Security guards must be trained to improve their observation and reporting skills	5.8.2	34 (61.82 %)
Security officers must not have their mobile phones in their possession while they are on duty	5.8.3	49 (89.09 %)
Guards must be more alert and awake during the night shift and especially during the high crime times at Eskom facilities (which are between 01h00 to 03h30)	5.8.4	49 (89.09 %)
Security patrols must be conducted consistently during the shifts (especially at night)	5.8.5	36 (64.45 %)
Increased support mechanisms must be put in place by top management for security officers to feel safe and committed in their jobs	5.8.6	43 (78.18 %)
Vetting must be done consistently prior to the deployment of security guards	5.8.6	29 (52.73 %)

To remedy the finding of this study as to why the supervisors cannot prevent cable theft at Eskom (see section 5.10), the Eskom in-house security officials must demand the following improvements from the private security companies for supervisors, which are set out in Table 7-2.

Table 7-2: Improvements required from the private security companies for supervisors

Improvements	**Cf.**	**Study findings for those participants (out of 55) that agree**
Supervisors must receive training and be developed to Eskom's security requirements	5.10.1	49 (89.09 %)

Relationships between security guards must improve	5.10.2	36 (65.45 %)
Vetting must be done consistently before supervisors are deployed	5.10.3	34 (61.82 %)
Supervisors should not be lead investigators, but rather first line investigators or assistants to the investigations	5.10.4	49 (89.09)
Proper support structures must be in place for supervisors to feel safe and committed to their jobs	5.10.5	33 (60 %)
Supervisors must improve their ability to create a significant impact on the security officers	5.10.6	34 (61.82 %)

To remedy various findings of the study, which are discussed in Chapter Five, Eskom in-house security officials must demand the following improvements from the private security companies for managers and the overall private security management team, which are set out in Table 7-3.

Table 7-3: Improvements required from the private security companies for managers and the overall private security management team

Improvements	**Cf.**	**Study findings for those participants (out of 55) that agree**
The commitment from security managers and company directors/owners must be given consistently during the contract period.	5.12.1	39 (70.91 %)
All security managers and company owners/directors should be vetted before contracting to Eskom	5.12.2	29 (52.73 %)
Security managers must be well supported, resourced and motivated by company owners/directors.	5.12.4	36 (65.45 %)
Security managers must provide clear, honest and definitive leadership	5.12.5	47 (85.45 %)
Security managers must be innovative thinkers	5.12.6	29 (52.73 %)
Company directors/owners must provide adequate resources to a security manager to avoid him/her becoming distracted from doing other functions	5.12.6	49 (89.09 %)

7.7 PROPOSED: ESKOM SECURITY STRUCTURE

The way in which the Eskom security structure connects its control systems, management systems and employees will have an impact on its ability to operate efficiently and effectively. The researcher believes that the security structure will be a determining factor between success and failure in preventing cable theft (see section 6.4.1).

Two main facts about the security structure constantly emerged during the interviews and discussions with participants participating in it. The first fact revealed the actual and potential contributions of the people, including managers, in the current structure. The second fact underscored various crises and failures currently prevalent that threaten Eskom's potential for reducing cable theft.

Regarding the former, for instance, while assessing the levels of management thus far attained in the structure, most participants were confident that, when conducted well, a smaller and more streamlined structure would have the potential to contribute significantly to the prevention of cable theft. In particular, during the group interviews, some participants underlined the fact that when there is a long process for making decisions and obtaining approvals, all other crime combatting activities also fail. Consequently, they argued that security at Eskom could not afford to continue with these long processes and so allow cable theft problems and losses to increase, as this would lead to the collapse of Eskom's core business, which is to 'keep the lights on'.

Generally, throughout the stages of discussions and interviews for this research, most participants viewed Eskom top managers in the security sections as being potential key players in prompting and enabling Eskom's security to unleash its abundant and true potential, if the structures could be more interactive. In some cases, these participants described some of the top managers as knowledgeable, committed and hardworking persons who value, and have chosen to maintain and sustain, Eskom's security mandate.

Indeed, some of the participants reported that they enjoyed having good relations with Eskom top management, and had spent time interacting on various projects with some of them. Some of them conceded that these interactions and related work projects had prompted them to think and act differently when approaching security projects or tasks.

At the same time, most participants highlighted several challenges that have hindered the high performance and productivity of top management, and urged the redress of these

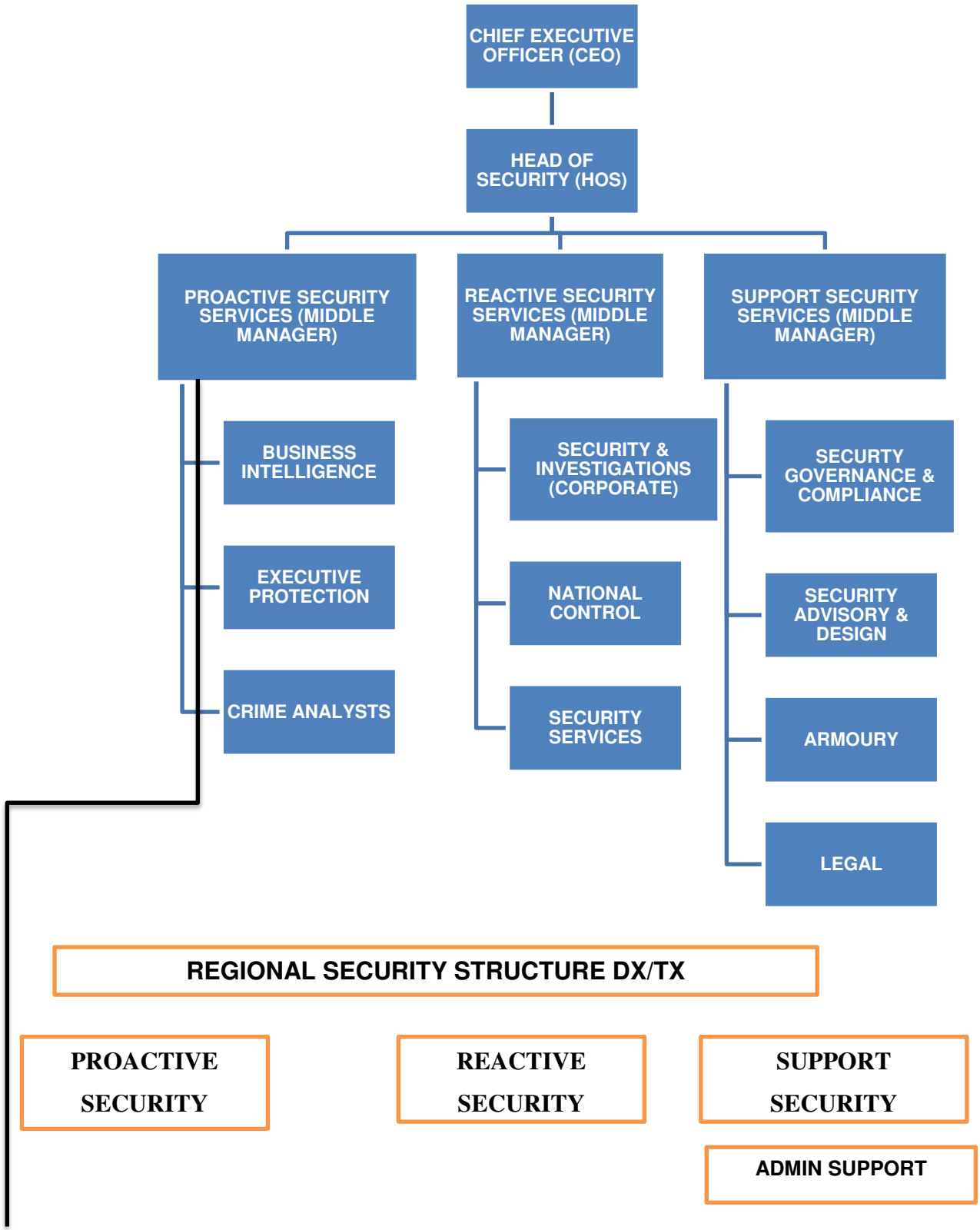
problems. With regard to the second fact mentioned above, most participants identified the crisis at top management, as well as the structural failures, and then argued that these crises and failures threaten the sustainable reaping of benefits from its in-house security teams. Regarding the crisis in management, these participants noted, on the one hand, the decline of regular interaction, updates and social dialogues that should make them feel part of the security structure.

In particular, the participants in the group interviews expressed concern following the increasing trend over the years to have a top-heavy management structure that is very costly, but also ineffective in many areas. The participants say this is sometimes characterised by slow decision making because accountabilities are often confused and it is unclear where the decisions needed to be taken.

They contended that the situation is further exacerbated by excessive controls in the system that stifles accountability. As a result, participants felt disengaged and were constrained in their work environments.

A proposed security structure model prepared by the researcher is schematically presented Figure 7.1 below, and is explained in section 7.8. Ras (2015) recommended that the main divisions under the head of security must be: Proactive, Reactive and Support Services.

NATIONAL SECURITY STRUCTURE



REGIONAL STRUCTURE DX/TX

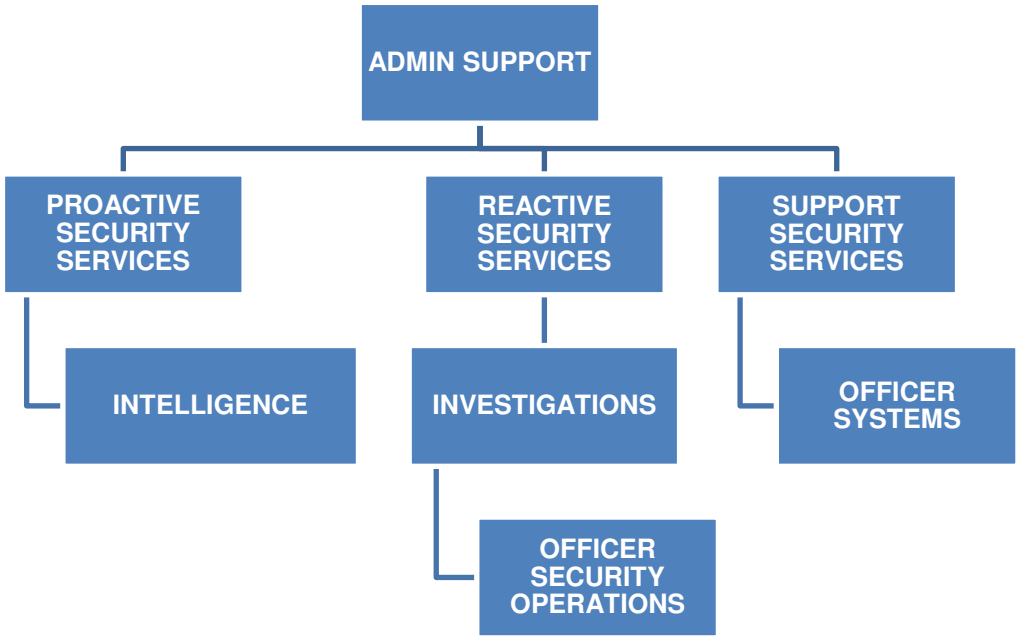


Figure 7.1: Proposed security structure model

7.8 EXPLANATION OF THE PROPOSED SECURITY STRUCTURE MODEL

The substantive grounded theory on the security structures that currently exist within Eskom, which is reflected in the study (see sections 5.4, 5.5 and 6.3), together with the findings of the study (see subsection 6.4.1), was used to develop the model in set out in Figure 7.1 above. This model was discussed with many industry security experts (Ras, 2015; Meek, 2014; Moodley, 2014; Moonsamy, 2015).

The discussions at the group interviews, for instance, resulted in an agreement that a more compact structure would have the potential to contribute to a more efficient reporting method, which would ultimately lead to the prevention of cable theft and ensure the sustainability of Eskom.

Specifically, some participants argued that oversized structures typically provide ground-level security employees with limited support and resources. Many of the participants were

strongly in favour of this proposed model (see section 7.7) for enhancing the security reporting structures and making the structure financially viable to Eskom.

The researcher adopted the "*Govender Approach*" (as described below) to examine the management levels within the security environment by identifying opportunities to improvement the structure. The new structure will consolidate functional activities; clarify lines of accountability; remove layers of management; and improve the spans of control. Ras (2015b) says that one highly qualified person, with support, can do more than those in ten highly paid managerial functions.

According to Phasiwe (2015), Eskom is currently in huge financial crises (http://www.citypress.co.za/business/blackouts-partly-blame-eskoms-financial-woes/).
Eskom requires increased financial resources to meet emerging challenges, and by minimising duplication of manpower and increasing coordination, Eskom can become financially stronger. Streamlining Eskom security structures is the next great frontier for reducing costs, enhancing quality, and building sustainable relationships with stakeholders.

The "*Govender Approach*" structure (see section 7.5) consists of a three-division approach – Proactive, Reactive and Support Security Services. While Ras (2015b) has mentioned these three (3) divisions to the researcher, the author has worked out this approach in more detail.

Proactive Security Services Structure is intelligence driven and the person undertaking this function will also be a second-in-command (2IC) to the Head of Security (HOS). This structure must provide assistance and information to help prepare, protect, and secure Eskom in anticipation of security attacks, problems, or events. The performance of this structure will directly reduce the number of incidents and threats to Eskom.

Reactive Security Services Structure will always be subject to the Proactive Security Services Structure and these services are normally triggered by an event or request, such as a report of a compromised breach in security, or something that was identified or triggered by an incident. Reactive services are the core component function of armed investigators and reactive security officers.

Support Security Services Structure will be subject to the Reactive Security Services structure. These services augment existing and well-established security structures that are independent of incident handling and threat identification and are traditionally performed by other areas in the structure, for example firearms management is carried out by a person

designated as the firearm officer for Eskom firearms. These services will generally be proactive, but will contribute indirectly to reducing the number of crime incidents at Eskom.

Intervention teams have not been identified in the organogram for the new structure because the researcher is of the view that the need for these teams should be on an 'as and when' required basis, and therefore should be built into private security contracts, but managed strictly with specifications of the scope of work outlined from the outset of the contract.

The regional Proactive, Reactive and Support Security Services structure will report direct to the national structure following an integrated response with strict security clearance to ensure confidentiality.

7.8.1 Implementation of the proposed security structure

Eskom top management should create a single, centralised regional security structure for both its Transmission and Distribution operating units that will consolidate and coordinate various aspects of the regional business units' security requirements and decision-making, such as effective negotiation of security demands, and coordinating action and the integration of a wide range of security-related policy, legislative, structural and oversight issues.

With regard to the asset owner's function in the region, it must remain relevant. Given the aforementioned, it will be up to the Head of Security (HOS) to determine the vision for security in Eskom, to refine skills in communication and analysis, and to undertake the disciplined approach required for effective executive leadership during this time of change.

One of the foundational steps in the strategy process will be the need to establish a comprehensive planning framework for security; one that defines a master set of core security capabilities and organises them in such a way that the new structure is aligning security as one body, nationally and regionally, with the direct reporting line displayed in Figure 7.1 above.

In general, all security guardians in the region must always be accountable to the asset owner, but the mandate for security processes and policies should come from the direct line reporting displayed in Figure 7.1. The asset owner's security budgets must be redirected to the Head of Security at national level for allocation and management.

Finally, Eskom's business objectives form the single most important driver of any cost saving exercises to be introduced. This forms the basis of many discussions utilised in

communicating the business cases for change, which will help prioritise initiatives based on Eskom's business needs, with the most important one being optimisation and cost saving, and the second being the risk of having so many people on the road doing the same job in the same area. The security strategy planning process must be explicitly mapped to the business objectives, which must be used to measure the integration success of the newly proposed security structure (see subsection 7.5.1).

7.9 NEWLY DESIGNED ESKOM TRAINING CURRICULUM FOR ALL PRIVATE SECURITY CONTRACTS AT THE ESKOM FACILITIES

On the 24 June 2016, the then Minister of Police, Nkosinathi Phiwayinkosi Thamsanqa Nhleko and PSIRA released new regulations in terms of Section 35 of the Private Security Industry Regulation Act, 2001 (Act 56 of 2001) regarding the minimum training standards, for security service providers in the private security industry (http://www.psira.co.za/psira/dmdocuments/circular/Published%20Training%20Draft%20Regulations.24%20June%202016.pdf)

Most participants argued that, with limited competency and training opportunities to enhance the private security guards, Eskom has experienced challenges to their effectiveness in preventing cable theft and other crimes. Indeed, most of the Eskom participants accepted responsibility for partly failing to provide the private security companies with a minimum entry requirement based on Eskom security standards (see subsection 5.14.2). The proposed training curriculum would create opportunities for private security guards and supervisors to enhance their knowledge and skills, thus rendering them more determined and more engaged in facilitating the acquisition of the relevant Eskom competences for improving their participation in the prevention of cable thefts from Eskom.

In general, if Eskom wishes to receive a high standard and quality security service from its contracted security companies, then the Eskom security division, in conjunction with the Eskom Academy of Learning (EAL), must develop a standard entry training curriculum for private security employees to qualify and approve them to work at the Eskom facilities.

In line with the aforementioned, participants regrettably conceded their failure, as one of them elaborated:

"… *We cannot expect the security guards to perform efficiently if we have not trained them to our specific requirements* …." (Participant 17, interview 17).

Another participant also shared the above regret and elaborated:

"… *These are security guards, what do we expect from them if they are poorly trained. We cannot blame them if we suffer losses; they have not been taught the basic skills of what Eskom needs. I don't even think they stay awake at night to observe the criminals, I don't even think they know how to be observant* …." (Participant 12, interview 12).

Some of the participants recommended that the Eskom Academy of Learning (EAL) and PSIRA accredited training centres would be knowledgeable, interested and capable of initiating the training curriculum programme to train the private security guards on Eskom's requirements.

One participant mentioned:

"… *EAL is a learning facility that is equipped to train security guards or they can allow the accredited and appointed trainers free space to train* …." (Participant 9, interview 9)

Another participant made a suggestion, saying:

"*Through SASSETA, the Sector Education and Training Authority in South Africa, Eskom can request to have the training programmes accredited to meet an articulated Government theoretical and practical standard that, in turn, will be linked to the larger South African National Qualifications Framework."* (Participant 2, interview 2).

The researcher recommends that the requirement linked to the delivery of the training must be the subjected to the examination or testing of the learning acquired by the learner (security guard).

It is important for the Eskom Academy of Learning to take into account the following compulsory standards to make the training effective (see subsection 7.7.1):

- First is the content of the basic training curriculum
- The mandatory number of hours of training per security person
- Refresher training

- Testing methods
- Specialist training for supervisors and managers
- Specialist training for specialised security services required (armed response, escorting)
- Additional managerial training for invoicing, communication, etc.

7.9.1 Course Content for the Standard Entry Training Curriculum to Qualify and Approve Security Personal Working to Work at the Eskom Facility

The researcher, on the advice of Ras (2015), has designed a basic course for the standard entry training for security personnel at Eskom. This section (section 7.9.1) endeavours to make an important contribution to the existing standards for directly assisting in preventing copper theft.

The following course content for the standard entry training curriculum for security personal working at an Eskom facility comprises a thirty-eight (38) hour programme and is divided into classroom and practical exercises. This programme is necessary and very much needed to improve the level and quality of security services at Eskom.

Unit standard 1, Induction to Eskom's operations: This session must introduce the learner to Eskom's purpose, values and strategic objectives.

(1 hour classroom)

Unit standard 2, Security officers' duties and responsibilities at Eskom: Security officers must understand their responsibilities at an Eskom facility. This session provides an overview of the principal duties and responsibilities involved in the security requirements, specifically dealing with Eskom requirements, namely managing security risks (potential cable theft), risk reduction, investigating any breaches of security, and collecting information/intelligence relating to the protection of Eskom assets, property and people, as well as evidence of breaches in the provision of security (perpetration of a crime against Eskom). This session must cover the policies and procedures of Eskom and, more importantly, the safety aspects concerning Eskom.

(3 hours classroom, 1 hour on site practical)

Unit standard 3, Eskom's Legal requirements (Legal status of a security officer; types of criminal offences; powers of arrest; use of force (minimum and restraining force techniques); search and seizure; trespassing and vandalism): This session reviews the sources and extent of authorities, and the legal confines within which they operate, and which may be exercised while deployed to the Eskom facility. This session must also discuss the potential legal consequences of wrongful exercise of laws, such as the Criminal Procedure Act, Firearm Control Act, Trespass Act, PSIRA Act, National Key Point Act (if deployed to a NKP site), etc. Firearms training will be covered in the mandatory Regulation 21 training, although the training programme can discuss issues related to the basic handling of firearms and extracts of the important and pertinent information on the Firearm Control Act, and the consequences of failing to abide by legislation and training.

(3 hours classroom, 1 hour practical)

Unit standard 4, Eskom's electronic and physical systems: This session provides the security officers with a basic understanding of the principles of the functioning of Eskom's electronic and physical systems, the use of the panic buttons, the safekeeping of the panic buttons, mobile radio and telephone communication, what to expect from the armed response unit during emergencies, what the dangers are with the electric fencing, why it is important to test the panic units, and how to report alarm tests and activations to the Eskom control room. It is crucially important for the security officers to understand Eskom's access/egress controls and measures involving the support of security elements, such as electronic systems and physical barriers (booms).

(2 hours classroom, 2 hours on site practical)

Unit standard 5, Eskom's access and egress control systems: The security officers must understand why it is essential to control movement of personnel and material into, out of, and within an Eskom facility (movement that is essential for normal operations) and why they need to prevent unauthorised access and egress.

(3 hours classroom, 1 hour on site practical)

Unit standard 6, Security writing, observation and crime scene skills: This session will assist the security officers to write reports, describe factors involved in note taking, what to include in notes, observing and recording suspicious activity, presenting facts about the

incident, and (where required) how to conduct themselves appropriately in court or at internal disciplinary hearings

(3 hours classroom, 2 hours on site practical)

Unit standard 7, Reaction to Eskom's emergencies (fire; break-ins): Security officers are expected to react in a tactical and safe manner to unexpected intruders and criminals to an Eskom facility. They need to ensure that they can either apprehend the criminals, or take evasive action and request back-up and monitor the situation in a safe manner. Security officers may be required to protect a scene after the intruders have left, so they should therefore understand the importance of crime scene management.

This session must stress Eskom's safety processes and the security officer's responsibilities in relation to those processes. The security officer must also be instructed in the correct and safe methods of searching, identifying and securing the area where the criminals could possibly be hiding. It is essential that security officers should understand the respective roles of private security personnel and the police, as well as the general principles governing their relations. Emergency procedures for all emergencies (incorporating the Eskom Emergency Preparedness Plan) must be covered in this session.

(4 hours classroom, 1 hour on site practical)

Unit standard 8, Guard patrol duties at Eskom: Purpose of a patrol, preparing for a patrol, patrolling effectively, patrolling safely, powers of observation.

(2 hours classroom, 1 hour on site practical)

Unit standard 9, Identification of Eskom cables and other assets: This session must introduce the different types of cables and material found at Eskom facilities. Samples of cables must be shown to the security officers and a discussion of the various different types of cables must be demonstrated. A catalogue of large assets that cannot be shown to the officers must be issued to them during training, and a practical exercise must be conducted with them to familiarise themselves with these Eskom assets. Catalogues must be given to them as part of their equipment issued to the site.

(3 hours classroom, 2 hours on site practical)

Unit standard 10, Physical exercise, fitness and self-defence skills: This session must introduce and test the level of physical fitness. Ras (2015) recommends 8 pull ups, 40 push ups, 60 sit ups and a 2.4 km (under 12 minutes) run. The idea is to get members fit. This session must teach the candidate about the importance of physical fitness for health and performance while working at an Eskom facility. The self-defence session must emphasise how to defend, not how to fight.

The session must begin with candidates learning about potentially unsafe situations and how to identify and avoid them. Safety skills, using observation, intuition and communication, must be the initial focus of this session. Appropriate training for security staff is vital in order to raise the standards of the private security sector and to enable Eskom to receive a higher quality of security services. This fitness for duty programme must be designed by Group Security of Eskom and managed by the in-house security officials in the regions.

(2 hours classroom, 2 hour on site practical).

Finally, upon completion of this programme, the learner must achieve an average score of 80 % to qualify and receive an accredited competence certificate, which should be valid for a period of 24 months. The learner must, however, complete a refresher programme after a 12-month period (date to be indicated on the certificate) for the certificate to remain valid for 24 months.

7.10 IMPROVEMENTS FOR THE CURA SYSTEM

In general, the CURA system was introduced to report Eskom crime incidents. It was introduced for the first time into Eskom in 2010 and from that time, until now in 2017 (7 years elapsed), there have been no improvements made to this system. This study endeavours, inter alia, to rectify and develop it in a more efficient manner so as to better plot cable thefts and prevent this crime.

The data from this system is used by Eskom security analysts to formulate the monthly crime reports for Eskom (see sections 1.5 & 6.8). The problem that Eskom is faced with is that the data reported in the system may not fully accord with the current system applied, and therefore may not provide an accurate picture of the extent of cable theft.

The study found (see section 6.6) that the current cable theft information is limited to the particulars of information collected by the security officials in the regions, and to the level

and accuracy of details recorded on the CURA systems. The study found that despite such obvious shortcomings, it is this data that forms part of the data available to produce the monthly (ENECC) and annual national crime statistics at Eskom (see section 1.4).

It is, therefore, true that top management cannot plan operations and direct resources if the information is not sufficiently specific. It is also true that top management needs to ascertain whether certain security companies are not proactively preventing cable theft and why Eskom facilities experience repeated incidents.

The other problem discovered which leads to Eskom experiencing inaccurate reporting of statistics is the lack of training provided to the people recording information on Eskom's CURA system (see section 6.6).

These participants noted that, with the CURA system, the cable theft data must be used for comparative purposes and to track trends of the cable theft incidence in certain areas of the business, and also for notifying management whether security companies are preventing or promoting cable theft in Eskom.

They underscored the point that specific crimes related cable theft at Eskom need to be understood within their own socio-cultural context. An understanding of the issues related to cable theft will avoid confusion and misunderstanding arising among the analysts that convert and transfer the information found on the CURA system to the ENECC report.

One participant said:

"... if the system was able to provide more options to the investigators recording crime incidents, analysts would stop calling them for further information on the cases that have been already reported on CURA. Cable theft incidents data is useful for compiling crime statistics because it represents an official record of crime occurring in Eskom ...." (Participant 6, interview 6).

Another participant said:

"... if management would make provision for all investigators using the CURA system to go on formal training, then they would understand the system better and would be able to operate it more efficiently ...."(Participant 4, interview 4).

7.10.1 NEW INFORMATION TEXT BOXES FOR CURA

In line with the aforesaid issue (see section 7.10), there is a need to include the following information text boxes for CURA:

- Where the cables are stolen from? (Guarded or unguarded premises, open network sites or project sites)
- The number of guards deployed to the site
- Indicate whether or not they were/are armed
- The name of security company providing the security service to that site
- Indicate whether this is a repeated theft and over what period of time
- Who detected the break-in? (Security guards, day or night shift; Eskom employees; or Eskom contractors)

It is important to note that the extent of cable theft from Eskom will never be completely measured if all cases are not reported accurately. Only cable theft incidents that have been reported can be measured. It is, therefore, true to conclude that understanding how the extent of cable theft is measured will help Eskom's security in future to estimate the costs of cable theft and it will also assist in the evaluation of crime prevention programmes.

Further emphasis needs to be placed on the ongoing professional employee development of the individuals working on the CURA system. To deal with this need, it is important to institute high quality refresher training programmes, which will equip those who conduct and run the CURA training courses with appropriate security-related skills, such as computer and management skills. This will ensure the suitability and the effective use of the CURA system. The manager's responsibility is to manage the training function in such a way that the people using the system are competent and comfortable when reporting cases on the CURA system.

Finally, a detailed, accurate and a more descriptive reporting system will help Eskom security analysts and management to understand the operational competency areas within the security environment.

7.11 IMPROVEMENTS TO THE ENECC REPORT

The ENECC report was discussed in great detail in Chapter Six (see section 6.7).

In this section, the researcher recommends various details that need to be included in the ENECC report:

7.11.1 Whether these losses (cable theft) occurred on Eskom's open network, guarded premises, or unguarded premises. This information must be structured to include a national figure and then specified for the business units in each of Eskom's nine regions.

7.11.2 What was the reason for the increase or decrease in crime for cable theft?

7.11.3 If any arrests led to convictions.

7.11.4 Whether Eskom had any control over the losses that it experienced through cable theft

7.11.5 The summary of the performance of the private security contractors should not be limited to the two private security companies contracted to investigate cable theft crimes mentioned in the current report, but it should extend to all the private security companies contracted to Eskom.

7.11.6 A table should be included, indicating Eskom's national cable theft hot spot areas.

From a survey of the above recommended changes, it will be seen that these changes are concerned with the reasons for the increase or decrease in cable theft, and the fate of those security companies that fail to protect Eskom's assets. These changes will further help management to quantify the losses and wasteful expenditure it has incurred in employing security companies that fail to protect its cables. It follows that, with this attitude of care and concern for the cable theft problem at Eskom, this would further help top management to comfortably engage in enhancing the capability of the security departments and private security companies.

A further scanning of the number of convictions highlighted in the ENECC report will demonstrate the effectiveness of the judicial system in cable theft matters. It will further evaluate the performance and the effectiveness of the Eskom investigators and private security companies regarding court matters relating to cable theft.

7.12 SUMMARY

In this chapter, the researcher discussed the duties of the legal experts (see section 7.2) and the law enforcement agencies in the fight against cable theft (see section 7.3). Discussions were set out around what must be done by the Eskom's internal security management team and those responsible for the capturing of all relevant information related to cable theft in order to prevent it (see section 7.4). This chapter provided action steps that must be taken by the Eskom's internal security management team and set out what they need to demand from in-house security personnel (see section 7.5).

The chapter also provided actions steps that must be taken by Eskom in-house security personnel and set out what they need to demand from the private security companies to prevent cable theft (see section 7.6). The chapter proposed a new security structure and provided details on how to implement it (see sections 7.7 & 7.8).

In addition, the chapter provided the necessary basic requirement training course content for Eskom to implement and make compulsory in order to approve and qualify all private security officers and supervisors to work at an Eskom facility (see section 7.9).

This chapter discussed the CURA reporting system and the changes required to make it more effective so as to allow users, who are tasked with the duty to record the information, to do so diligently and accurately (see section 7.10). Recommendations were provided for extending the current information boxes in the CURA reporting system (see section 7.10.1).

Finally, the chapter discussed the ENECC Report and the changes required to ensure that it prevents cable theft and does not exacerbate it (see section 7.11) and provided a summary to conclude the chapter (see section 7.12).

The next chapter discusses the findings, conclusion and recommendations of the study.

CHAPTER EIGHT
FINDINGS, CONCLUSIONS AND RECOMMENDATIONS

8.1 INTRODUCTION

The general aim of this thesis was to investigate why Eskom's copper cables are not well protected and why all Eskom's security seems unable to stop copper theft it. It also wants to determine what action steps must be taken to ensure that no cable theft occurs. The purpose of this chapter is to present a summary of the findings and conclusions, and to make recommendations in the light of what has been discussed in the previous chapters. This is in line with research aim 1.8.8 set out in Chapter One (under the heading "Research Aims").

While Chapter One of this research was a general orientation to this study, Chapter Two has focused on the research methodology, Chapter Three on the extent of cable theft at Eskom, Chapter Four on Eskom's in-house security, Chapter Five on private security in Eskom, Chapter Six on the Eskom internal security management team and those responsible for the capturing of all relevant information related to cable theft, and Chapter Seven on the actions steps that can be taken to prevent cable theft. Chapter Eight concludes with the findings, conclusions and recommendations.

8.2 GENERAL REMARKS

This summary of the general remarks serves as a synthesis, presenting the key essentials of this thesis as a coherent and logical whole, before embarking on answering the research findings and making several specific recommendations.

This study has focused on the gathering of relevant data to gain an understanding of the extent of the problem of cable theft from Eskom facilities. It has also explored the role of private security, contracted to Eskom to prevent cable theft, on Eskom's in-house security and it has included those responsible for the capturing of all relevant information related to cable theft.

8.3 LIMITATIONS OF THE PRESENT STUDY

Although no serious limitations or problems were encountered during the course of this study, the researcher would like to record the following:

- As already pointed out, not much academic study exists within South Africa and in the international arena on cable theft, despite this being a massive problem which impacts negatively on economies around the world.
- This study has made use of a qualitative research approach, inter alia, to investigate the prevention of copper theft at Eskom.

8.4 FINDINGS

The researcher would like to point out the undermentioned points, when it comes to reporting feedback on the research hypotheses that were formulated.

The hypotheses in this research were (see section 1.7):

First Hypothesis:

A better comprehension of the extent of cable theft at Eskom will assist us in preventing it (see subsection 1.7.1).

Second Hypothesis 2

The present strategies to prevent cable theft are ineffective and need to be revised to prevent it (see subsection 1.7.2).

8.4.1 Feedback on first hypothesis

In terms of the first hypothesis, the researcher can say that the extent of cable theft was discussed comprehensively in Chapter 3. The researcher explained that the value of the copper in Eskom's cable is the main reason why Eskom experiences 95 % more thefts of its copper cables than of its aluminium cables (see section 3.2).

The researcher discussed some of the reasons why cable theft has increased at Eskom (see section 3.3), which were: the high price of copper (see subsection 3.3.1); Eskom's unsecured asset on its open network (see subsection 3.3.2); the difficulty in identifying Eskom copper cables after they have been stolen (see subsection 3.3.3); lack of commitment and dedication by private security officers deployed to Eskom premises (see subsection 3.3.4); lack of adequate security measures at Eskom facilities (see subsection 3.3.5); poor control over stock (cable) movements and unused materials on construction/project sites (see subsection 3.3.6); socio-economic Factors (unemployment and poverty) (see subsection 3.3.7); criminals being

brazen in their attacks on Eskom (see subsection 3.3.8); and the involvement of private security and law enforcement personnel in cable theft (see subsection 3.3.9).

The researcher also provided statistical figures for the financial losses which Eskom has experienced through cable theft (see section 3.4) and further described the hidden costs incurred by Eskom through this cable crime (see section 3.6).

Resonating with the above-mentioned information, and in line with the first hypothesis, Chapter Seven provided action steps to prevent cable theft.

This means that the first hypothesis is accepted (see subsection 1.7.1 for the First Hypothesis).

8.4.2 Feedback on second hypothesis

As set out in subsection 1.7.2, the **second hypothesis** was formulated as:

> The present strategies to prevent cable theft are ineffective and need to be revised to prevent it.

There is no doubt in the researcher's mind that, through this study, he was able to get a telescopic view into the present security strategies that Eskom applies to prevent cable theft. This study was prompted by the increasing number of cable theft incidents from Eskom, while it nevertheless spends millions of rand on security to protect it. Considering the high financial losses for Eskom, and its vast spending on security, the researcher had to design and recommend interventions that would improve the present security measures at Eskom.

Taking the view that Eskom should and must receive a return on its investment in security, and value for the money it spends on security, this study focused on exploring the views of participants who had voluntarily participated in the study. The study also examined measures that were taken, and can be taken, to prevent cable theft.

The study's empirical research component involved a process of progressive stages of critical self-reflection within and between the different participants. During these stages, participants reflected and deliberated on themes and questions regarding security at Eskom: what are the practical reasons why Eskom and private security cannot prevent cable theft; why the cable thefts continue despite security deployment; what is needed by Eskom security and private

security to prevent theft; and what Eskom top management and private security management need to do to prevent cable theft. Chapter Seven provided action steps to prevent cable theft.

This means that second hypothesis is accepted (see subsection 1.7.2 for the Second Hypothesis).

8.5 SUMMARY OF THE FINDINGS

8.5.1 Why do the private security guards not prevent cable theft at Eskom?

In Chapter Five, the researcher described the possible reasons for why private security guards cannot prevent cable theft at Eskom (see subsections 5.8.1–5.8.7): namely, security guards are not adequately trained to protect Eskom facilities and identify Eskom's cables; lack of proper observation and reporting skills; security officers are distracted by their mobile phones while on duty; guards sleep on duty; effective and dependable security patrols are not conducted consistently during the shifts (mainly at night); inadequate protection is provided to security officers for them to feel safe and committed to their jobs; and vetting is not done consistently before deployment to Eskom.

These findings show that private security guards lack the necessary training on Eskom standards and are in dire need of development of their skills, if Eskom is to prevent cable theft. The findings forecast that if private security is not correctly managed, there will be continuous recurrences of cable theft at Eskom.

8.5.2 Why the supervisors of the private security guards cannot prevent cable theft at Eskom?

In Chapter Five, the researcher described the possible reasons for why the supervisors cannot prevent cable theft at Eskom (see subsection 5.10.1–5.10.7): namely, the contract supervisors are ineffective, unprofessional and unreliable; there are relationship problems between supervisors and security guards; vetting is not done consistently before supervisors are deployed to supervise Eskom contracts; supervisors should do first line investigations only; inadequate support structures are provided to supervisors for to remain committed to their jobs; and supervisors lack the ability to create a significant impact on the security officers.

These findings show that the lack of training and the inadequate oversight management practices are a major problem influencing the reasons for why supervisors cannot prevent cable theft.

8.5.3 Why do the managers and company owners/directors not prevent cable theft at Eskom?

In Chapter Five, the researcher described the possible reasons for why the managers and company owners/directors cannot prevent cable theft at Eskom (see subsections 5.12.1–5.12.6): namely, the contractual commitment by security managers and company directors/owners is not shown consistently throughout the contract period; all security managers and company owners/directors should be vetted before contracting to Eskom; security managers are not well supported by company owners/directors; security managers fail to provide clear, honest and definitive leadership roles in their positions; security managers are not innovative enough; and security managers "wear different hats" during the contractual period, thus having to carry out many functions simultaneously.

These findings clearly demonstrate the need for Eskom security to ensure that their security contracts are written out and prepared in such a manner that they specify the duties and responsibilities of both the security manager and the company owners/directors for the duration of contract, and Eskom must monitor this closely.

8.5.4 The real problems why security contracted out to Eskom cannot prevent cable theft

In Chapter Five, the researcher described the real problems which cause security personnel contracted out to Eskom to fail to prevent cable theft (see subsections 5.14.1–5.14.7): namely, the high turnover rate of security guards at Eskom facilities; Eskom lacks a standard training entry requirement for private security employees to work its facilities; Eskom private security contractors should use security patrol dogs at all its high crime facilities; Eskom private security contractors should use patrol vehicles at all its high crime facilities; Eskom security managers must manage in line with the security contract agreement; and improper utilisation of security manpower at Eskom facilities.

These findings clearly demonstrate the need for Eskom security to improve the major constraints that have a negative impact on the security protection methods it applies to

safeguard its facilities and those that support the private security. The finding in this study was that private security resources operate without being trained on a minimum entry requirement, which should be based on Eskom security standards. The findings further demonstrate the risk inherent in having multiple security officers working at its facilities as a result of high turnover numbers.

8.5.5 General remarks made by the participants on reducing cable theft

In Chapter Five, the researcher reviewed some of the general remarks made by the participants on reducing cable theft (see subsections 5.16.1–5.16.5): namely, security companies must deploy armed response to all facilities and improve its response times to panic alarms; private security must reduce the opportunities for criminals to commit crime at Eskom facilities; private security companies must target the underlying causes of crime committed against Eskom; Eskom management must improve its housekeeping procedures and lock up unused material; and Eskom security management must create early warning crime prevention programmes.

These findings clearly show the need for Eskom security and private security to work more closely in reducing and preventing cable theft. Joint operations to conduct risk assessments, and oversight visits to establish how security can be improved at all Eskom facilities, are urgently needed.

8.5.6 Why does the internal security management team not stop theft at Eskom?

In Chapter Six, the researcher described possible reasons for why the internal security management team cannot stop theft at Eskom (see subsections 6.4.1–6.4.6): namely, Eskom's security structures are not properly aligned; succession planning policies are not applied consistently within Eskom security divisions; Eskom Security managers fail to consider recommendations made by private security companies for improving security measures to reduce losses; there are disjointed relationships between security managers and in-house security officials; security contracts and oversight ownership are not structured evenly at Eskom; and it seems that at times criminals are adequately equipped and more determined than security members are.

These findings clearly show the need for Eskom's management to have closer interactions and relationships with its workforce.

8.5.7 The exact problems why the internal security management team struggle to prevent cable theft

In Chapter Six, the researcher described the exact problems which cause the internal security management team to struggle to prevent cable theft (see subsections 6.6.1–6.6.7): namely, the absence of an accurate crime reporting culture relating to cable theft at Eskom; Eskom appoints security companies that fail to establish strategic partnerships and develop crime prevention programmes for preventing cable theft; security assessments in Eskom are not conducted meticulously and accurately enough to prevent repeated incidences of crimes; there is a need for Eskom investigators to forge closer relationships with police investigators and prosecutors in the justice department; the fact that Eskom security cannot identify Eskom cable after it is stolen increases the risk of continued cable thefts; Eskom security must support the use of intelligent security systems to manage private security guards and supervisors; and Eskom in-house security officials need to work shifts to provide proper oversight management for security contractors. The fact that Eskom security members cannot identify Eskom cable after it is stolen, and the need for security officials to work shifts, are two issues which also need to be addressed by Eskom's internal security management team.

These findings clearly show how Eskom security has not progressed in certain critical areas, and in this process, has missed the opportunity to prevent cable theft.

8.6 CRITICAL CONCLUSIONS ON SPECIFIC FINDINGS

The specific findings presented and discussed in Chapters Five and Six, and summarised in section 8.5 above, lead to the following specific conclusions.

Restructuring: Eskom's security structures must be realigned: Eskom must create a single, centralised regional security structure for both its Transmission and Distribution business units that will consolidate and coordinate the various aspects of the regional business units' security requirements and decision-making, such as effective negotiation of security demands, and coordinating action and the integration of a wide range of security-related policy, legislative, structural and oversight issues. The "*Govender Approach*" structure (see sections 7.7 and 7.8) can be adopted by Eskom; this approach consists of a three-division approach – Proactive, Reactive and Support Security Services (Ras, 2015b).

Training entry requirement: A standard training entry requirement is needed for private security employees to work at Eskom facilities: An area of concern is that the training provided at private security institutions is not adequate and sometimes not up to standard. It furthermore does not meet Eskom's specific requirements. Eskom's substantial asset value and economic mandate towards South Africa require that its assets be properly secured by properly trained and professional security personnel. The successful introduction of the prerequisite training entry for private security guards will ensure that properly trained security personnel will work at Eskom facilities and prevent cable theft.

Eskom's Management: The Eskom internal security management team and the private security officials seemingly cannot prevent cable theft from Eskom: The areas of concern here are: the lack of cohesion, as well as inadequate communication and interaction, among the various security divisions and employees within Eskom; the lack of critical training for employees to perform professionally and effectively; and the lack of detailed and accurate information, which in effect allows opportunity for the continued, and exacerbated, incidence of cable theft.

Eskom management has a critical role to play in bridging the gap of social cohesion and in implementing compulsory training to ensure that Eskom receives good value from its employees and that they work towards the prevention of cable theft. Their participation in joint cooperation partnerships, such as researching the necessary training required for contract management, management of security service providers, cable theft investigations, and making resources available for training and team building initiatives to improve social cohesion, will improve and relieve the challenges that are facing the Eskom security departments.

A critical area of concern, and a worrying factor, is that Eskom is not receiving value for the money it pays to private security companies to prevent cable theft (and other crimes) from its facilities. It is very concerning to the researcher to find that the contracts, which are signed by the security companies committing them to protect Eskom's cables and other assets, provide a false sense of confidence to Eskom that its assets will be protected. The security companies fail to protect Eskom's assets (cables), as a result of which Eskom suffers major financial losses, which impact negatively on Eskom in terms of service delivery to South Africa.

The researcher has established and concluded that there is a direct relationship between the factors why private security performs poorly, and why they cannot prevent cable theft from

Eskom. Most of the unprofessional and poor crime prevention strategies applied by the private security companies and their personnel are the result of deviations from the contractual obligations on the part of both Eskom management and the private security companies, as well as a result of the abdication of responsibilities by Eskom security divisions to professionally and strictly manage these contracts.

Security reports: Eskom security reports are inaccurate and inconclusive: The study concludes that the deficiencies that have been highlighted now provide opportunities for Eskom security to improve its strategy and make it more transparent and interactive.

The request for ongoing training is submitted as a desperate measure by the participants to prompt Eskom to update employees' skills, and in that way, ensure that Eskom receives more productivity from them. The practice of not reporting cable theft and other crimes directly allows for opportunities to persist for criminals to continue with cable theft, thereby exacerbating the problem, because senior management in Eskom is not aware of the unrecorded losses which will not be featured in the ENECC report.

These alleged tendencies affect the image of, and erode trust and confidence in, the security departments of Eskom, and this encourages security companies to continue to perform poorly, which as a consequence negatively affects the accuracy of the crime statistics. The study has further assessed that, despite the good intentions of some security personnel to report cable theft and crime incidents, those that fail to report nevertheless facilitate the recording of an inaccurate picture of the actual cable theft and crime situation at Eskom.

The factors that contribute to this existing situation are multi-facetted and comprise the lack of proper training; few people, instead of many, have access to the CURA system; security managers are lacking in performing, or even abdicate, their responsibilities; and laziness on the part of the people tasked to report cable theft and crimes on the CURA system.

Personal commitment: The important point that the researcher wants to make is that there must be a personal commitment from managers to ensure that their staff are properly trained, and that they prevent copper theft and report crimes accurately and timely.

8.7 RECOMMENDATIONS FOR THE STUDY

The recommendations contained in this section are aimed at contributing to the optimisation of the effectiveness and operational efficiency of the Eskom security department. They take

into account the realities of the security environments in which security personnel have to operate and that they have to manage.

The researcher recommends the following, which would be of benefit to Eskom security management:

- Improve relationships between security managers and in-house security officials (see subsection 7.4.1)
- Eskom security management must realign its security contracts and form strategic partnerships with private security companies, and also develop effective crime prevention programmes to prevent cable theft (see subsection 7.4.2)
- Security assessments for Eskom facilities must be improved through further training, education, monitoring and accountability (see subsection 7.4.3)
- Management must improve the awareness culture for employees on the issue of cable theft (see subsection 7.4.4)
- Eskom security personnel must report crime incidents accurately and diligently on the CURA system (see subsection 7.4.5)
- Cable theft experts are needed to testify in court, if criminals are to receive lengthy jail terms (see subsection 7.4.6)
- Eskom security management must create a structured plan for the in-house security officials for supervising and managing private security contracts (see subsection 7.5.1)
- Eskom management must insist that private security companies deploy competent and reliable personnel to Eskom facilities (see subsection 7.5.2)
- In-house security officials must encourage line management to report non-performance issues of private security companies and employees (see subsection 7.5.3)
- There is a need for a realignment of the Eskom security structure. Eskom should consider the proposed Eskom security structure described in Chapter Seven (see section 7.7)

- Eskom should implement the proposed standard training entry requirement for private security employees to work at Eskom facilities (see section 7.9)
- Eskom should consider the suggested improvements for the CURA system (see section 7.10)
- Eskom should consider the suggested improvements to the ENECC report (see section 7.11).

8.8 AREAS FOR FURTHER RESEARCH

This research is viewed as a pioneering study in the investigation towards achieving the prevention of cable theft at Eskom. As a matter of fact, this study had to cover a limited scope and is capable only of unearthing some aspects of the prevailing situation of cable theft from Eskom. The researcher, therefore, recommends that further research be undertaken on the following areas in respect of prevention of cable theft in Eskom:

- The prevention of cable theft from Eskom's open line networks.
- The financial impact of Eskom's losses through cable theft.
- The implementation of effective crime prevention programmes to prevent cable theft
- Copper theft, scrap dealers, and copper theft exporters.

8.9 SUMMARY

In Chapter Eight, the researcher made general remarks (see section 8.2), wrote about the limitation of the study (see section 8.3), discussed the findings on the hypotheses (see section 8.4), and made remarks concerning a summary of findings of the study (see section 8.5).

Critical conclusions of specific findings (see section 8.6) were made, recommendations were made (see section 8.7), and after this, areas for further research were recommended (see section 8.8). A summary of the study (section 8.9) is then followed by final remarks (see section 8.10).

8.10 FINAL REMARKS

This study undertook a qualitative approach to investigate the extent of cable theft at Eskom and how it can be prevented. Although the researcher has come to the end of his

investigation, he feels that more needs to be uncovered and improved, in order for Eskom to more comprehensively prevent cable theft.

The researcher believes that it is appropriate to urge Eskom management to create the right environment for operational-level employees, those responsible for the capturing of all relevant information related to cable theft, and to hold the private security companies and their employees responsible for any breaches according to their contractual obligations. There is no doubt that the main reason for all the cable theft in Eskom is the present inability of all security personnel working for Eskom and those contracted to it. It is the people (all security personnel) responsible for protecting Eskom's cables who need to get their act together, do their jobs properly, and proactively protect Eskom's valuable assets.

The prevention of cable theft will greatly ease the financial burden of Eskom's financial situation. Eskom will then be in a better position to provide electricity to areas which require it, and further, it will keep the lights on for those who already have it.

If the insights of this study can be used to improve the current security efforts within Eskom to prevent cable theft and to improve security standards, then all this work will not have been in vain.

LIST OF REFERENCES

3 News. (2008). *P addicts ignore danger to steal live cables*. <http://www.3news.co.nz/nznews/p-addicts-ignore-danger-to-steal-live-cables-2008020116#ixzz3M9YGUBxf> [Accessed on 17 December 2014].

Abrahamsen, R. & Williams, M. C. (2005). *The globalisation of private security. Country report: Kenya*. Aberystwyth: Department of International Politics, University of Wales.

Achumba, I.C., Ighomereho, O.S. & Akpor-Robaro, M.O.M. (2013). Security Challenges in Nigeria and the Implications for Business Activities and Sustainable Development. *Journal of Economics and Sustainable Development*. 4(2). ISSN 2222-1700 (Paper) ISSN 2222-2855 (Online).

Addison, S. (2002). *Introduction to security risk analysis and the cobra approach*. C & A security system report (Online serial). < www.security-risk-analysis.com> [Accessed on 06 January 2015].

Adepoju, P. (2013). *NITEL Warehouse Manager among 17 arrested for cable theft in Nigeria*. <http://www.humanipo.com/news/3316/nitel-warehouse-manager-among-17-arrested-for-cable-theft-in-nigeria/> [Accessed on 19 January 2015]

Agénor, P.R. (2004). *Unemployment-Poverty Trade-Offs*. World Bank, Washington, D.C. © World Bank. <https://openknowledge.worldbank.org/handle/10986/14028 License: CC BY 3.0 Unreported> [Accessed on 5 March 2015].

Akkalkot, M. (2013). Times of India. *MTNL announces reward to curb telephone cable theft.* <http://timesofindia.indiatimes.com/city/mumbai/MTNL-announces-reward-to-curb-telephone-cable-theft/articleshow/22783146.cms> [Accessed on 17 December 2014].

Akrava, M.L. & Lane, T.A. (1983). *Beginning social work research*. Boston, MA: Allyn & Bacon.

Angula, N. (2012). http://en.starafrica.com/news/moz-power-utility-loses-us323000-to-cable-theft-sabotage.htm. [Accessed on 10 January 2015]

Asset Forfeiture Unit. National Prosecuting Authority. (2016). Available at: https://www.npa.gov.za/node/13 Accessed on 30 July 2017.

Babbie, E. & Mouton, J. (2009). *The Practice of Social Research*. South African edition. Cape Town: Oxford University Press.

Babbie, E., & Mouton, J. (2001). *The practice of social research*. South African edition. Cape Town: Oxford University Press.

Baccus, S. (2015). *Personal conversation with Baccus during July - November 2015*. She is a security manager employed at Eskom's security division. She has more than 8 years of operational experience at Eskom.

BACSA. (2009a). *Initiatives of the Non-Ferrous Crime Combating Committee (NFCCC) BAC* [Online]. < http://www.bac.co.za/content.asp?PageID=327> [Accessed on 10 November 2014]

Barbour, R.S. (2001). Checklists for improving rigour in qualitative research: a case of the tail wagging the dog? *BMJ : British Medical Journal*, 322(7294), 1115–1117.

Bayne, J. (2002). *An Overview of Threat and Risk Assessment.* South African National Standards (SANS). Pretoria: Groenkloof. SANS Institute InfoSec Reading Room.

Bennett, L. (2008a). *Metal theft – anatomy of a resource crime*. Unpublished. S.I:S.N.

Bennett, L. (2008b). *"Assets Under Attack: Metal Theft, the Built Environment and the Dark Side of the Global Recycling Market."* Environmental Law and Management, 20:176-83.

Bent, F. (2006). Five Misunderstandings About Case-Study Research, *Qualitative Inquiry*, 12(2), April 2006, pp. 219-245.

Berg J. & Nouveau, J.P. (2011). Towards a third phase of regulation, Re-imagining private security in South Africa. *SA Crime Quarterly,* 38.(38): 23-32.

Berg, B. (2007). *Qualitative Research Methods for the Social Sciences* (6th ed). Boston: Pearson Education.

Berg, J. (2007). *The accountability of South Africa's private security industry: Mechanisms of control and challenges to effective oversight*. Cape Town: Pinelands. Open society foundation for South Africa.

Berk, R.A., Campbell, A., Klap, R. & Western, B. (1992) A Bayesian analysis of the Colorado Spouse Abuse Experiment. *Journal of Criminal Law and Criminology,* 83(1): 170–200.

Binderman, R. (2012). Traceable solutions. *Traceability Solutions joins the fight again copper cable theft.* <http://www.tracesol.co.za/about/articles/traceability-solutions-joins-the-fight-again-copper-cable-theft> [Accessed on 19 August 2014].

Bloor, M. (1997). *Techniques of validation in qualitative research: a critical commentary*, in Miller G, Dingwall R, (Editors). Context and method in qualitative research. London: Sage. pp. 37–50, 1997.

Bogdan, R.C. & Biklen, S.K. (1992). *Qualitative Research for Education: An Introduction to Theories and Methods*. Boston MA: Allyn and Bacon.

Bogdan, R.C. & Biklen, S.K. (2007). *Qualitative research for education: An introduction to theory and methods*. Latest edition. Boston, MA: Pearson.

Booysen, A. (2014). *Telephonic conversation with Booysen on 18 November 2014*. He is a crime risk officer employed at Eskom's cable theft Distribution division in the North West Province. He is a former policeman. He has more than 8 years of operational experience at Eskom.

Born, H., Caparini, M. & Cole, E. (2007). *Regulating Private Security in Europe: Status and Prospects. Policy Paper No 20*. Geneva: Geneva Centre for the Democratic Control of Armed Forces (DCAF).

Bouma, G.D. & Ling, R. (2004). *The Research Process*. (5th edition). London: Oxford University Press.

Brydon-Miller, M., Greenwood, D. & Maguire, P. (2003). *Why action research?* Volume 1(1): 9–28: 034201[1476-7503(200307)1:1]. Sage Publications London: Thousand Oaks CA.

Buckley, S. (2014). *Brazil's Sercomtel sees rise in copper theft*. <http://www.fiercetelecom.com/story/brazils-sercomtel-sees-rise-copper-theft/2014-02-07> [Accessed on 20 January 2015].

Bureau of Labour Statistics, US Department of Labor. (2009). Occupational Outlook Handbook, 2008-09 Edition (2009). *Security Guards and Surveillance Officers*. <www.bls.gov.co.za> [Accessed on 30 December 2014].

Burger, J. & Lancaster, L. (2014). *The increasing burden of crime on business in South Africa*. Institute of Security Studies (ISS).> http://www.issafrica.org/iss-today/the-increasing-burden-of-crime-on-business-in-south-africa> [Accessed on 27 November 2014].

Burgess, M. (2008). The Age. *Police bust copper theft racket*. <http://www.theage.com.au/news/national/police-bust-copper-theft-racket/2008/03/03/1204402346708.html> [Accessed on the 18 December 2014].

Business Against Crime. (2016). Available at: http://bac.org.za/ Accessed on 30 July 2017.

Cable theft surge prompts railways to seek EU action. (2012). <http://www.euractiv.com/transport/growing-cable-thefts-prompt-rail-news-515740> [Accessed on 15 December 2014].

Chamber of Mines. (2010). *Introduction: towards sustainable growth and development.* Annual report (2009-2010). <http://www.bullion.org.za/documents/AR%202010 %20small.pdf> [Accessed on 19 August 2014].

Cheerkoot, J. (2014). *Personal conversation with Cheerkoot between February and October 2014*. She is a middle manager employed at Eskom's security division at Eskom's Westville office. She has more than 10 years of operational experience at Eskom and, although based at Eskom's Westville office, she works in all regions as a Business Partner to the Transmission division in Eskom (SA).

Clarke, R. (2008). *Situational crime prevention*, in: R. Wortley (Ed.) Environmental criminology and crime analysis, pp. 178–194. Cullompton, Devon: Willan Publishing.

Community of European Railway and Infrastructure Companies (CER). (2014) Metal Theft. *The Community of European Railway and Infrastructure Companies (CER) 2014 report*. <http://cer.be/> [Accessed on 20 August 2014].

Corbin, J. & Strauss, A. (2008). *Basics of Qualitative Research*. Los Angeles: Sage.

Cordeur, M.L. (2015). *Irvin Jim steps in as Medupi unrest intensifies*. Fin24. <http://www.fin24.com/Economy/Irvin-Jim-steps-in-as-Medupi-unrest-intensifies-20150410> [Accessed on 29 June 2015].

Cox, A. (2014). *Classify cable theft as sabotage*. IOL News [Online] <http://www.iol.co.za/news/crime-courts/classify-cable-theft-as-sabotage-1.1761319> [Accessed on 28 May 2015].

Crank, J.P. (1996). *The construction of meaning during training for probation and parole*. Justice Quarterly, 13(2):265-290.

Creswell, J.W. (1994). *Research design: qualitative and quantitative approaches*. London: Sage Publications.

Cullen, F.T. (2011) Beyond adolescence-limited criminology: Choosing our future – the American Society of Criminology 2010 Sutherland Address. *Criminology* 49(2): 287–330.

CURA system. (2014). < http://www.curasoftware.com/solutions/enterprise-risk-management/operational-risk-management-software.html> [Accessed on 06 November 2014].

Dalton, R.D. (1995). *Security management: Business strategies for success*. USA: Butterworth-Heinemann.

Dash, D.P. (1999). Current debates in action research. *Systemic Practice and Action Research*, 12(5): 457-92.

Dawood, Z. (2014). *Electricity thieves cost ratepayers R190 m*. IOL News. <http://www.iol.co.za/news/crime-courts/electricity-thieves-cost-ratepayers-r190 m-1.1788154> [Accessed on 01 December 2014].

Dawson, C. (2002). *Practical research methods*. Trowbridge, Wiltshire UK: Cromwell Press.

Dawson, C. (2002). *Practical research methods*. Wiltshire. UK; Cromwell Press, Trowbridge.

De Vos, A.S. (2002). *Research at Grass roots*. Pretoria: J. L. van Schaik Publishers.

De Vos, A.S., Strydom, H., Fouché, C.B. & Delport, C.S.L. (2000), *Research at grassroots*. A primer for the caring professions. 2nd edition, Pretoria: Van Schaik.

De Vos, A.S., Strydom, H., Fouché, C.B. & Delport, C.S.L. (2005). *Research at grass roots: For the social sciences and human service professions*. (3rd edition.). Pretoria: Van Schaik.

De Vos, A.S., Strydom, H., Fouché, C.B. & Delport, C.S.L. (2008). *Research at Grass roots for the Social Sciences and Human Service Professions*. 3rd edition. Pretoria: Van Schaik.

Dey, I. (1993). *Qualitative data analysis*. New York: Routledge.

Dike, V.E. (2009). Addressing youth unemployment and poverty in Nigeria: A call for action, not rhetoric. *Journal of Sustainable Development in Africa*, 11(3). ISSN: 1520-5509. Clarion University of Pennsylvania, Clarion, Pennsylvania.

Dingwall, R., Murphy, E., Watson, P., Greatbatch, D & Parker, S. (1998). Catching goldfish: quality in qualitative research. *Journal of Health Services Research and Policy* 1998(3): 167-72.

Du Preez, G.T. (1991). *Security forum*. South Africa: Butterworths.

Dzansi, D.Y., Rambe, P. & Mathe, L. (2014). *"Cable Theft and Vandalism by Employees of South Africa's. Electricity Utility Companies: A Theoretical Explanation and Research Agenda"*. Department of Business Support Studies; Faculty of Management Sciences Central University of Technology, FS; Bloemfontein South Africa. J Soc Sci, 39(2): 179-190 2014).

Easterby-Smith, M., Thorpe, R. & Lowe, A. (2004) *Management Research – An Introduction*. London: Sage Publications

Eskom factsheet. (2014). *Generation Communication* TD 0002 Revision 8.

Eskom Heritage. (2014). *Arnot Power Station*. <http://heritage.eskom.co.za/arnot/arnot.htm> [Accessed on 19 November 2014].

Eskom. (2014). *Eskom Annual Report 2014*. <http://integratedreport.eskom.co.za/>. [Accessed on 24 June 2015].

Eskom. (2015). *Eskom Network Equipment Crime Committee (ENECC) Reports*. *2014 – 2015*. Eskom internal document.

Eskom. (2015). *Eskom Power Stations in South Africa*. <http://www.eskom.co.za/Whatweredoing/ElectricityGeneration/PowerStations/Pages/Map_Of_Eskom_Power_Stations.aspx> [Accessed on 23 June 2015].

Eskom. (2015). *Network Planning Guideline for Eskom Lines and Cables*, unique number 34-619.

Eskom. (2016) *Eskom Annual Report 2016*. <http://www.eskom.co.za/IR2016/Pages/default.aspx/>. [Accessed on 01 August 2017].

Eskom. (2016). Eskom Corporate Affairs Division. *Eskom and the CSIR sign a new security agreement.* Internal mail.

Eskom. (2016). *Eskom Network Equipment Crime Committee (ENECC) reports.* Unpublished confidential documents.

Eskom. (2016). *Recruitment criteria for security division*. Unpublished internal document.

Eskom. (2016). *Security division resource planning*. Unpublished internal document.

Eskom. Group Security Mandate. <http://sustainability.eskom.co.za/sites/gs/Pages/Default.aspx> [Accessed 23 October 2014].

Etzinger, A. (2008). *Metal theft is crippling industry.* IOL News. <http://www.iol.co.za/news/south-africa/metal-theft-is-crippling-industry-1.409566> [Accessed on 11 November 2014].

Evans, C. (2011). *Copper Theft: a Crime Wave from History*. <http://historydivision.blogs.southwales.ac.uk/2011/06/08/147625/> [Accessed on 06 January 2015].

Factsheet South Africa: *Official crime statistics for 2012/13.* >http://africacheck.org/factsheets/factsheet-south-africas-official-crime-statistics-for-201213/> [Accessed on 13 October 2014].

Fin24. (2004). *Cable theft down 57%.* <http://www.fin24.com/Companies/Cable-theft-down-57-20040811>[Accessed on 22 January 2015].

Fin24. (2014). *Sacci calls for copper theft unit*. <http://www.fin24.com/Economy/Sacci-calls-for-copper-theft-unit-20140626> [Accessed on 21 January 2015].

Fin24. (2015). *Delays at Medupi as strike enters 6th week*. <http://www.fin24.com/Economy/Eskom/Delays-at-Medupi-as-strike-enters-6th-week-20150506 > [Accessed on 29 June 2015].

Firearm Control Act No. 60 of 2000. Pretoria: Government Printers.

Fischer, R.J., Halibozeck, E. & Green, G. (2008). *Introduction to security*. (8th edition). Boston: Butterworth Heinemann.

Fouché, C.B. & Delport, C.S.L. (2011). *In- depth review of literature,* in De Vos, A.S., Strydom, H., Fouché, C.B. & Delport, C.S.L. (Editors). Research at grass roots for the social sciences and human services professions. Pretoria: Van Schaik. pp. 133 – 141.

Garcia, M.L. (2008). *The design and evaluation of physical protection systems*. 2nd edition. Boston: Butterworth/Heinemann.

Garrett, C. (2004). *Developing a Security Awareness Culture – Improving Security Decision Making*. SANS Institute.< https://www.sans.org/reading-room/whitepapers/awareness/developing-security-awareness-culture-improving-security-decision-making-1526> [Accessed on 14 January 2015].

Geldenhuys, K. (2008). *Non-ferrous Metal Theft brings cities to their knees. Servamus Safety and Security Magazine*.

<http://www.telkom.co.za/general/cabletheft/metal_theft.html> [Accessed on 10 January 2015].

Gernetzky, K. (2015). *Thousands of Medupi workers return to site*. Business Day Live.<http://www.bdlive.co.za/national/labour/2015/05/19/thousands-of-medupi-workers-return-to-site> [Accessed on 29 June 2015].

Goldstein, H. (1990). *Problem-oriented policing.* New York: McGraw-Hill.

Govender, D. (2012). *Management of security information in the security industry.* Doctor of literature and philosophy (DLitt et Phil) dissertation. University of South Africa, Pretoria.

Govender, R. (2014). *A case study of factors contributing to discipline problems of security officers: Eskom distribution centres, KwaZulu-Natal North Coast region*. Masters Dissertation. UNISA.

Gray, D.E. (2004). *Doing research in the real world*. London, UK: Sage Publications.

Gray, E.D. (2009). *Doing research in the real world*. (2nd edition.). London: Sage publishers.

Greg, W.G. (2004). *A standard for medium-voltage cable systems in Eskom Distribution*. Eskom Distribution Central Region.

Hammer, A. & Jones, L. (2012). *China's dominance as a global consumer and producer of copper*. USITC Executive Briefings on Trade.

Haynes, C. (2008). *Precious Metals*. Jane's Police Review, 11 April: 18 –21.

Heriyati, P. & Ramadhan, A.S. (2012). The Influence of Employee Satisfaction in Supporting Employee Work Performance and Retention Moderated by the Employee Engagement Factor of an Institution. *International Journal of Economics and Management*, 6(1): 191-200.

Hinds, L. (2008). Public satisfaction with police: the influence of general attitudes and police citizen encounters. *International Journal of Police Science & Management*. 11(1): 54 - 66.

Hi-Tech Security Solutions. (2009). *The allure of copper theft and how to stop it.* [Online]. <http://www.securitysa.com/article.aspx?pklarticleid=5592> [Accessed on 28 November 2014].

Hi-Tech Security Solutions. (2010). *Solving copper theft.* [Online]. <http://www.securitysa.com/article.aspx?pklarticleid=5905> [Accessed on 29 January 2014].

Hi-Tech Security Solutions. (2011*). Copper Cable Theft Conference*. <http://www.securitysa.com/article.aspx?pklarticleid=6974> [Accessed on the 13 June 2014].

Horn, R.E. (2012). *A pro-active approach to curb asset theft at a South African Mine*. Masters Dissertation. UNISA.

Howell, R.T., & Howell, C.J. (2008). *The relation of economic status to subjective well-being in developing countries: A meta-analysis*. Psychological Bulletin, 134, 536-560.

Howell, R.T., Kurai, M., Yin, W. & Tam, L. (2013). *Money buys financial security and psychological need satisfaction : testing need theory in affluence,* 110: 17–29.

Huffman, T. (2013). Pragmatic Fieldwork: Qualitative Research for Creative Democracy and Social Action. *Journal of Social Justice* 3, 2013. Transformative Studies Institute.

Ingula Pump Storage. (2014). <https://en.wikipedia.org/wiki/Ingula_Pumped_Storage_Scheme> [Accessed on 23 June 2015].

Institute for Security Studies (ISS) Africa. (2014*). Cable theft is strangling SA's economy: can we escape the noose?* < http://www.issafrica.org/events/cable-theft-is-strangling-sas-economy-can-we-escape-the-noose> [Accessed 10 November 2014].

Institute of Security Studies (ISS). (2014). *Who profits from Copper?* <http://www.issafrica.org/iss-today/who-profits-from-copper-theft> [Accessed on 18 August 2014].

International Copper Study Group. (2013). <http://www.icsg.org/index.php/press-releases/finish/170-publications-press-releases/1188-2013-world-copper-factbook> [Accessed on the 12 January 2015].

Irvine, A. (2010). *Using phone interviews*. Social Policy Research Unit, University of York.

Jabareen, Y. (2009) Building a Conceptual Framework: Philosophy, Definitions, and Procedure. *International Journal of Qualitative Methods 2009, 8(4).*

Jähi, M. (2012). *Key drivers of customer value in business-to business security guard services. More value from security, Redefining value creation and service provision in security services*. VTT Technical Research Centre of Finland. <http://www.vtt.fi/publications/index.jsp> [Accessed on 15 January 2015].

Jeffery, C.R. (1977). *Crime Prevention Through Environmental Design*. Beverly Hills, CA: Sage.

Jeffery, C.R. (1996). *Mental health and crime prevention: a public health model*. Paper presented to the International Crime Prevention Practitioners Conference, Vancouver.

Jenkins, A. (2015). *Personal conversation with Jenkins during July - November 2015.* He is a senior security advisor employed at Eskom's security division. He has more than 15 years of operational experience at Eskom.

Kamath, D. (2012). DNA Analysis. *Cable theft hits train service for 4 hours on Konkan route* <http://www.dnaindia.com/mumbai/report-cable-theft-hits-train-service-for-4-hours-on-konkan-route-1753599> [Accessed on 17 December 2014].

Kingdon, G.G. & Knight, J. (2004). *Unemployment in South Africa: The Nature of the Beast*. World Development, 32, 3, 319-408. < www.elsevier.com/locate/worlddev> [Accessed on 05 February 2015].

Kooi, B. (2010). *Theft of Scrap Metal. Problem-oriented Guides for Police Series. Guide no. 58.* Washington, DC: U.S. Department of Justice, Office of Community Oriented Policing Services.

Koshy, E., Koshy, V. & Waterman, H. (2010). *Action research in healthcare*. London: Sage.

Krause, M. (2014). *Personal conversation with Krause on the 13 November 2014). He is an operations security manager for IPSS Security*. They provide security for Eskom in Zululand KZN. He was previously employed at Eskom's security division for 8years. He worked many years for SAPPI paper as a security manager and was also a former policeman.

Kvale, S. (1996). *An introduction to qualitative research interviewing*. London. Sage.

Kvale, S. (1996). *Interviews: an introduction to qualitative research interviewing*. London: Sage Publications.

Lab, S.P. (1997). *Crime prevention at a crossroads*. Cincinnati, Ohio: Anderson.

Landman, K. (2002). *Gated communities in South Africa: building bridges or barriers?* International Conference on Private Urban Governance. Mainz, Germany. June 6-9, 2002). <http://www.csir.co.za/Built_environment/Planning_support_systems/gatedcomsa/docs/bridges_barriers.pdf> [Accessed on 05 February 2015].

Laufer, W.S. & Adler, F. (Eds.). (2013). *The Criminology of Criminal Law*. New Brunswick, New Jersey, USA: Transaction Publishers.

Le Roux, G.J. (2004). *A quantitative risk analysis model for private security managers*. DLit et Phil thesis, University of South Africa, Pretoria.

Leedy, P.D. & Ormrod, J. E. (2004). *Practical research: Planning and design*. 8th Edition. New York, NY: Prentice Hall.

Levy, L., Santhakumaran, D. & Whitecross, R. (2014). *What Works to Reduce Crime?: A Summary of the Evidence*. Justice Analytical Services. Scottish Government.

Lewin, K. (1946). Action research and minority problems. *Journal of Social Issues*, 2(4), 34-46.

Lumina, C. (2006). *Police accountability and policing oversight mechanisms in the Southern African development Community*. In: African Security Review, 15 (1): 92 108.

Mabeba, M.Z. & Prinsloo, E. (2000). Perceptions of discipline and ensuing discipline problems in secondary education. *South African Journal of Education*, 20(1): 34-41.

Makubu, N. (2013). IOL News [Online]. *Copper theft costs SA R7 bn, hits city hard*. <http://www.iol.co.za/pretoria-news/copper-theft-costs-sa-r7 bn-hits-city-hard-1.1468118> [Accessed 28 October 2014].

Mantshantha, S. (2014). Financial Mail. *Eskom's power crisis is far from over*. <http://www.financialmail.co.za/coverstory/2014/03/13/eskom-s-power-crisis-is-far-from-over> [Accessed on 29 June 2015].

Marshall, C. & Rossman, G.B. (2006). *Designing Qualitative Research*. 4th edition. London: Sage Publications.

Marshall, C. & Rossman, G.B. (2006). *Designing qualitative research.* Thousand Oaks, CA: Sage.

Marshall, C. & Rossman, G.B. (2011). Designing Qualitative Research. 6th edition. USA: Sage.

Maseema, P. (2013). *Cable theft solution – technical or socio-economic?* E+C SPOT ON June 2013. City of Tshwane.

Maseko, O.B. (2011). *Perceptions on Madadeni policing by the residents in a post-apartheid era*. Doctoral Thesis. KwaDlangezwa: University of Zululand.

Masinde, F. (2014) *Copper thieves continue to be a plague for African Telcos. Issue No 332.* <http://www.balancingact-africa.com/news/en/issue-no-332/telecoms/copper-thieves-conti/en> [Accessed on 09 January 2015].

Mason, J. (2002). *Qualitative Researching*. 2nd edition. London: Sage.

Maxwell, J. (2014). *Personal conversation with Maxwell in October 2014*. He is employed as a director at G4S and currently providing a security service to Eskom in KZN. He has more than 4 years of operational experience at Eskom. He is a former policeman.

Mays, N. & Pope, C. (1996). *Rigour in qualitative research*, in Mays, N. & Pope, C., (Editors). Qualitative research in health care. London: BMJ Books.

Mays, N. & Pope, C. (2000). Assessing quality in qualitative research. *BMJ : British Medical Journal*, 320(7226), 50–52.

McMillan, J.H. & Schumacher, S. (1993). *Research in education. A conceptual introduction*. 3rd Edition, New York, NY: Harper Collins.

McMillan, J.H. & Schumacher, S. (2001). *Research in Education. A conceptual introduction.* 5th Edition. London: Longman.

McMillan, J.H. & Schumacher, S. (2010). *Research in Education: Evidence-Based Inquiry*.7th edition. Boston: Pearson Education.

McNeeley, S. & Warner, J. (2015). Replication in criminology: A necessary practice. *European Journal of Criminology 2015*, 12(5): 581– 597.

Meek, C.D. (2014). *Personal conversation with Meek during July 2014*. He is a security manager employed at Telkom. He has more than 15 years of operational experience at Telkom.

Merriam, S. (2009). *Qualitative Research: A Guide to Design and Implementation*. San Francisco, CA: John Wiley & Sons.

Minnaar, A. (2007) 'Oversight and Monitoring of Non-State/Private Policing: The Private Security Practitioners in South Africa', *ISS Monograph* 139: 127-150.

Mind Tools. (2015). *Henri Fayol's Principles of Management. Early Management Theory*. <https://www.mindtools.com/pages/article/henri-fayol.htm> [Accessed on 05 February 2016].

Mistry, D., Minnaar, A., Patel, C. & Rustin, C. (2003). *Criminal Justice Research Methodology*. South Africa: Technikon SA.

Mokonyane, N. (2014). *City of Johannesburg Electricity convention to put cable theft in the spotlight*. <http://joburg.org.za/index.php?option=com_content&view=article&id=9230:electricity-convention-to-put-cable-theft-in-the-spotlight&catid=88:news-update&Itemid=266#ixzz3G0gem9aY> [Accessed on 13 October 2014].

Moodley, D.M. (2014). *Personal conversation with Moodley during between July – October 2014*. He is a Captain in the South African Police Service working in the Organised Crime Unit. He has more than 20 years of operational experience in the SAPS and has a Master's degree in Security Management.

Moonsamy, R. (2015). *Personal conversation with Moonsamy during 2015*. He is a General Manager for IPSS Security. They provide security for Eskom in Zululand KZN.

Mouton, J. (2001). *How to succeed in your master's and doctoral studies: a South African guide and resource book*. Pretoria: Van Schaik.

Msimanga v S. (2013) (A119/12) [(2013] ZAFSHC 26 (4 February 2013).

Naidoo, P. (2014). *Telephone conversation with Naidoo on the 21 November 2014*. He is employed for more than 10 years as a Director for Fidelity Security. They provide security to Eskom in South Africa.

Napier, M., Du Plessis, C., Liebermann, S., Kruger, T., Shaw, M., Louw, A. & Oppler, S. (1998) *Environmental design for safer communities in South Africa, Vols. 1 and 2* (Pretoria: Council for Scientific and Industrial Research).

Narayan, R. & Regan, J. (2013). *Reducing Copper Theft in Telecommunications*. ERICO.

National Key Point Act No. 102 of 1980. Pretoria: Government Printers.

National Prosecuting Authority. (2016). Available at: https://www.npa.gov.za/ Accessed 30 July 2017.

Ndlovu, S. & Magwaza, N. (2008). *Metal theft is crippling industry.* IOL News. <http://www.iol.co.za/news/south-africa/metal-theft-is-crippling-industry-1.409566> [Accessed on 11 November 2014].

NEC Contract. (2015). *Term Services Contract*. <https://www.neccontract.com/Products/Contracts/Term-Service-Contract> [Accessed on 10 May 2015].

Nel, A. (2014). *Cable theft treated as a petty crime*. News24. <http://www.citypress.co.za/news/cable-theft-treated-petty-crime-andries-nel/> [Accessed on 25 February 2015].

Nell, L. (2007). *Non-Ferrous Metal Theft Reduction. Business Against Crime*. Available at: http://web.vdw.co.za/Portals/25/Documents/Papers/2007/2%20-%20Lorinda%20Nell.pdf Accessed on 30 July 2017.

Nemeth, C.P. (2010). *Private security and the investigative process*. 3rd edition. United States: CRC Press.

Newman, O. (1973) *Defensible space people and design in the violent city.* London: Architectural Press.

News24. (2012). *Limpopo cop held after copper sting* <http://www.news24.com/SouthAfrica/News/Limpopo-cop-held-after-copper-sting-20120122> [Accessed on 03 February 2015].

News24. (2014). *4 things you didn't know about copper theft.* <http://www.news24.com/SouthAfrica/News/4-things-you-didnt-know-about-copper-theft-2014)0626)> [Accessed on 10 February 2015].

Nicolaides, G. (2014). *JHB businessman in court for cable theft.* Eye Witness News. <http://ewn.co.za/2014/10/20/JHB-businessman-in-court-for-cable-thef> [Accessed on 25 February 2015].

Nicols, (2012). *Crime Prevention Through Environmental Design Strategies – April 2012.* Oshkosh Police Department Crime Prevention Unit. Available at: http://www.oshkoshpd.com/Resources/pdf/Publications/Crime_Prevention_Through_Environmental_Design_Handbook.pdf Accessed on 28 June 2016.

Nieuwenhuis, J. (2012). Qualitative research designs and data gathering techniques. In: Maree, K. (eds.) *First steps in research.* 2012. Pretoria: Van Schaik.

Nkabinde, T. (2014). *Personal conversation with Nkabinde during July – December 2014.* He is a Crime Risk Officer employed at Eskom cable theft Distribution division in KZN.

He has more than 8 years of operational experience at Eskom. He is a former policeman.

Noor, K.B.M. (2008). *Case Study: A Strategic Research Methodology*. American Journal of Applied Sciences, 5(11), 1602-1604.

Novick, G. (2008). *Is There a Bias Against Telephone Interviews In Qualitative Research?* Research in Nursing & Health, 31(4), 391–398. DOI:10.1002/nur.20259.

Nowell. L. (2015) Pragmatism and integrated knowledge translation: exploring the compatabilities and tensions. *Nursing Open*. 2(3): 141–148

Ogle, J. (2014). *Personal conversation with Ogle during July – December 2014*. He is an investigator employed at Eskom cable theft Distribution division in KZN. He has more than 8 years of operational experience at Eskom. He is a former policeman.

Okolie, I. (2013). *NITEL cable theft: I have no regrets – suspect*. <http://www.vanguardngr.com/2013/04/nitel-cable-theft-i-have-no-regrets-suspect/> [Accessed on 19 January 2015).

Parliamentary Monitoring Group meeting held on the 28 February. (2012). *Copper Theft, & Solar Water Heating: progress reports.* <http://www.pmg.org.za/report/20120228-departments-energy-public-enterprises-justice-salga-transnet-and-esko> [Accessed on 20 January 2015].

Patrick, E.M., Wrightman, P., Schoeni, R.F. & Schulenberg, J.E. (2012). Socioeconomic Status and Substance Use Among Young Adults: A Comparison Across Constructs and Drugs. *J Stud Alcohol Drugs*. 2012 September; 73(5): 772–782.

Patton, M.Q. (2002). *Qualitative research and evaluation methods*. 3rd Edition. Thousand Oaks CA: Sage Publications.

Peters, S. (2014*). Engineer's Death Blamed on Cable Theft*. IOL News [Online Edition]. <http://www.iol.co.za/dailynews/news/engineer-s-death-blamed-on-cable-theft> [Accessed on 04 October 2014].

Phakathi, B. (2010). *Drastic new steps to halt copper theft*. Business Day. <http://www.allafrica.com/stories/2010)0622047)3.html> [Accessed on 19 August 2014].

Phasiwe, K. (2015). News 24. *Blackouts partly to blame on Eskom's financial woes.* <http://www.news24.com/Archives/City-Press/Blackouts-partly-to-blame-on-Eskoms-financial-woes-20150429.[Accessed on 04 March 2015].

Pillay, K. (2001). Repositioning the private sector industry in South Africa in the 21st century – the need for professionalism of the private security practitioner. *Acta Criminologica: Southern African Journal of Criminology*, 14(3): 66-77.

Planting, S. (2011). *Copper theft: government and big business unite to do battle*. Citizen Business [Online]. <http://www.citizen.co.za/citizen/content/en/citizen/business-news?oid=217606&sn=Detail&pid=146848&Copper-theft--government-and--big-business-unite-to-do-battle> [Accessed on 20 July 2014].

Pol-Primett II. (2015). *Latest metal theft news from Portugal*. < http://www.pol-primett2.org/news/2784/latest-metal-theft-news-from-portugal> [Accessed on 15 March 2015].

Power Technology. Com. (2015). *Kusile Power Station, South Africa*. <http://www.power-technology.com/projects/kusilepowerstation/> [Accessed on 29 June 2015].

Powers, G.T., Meenaghan, T.M. & Toomey, B.G. (1985). *Practice focused research: Integrating human service practice and research*. New Jersey: Prentice hall.

Pretorius, W.L. (2012). *A Criminological analysis of copper cable theft in Gauteng*. Master's dissertation. UNISA.

Private Security Industry Regulation Act 56 of 2001. (2015a) <http://www.psira.co.za/psira/dmdocuments/2014%20PSIRA%20ACT.pdf> [Accessed on 18 November 2015].

Private Security Industry Regulation Act No 56 of 2001. Pretoria: Government Printers.

Private Security Industry Regulation Authority (PSIRA). (2015b). *Code of conduct for security service providers*.

<http://www.psira.co.za/joomla/pdfs/code_of_conduct.pdf> [Accessed on 17 November 2014].

Private Security Industry Regulation Authority (PSIRA). (2015c). *Strategic Plan (2014/15-2018/19.* <http://www.psira.co.za/psira/> [Accessed on 17 November 2014].

Private Security Industry Regulation Authority (PSIRA). (2016). *Draft regulations for the training of security service provider, 2016*. <http://www.psira.co.za/psira/dmdocuments/circular/Published%20Training%20Draft%20Regulations.24%20June%202016.pdf> [Accessed on 01 June 2016].

Private Security Industry Regulatory Authority levies Act No 23 of 2003. Pretoria: Government Printers.

Rajkumar, D. (2014). *Personal conversation with Rajkumar on the 17 October 2014 at Westville, Durban*. He is a commercial procurement officer for the past 10 years and is employed at Eskom Distribution division in KZN.

Ras, J.M. (2006). *Body guarding in a private security context*. Doctoral thesis. KwaDlangezwa: University of Zululand.

Ras, J.M. (2010). *Understanding Al-Qaeda: A Qualitative Enquiry.* Doctoral thesis. KwaDlangezwa: University of Zululand.

Ras, J. M. (2012a). The Drug Trade and the Death Penalty in Pakistan: Childhood and Practical Remarks from a Narrative-Existential Point of View. *Pakistan Journal of Criminology.* April 2012. Vol. 3(2) & 4(1):109-121.

Ras, J. M. (2012b). *Understanding Al-Qaeda. Understanding their mindset.* Saarbrücken: Lambert Academic Publishing.

Ras, J.M. (2014*). Personal conversation with Ras on the 12 December 2014.* He is the Head of Department of Criminal Justice at the University of Zululand.

Ras, J.M. (2015a). *Personal conversation with Ras on the 16 January 2015.* He is the Head of Department of Criminal Justice at the University of Zululand.

Ras, J. M. (2015b). *Telephonic conversation with Ras on the 16 February 2015.* He is the Head of Department of Criminal Justice at the University of Zululand.

Ras, J.M. (2016). *Personal conversation with Ras on the 24 June 2016.* He is the Head of Department of Criminal Justice at the University of Zululand.

Rau, N. (2014). *Eskom's power crisis is far from over*. Financial Mail. <http://www.financialmail.co.za/coverstory/2014/03/13/eskom-s-power-crisis-is-far-from-over> [Accessed on 29 June 2015].

Ritchie, J., Lewis, J., Mcnaughton nicholls, C. & Ormston, R. (2013). *Qualitative Research Practice. A guide for social science students and researchers*. London: Sage Publications.

Robbins, P.S. & Judge, A.T. (2012). *Essentials of organisational behaviour*. England: Pearson.

Roberts, I. & Rush, A. (2011). *Sources of Chinese demand for resource commodities, RBA*. Research discussion paper, Reserve Bank of Australia, No 2010–8.

Rogers, C. (2008). A security risk management approach to the measurement of crime in a private security context. *Acta Criminological. Southern African Journal of Criminology*. Crimsa 2008 Conference Special Edition, (3) 2008: 150-156.

Ronna, L.S. (1969). *An experimental study of the effects of personal proximity upon selected aspects of conversational content*. Dissertations and Theses. Paper 631. Available at: http://pdxscholar.library.pdx.edu/cgi/viewcontent.cgi?article=1630&context=open_access_etds. Accessed on 28 June 2016.

Russel, E. (2013). What Does It Mean to Be Pragmatic? Pragmatic Methods, Measures, and Models to Facilitate Research Translation. *National Cancer Institute.* 40(3): 257-265.

Salim, K. (2014). *Telkom Kenya probes cable theft at Main Station*. Issue No 320. <http://www.balancingact-africa.com/news/en/issue-no-320/telecoms/telkom-kenya-probes/en> [Accessed on 09 January 2015].

SAPS Strategic Plan. (2015). Available at: https://www.saps.gov.za/about/stratframework/strategic_plan/2015_2019/strategic_plan_%202015.pdf Accessed 30 July 2017.

SAQA – South African Qualifications Authority. Unit Standard Number 246693. *Requirements for safeguarding a national key point*. <http://regqs.saqa.org.za/showUnitStandard.php?id=246693> [Accessed on 29 December 2014].

Saunders, M., Lewis, P. & Thornhill, A. (2007). *Research Methods for Business Students*. 4th Edition. New York: Prentice Hall.

Sauti, L. (2012) *Cable theft is strangling SADC's economy: Can the region escape the noose?* <http://lazarussauti.wordpress.com/2014/11/17/cable-theft-is-strangling-sadcs-economy-can-the-region-escape-the-noose/> [Accessed on 13 December 2014].

Schermerhorn, J.R. (2002). *Management.* 7th edition. USA: R.R. Donnelly and Sons.

Sennewald, C.A. (2011). *Effective security management*. 5th edition. Butterworth-Heinemann.

Shaban, B. (2013). *Copper theft a problem in Libya*. <http://www.esi-africa.com/copper-theft-a-problem-in-libya/> [Accessed on 13 December 2014].

Shanghaidaily.com. *No train services to Dutch airport Schiphol due to cable theft.* <http://www.shanghaidaily.com/article/article_xinhua.aspx?id=239539> [Accessed on 09 January 2015].

Sharma, H. (2014). *Wind dragons' to check power cable theft*. IBN Live. <http://ibnlive.in.com/news/wind-dragons-to-check-power-cable-theft/443592-3-239.html> [Accessed on 17 December 2014].

Shearing, C. & Stenning, P.C. (1980). *Police Training in Ontario: An Evaluation of Recruit and Supervisory Courses*. Toronto: Centre of Criminology, University of Toronto.

Shearing, C.D. & Stenning, P.C. (1983). Private Security: Implications for Social Control, *Social Problems* 30(5): 493-506.

Sidebottom, A., Belur, J., Bowers, K., Thompson, L. & Johnson, S.D. (2011). Theft in price-volatile markets: On the relationship between copper price and copper thefts. *Journal of Research in Crime and Delinquency*, 48, 396-418.

Sidebottom, A.J., Ashby, M. & Johnson, S.D. (2014). Copper Cable Theft: Revisiting the Price–Theft Hypothesis. *Journal of Research in Crime and Delinquency* 1-17.

Simonsen, C.E. (1998). *Private security in America: An introduction.* Upper Saddle River, New Jersey: Prentice Hall.

Singh, N. & Omar, Y. (2011). *R20 m a month to replace stolen cable*. IOL news [Online]. <http://www.iol.co.za/news/south-africa/kwazulu-natal/r20 m-a-month-to-replace-stolen-cable-1.1108994> [Accessed on 19 August 2014].

Snyman, CR. (1986). *Strafreg*, 2nd edition. Durban: Butterworths.

Solomon, R. (2013). *Unintended consequences of war on copper cable theft – proposed export curb will cause huge job losses*. BizNews.com. <http://www.biznews.com/thought-leaders/2013/08/17/unintended-consequences-of-war-on-copper-cable-theft-export-curb-to-cause-huge-job-losses/> [Accessed on 28 October 2014].

South Africa. (1996). *The Constitution of the Republic of South Africa, Act 108 of 1996).* Pretoria: Government Printer.

South African Law Commission. *Research paper 18. Conviction rates and other outcomes of crimes reported in eight South African police areas*. Project 82. German Technical Cooperation. Available at: http://www.justice.gov.za/salrc/rpapers/rp18.pdf [Accessed on 20 May 2015].

South African Revenue Services. (2016). Available at: http://www.sars.gov.za/Pages/default.aspx Accessed on 30 July 2017.

Spence, T. (2012). EurActiv.com. *Cable theft surge prompts railways to seek EU action*. http://www.euractiv.com/section/transport/news/cable-theft-surge-prompts-railways-to-seek-eu-action/[Accessed on 20 May 2015].

Starker, L. (2012). *Cable theft surge prompts railways to seek EU action*. <http://www.euractiv.com/transport/growing-cable-thefts-prompt-rail-news-515740> [Accessed on 10 January 2015].

Statistics South Africa. (2015). *Quarterly Labour Force Survey Quarter 2:2015.* http://www.statssa.gov.za/publications/P0211/P02112ndQuarter2015.pdf [Accessed on 23 December 2015].

Steenkamp, D. (2002). *The role of private security in crime prevention*. D.Phil thesis. KwaDlangezwa: University of Zululand.

Steyn, J. (2002). *The effect of "group think" in the South African Police Service: An experimental analysis*. MTech: Policing dissertation: Pretoria: Technikon Pretoria.

Stott, T. (2014). *Eskom's power crisis is far from over*. Financial Mail. <http://www.financialmail.co.za/coverstory/2014/03/13/eskom-s-power-crisis-is-far-from-over> [Accessed on the 29 June 2015].

Struwig, T.S. & Stead, D. (2007). *Planning, designing and reporting research*. Maskew Miller Longman. Cape Town, Pearson Education South Africa.

Strydom, H. (2007). *Sampling and sampling methods,* pp 192-204, in De Vos, A.S., Strydom, H. Fouché, C.B. & Delport, C.S.L., (2007). Research at grassroots: For the social sciences and human service professions. 3rd edition. Pretoria: van Schaik.

Swingler, S. (2016). *South Africa's R40bn private security industry under threat*. Daily Maverick. Available at: https://www.dailymaverick.co.za/article/2017-05-14-south-africas-r40bn-private-security-industry-under-threat/ Accessed on 31 July 2017.

Tai-hoon, Kim & Sakurai, K. (2008). Definition of Security Practices in Security Management Part of Security Level Management Model. *International Journal of Security and Its Applications*. 2(1).

Talbot, J. & Jakeman, M. (2009). *Security risk management body of knowledge: (SRMBOK)*. New Jersey: John Wiley and Sons.

Taylor, J.R., Norrholm, S.D., Bibb, J.A., Nestler, E.J., Ouimet, C.C. & Greengard, P. (2003). Corrigendum to "cocaine-induced proliferation of dendritic spines in nucleus

accumbens is dependent on the activity of cyclin-dependent kinase-5". *Neuroscience* 116 (1): 19–22.

Terre Blanche, M. & Durrheim, K. (2002). *Research in practice applied methods for the social sciences*. Cape Town: UCT Press.

Tewksbury, R. (2009). Qualitative versus Quantitative Methods: Understanding Why Qualitative Methods are Superior for Criminology and Criminal Justice. *Journal of Theoretical and Philosophical Criminology*. 1(1): 38-58.

The City of Cape Town. *Security services: the hidden cost of vandalism and theft*. <https://www.capetown.gov.za/en/Pages/Securityserviceshiddencostvandalismtheft.aspx> [Accessed on 01 December 2014].

The Eskom Factor. (2011). <http://www.eskom.co.za/OurCompany/SustainableDevelopment/Pages/The_Eskom_Factor.aspx> [Accessed on 15 February 2015].

The Express Tribune. (2015). *Army Major arrested in Pakistan Railways copper heist case.* <http://tribune.com.pk/story/250715/pakistan-railways-arrests-major-in-copper-heist-case/> [Accessed on 14 December 2015].

Thelwell, E. (2014). *4 things you need to know about copper theft*. News24.Com. <http://www.news24.com/SouthAfrica/News/4-things-you-didnt-know-about-copper-theft-20140626)> [Accessed on 15 January 2015].

Tomo, A. (2013). *Moz power utility loses US$323,000 to cable theft, sabotage*. <http://en.starafrica.com/news/moz-power-utility-loses-us323000-to-cable-theft-sabotage.html> [Accessed on 02 March 2015].

Traceable solutions. (2014). *Traceability Solutions joins the fight again copper cable theft.* <http://www.tracesol.co.za/about/articles/traceability-solutions-joins-the-fight-again-copper-cable-theft> [Accessed on 19 August 2014].

United States Department of Energy. (2010). *Updated Assessment of Copper Wire Thefts from Electric Utilities*. <https://www.oe.netl.doe.gov/docs/Updated%20Assessment-Copper-Final-101210%20c.pdf> [Accessed on 20 November 2014].

United States Nuclear Regulatory Commission. (2014). < http://www.nrc.gov/> [Accessed 20 November 2014].

Van de Sande, A. & Schwartz, K. (2011). *Research for Social Justice: A Community-Based Approach*. Canada: Fernwood.

Van der Walt, P.J., Cronje, G. & Smit, B.F. (1982). *Criminology. An Introduction*. Pretoria: Haum.

Van Onselen, G. (2013). *South Africa: critical but stable. Rhodes University*. <http://www.ru.ac.za/perspective/perspectivearticles/southafricacriticalbutstable-1.html> [Accessed on 23 December 2014].

Van Steden, R. & Sarre, R. (2007). The Growth of Private Security: Trends in the European Union. *Security Journal*, 20: 222-235. <http://www.academia.edu/1115424/Examining_The_Roles_Of_The_Police_And_Private_Security_Officers_In_Urban_Social_Control> [Accessed on 13 March 2015].

Voskuilen, C. (2014). *Personal conversation with Voskuilen during July 2014*. She is a senior advisor employed at Eskom Group Security. She is based Eskom's main office in Megawatt Park, JHB.

Wainwright, I. (2014). *17 EU Member States in coordinated action against metal thieves.* The Hague, the Netherlands. <https://www.europol.europa.eu/content/newsletter-17-eu-member-states-coordinated-action-against-metal-thieves> [Accessed on 09 January 2015].

Wakefield, A. (2003). *Selling Security: The Private Policing of Public Space*. Devon and Oregon: Willan Publishing.

Walliman, N. (2011). *Research Methods, the basics*. USA: Routledge.

Webb, E.J., Campbell, D.T., Schwartz, R.D. & Sechrest, L. (1966). *Unobtrusive Measures: Nonreactive Measures in the Social Sciences*. Chicago: Rand McNally.

Welman, C., Kruger F. & Mitchell, B. (2005). *Research Methodology.* 3rd ed. Cape Town: Oxford University Press.

Welman, J.C. & Kruger, S.J. (2005). *Research methodology*. 3rd ed. Cape Town: Oxford University Press.

Welsh, B.C. & Farrington, D.P. (2010). *The Future of Crime Prevention: Developmental and Situational Strategies*. National Institute of Justice. Bethesda. Maryland.

Whiteacre, K.L., Medler, D., Rhoton & Howes, R. (2008). *Indianapolis Metals Theft Project: Metal Thefts Database Pilot Study*. Indianapolis, IN: University of Indianapolis, Community Research Centre.

Wiid, J. & Diggines, C. (2013). *Marketing research*. 2nd ed. Cape Town: Juta.

Wilkinson, K. (2015). *Does SA have the largest private security industry in the world?* Africacheck. < http://africacheck.org/reports/does-sa-have-the-largest-private-security-industry-in-the-world> [Accessed on 26 March 2015].

Winter, W. (1996). *Some Principles and Procedures for the Conduct of Action Research, NewDirections in Action Research (pp. 13-27)*. London: The Falmer Press.

Wortley, R. & Mazerolle, L. (Editors). (2011). *Environmental Criminology and Crime Analysis.* New York: Routledge.

Zhang, Y. & Wildemuth, B.M. (2005). Qualitative analysis of content. Available at: http://philpapers.org/rec/ZHAQAO. Accessed on 15 June 2016.

ANNEXURE A

Annexure A1



Photograph of redundant underground mining operation after copper cable theft (Horn, 2012), cf section. 1.10.2).

Annexure A2



Photograph of a train derailment in Pretoria (South Africa) caused by cable theft (CR. 1.2) Source:<http://www.news24.com/SouthAfrica/News/Cable-theft-caused-train-collision-20130131>.

Annexure A3



Stolen copper cables recovered at a scrap metal dealer in Roodepoort.
Source: http://ewn.co.za/2014/10/20/JHB-businessman-in-court-for-cable-theft (cf. section 3.8).

Annexure A4



A joint operation involving Eskom, Transnet, the SAPS and led to the recovery of copper wire from a scrapyard dealer in Durban. Source: <http://www.iol.co.za/news/south-africa/kwazulu-natal/r20 m-a-month-to-replace-stolen-cable-1.1108994?ot=inmsa.ArticlePrintPageLayout.ot>.

Annexure A5



The Durban Flying squad (10111) received information of the cables being stored at premises in Wood Hurst, Chatsworth. When the police searched the house, they found two foreign nationals and a South African who were striping the copper cables. The three was arrested and the copper valued at R1.8 Million was recovered. Further investigations into this matter revealed that the cable belonged to the EThekwini Municipality in KwaZulu-Natal.

Source: R1.8 million rand copper seized from Chatsworth home by the SAPS. Article published in the Chatsworth Rising Sun newspaper, 29 November 2014. <http://risingsunchatsworth.co.za/28561/stolen-copper-cables-worth-r1-8-million-recovered-suspects-arrested-chatsworth/>.

Annexure A6



Colonel Emelda Setlhako of the SAPS Corporate Communication Centre in the North West reports that a man transporting copper cable worth an estimated R150 000 was arrested on 6 March 2014 after the Phokeng K9 unit received information and spotted the suspect's white Toyota Hilux on the N4. The driver was pulled off and the cables were found hidden under a blanket. The driver was unable to produce the necessary documents and authorisation to transport the copper cable; the driver was arrested for the possession of stolen goods and the vehicle was impounded (http://www.platinumweekly.co.za/articleA414.html).

Source: Copper Cable Bust in North West Province of South Africa <http://www.platinumweekly.co.za/articleA414.html>.

Annexure A7



City Power (Johannesburg) has reported that it had suspended five employees for the theft of drums of cable worth R4.5 m at the Randburg depot in Johannesburg. Each of the cable drums stolen carries cable that is 300 metres long.

Source: <http://www.fin24.com/Economy/City-Power-employees-nabbed-for-cable-theft-20140819>.

Annexure A8



Annexure A9



Annexures A8 and A9 show that perpetrators are willing to enter Eskom premises, notwithstanding the presence of security guards.

Annexure A10



Security officers tied up during a robbery at an Eskom facility (cf. sections. 3.3.8; 6.4.10)

Annexure A11



Mr Krause and the researcher discussing security issues at an Eskom substation on the North Coast, KwaZulu-Natal (cf. sections. 2.5.3; 2.5.5)

Annexure A12



The researcher and Mr T Nkabinde (Eskom Crime Risk Officer) discussing the CURA system and discussing the cable theft issue Eskom (cf. section 2.5.3).

Annexure A13



The researcher, Mr J Ogle (Eskom investigator) and Mr T Nkabinde (Eskom Crime Risk Officer) discussing the CURA system and discussing the cable theft issue Eskom (cf. section. 2.5.3).

Annexures A14/A15/A16/A17/A18: EXAMPLES OF POOR HOUSEKEEPING



(cf. sections 3.6.6; 5.16.4; 6.6.5; 7.7.3)

Annexure A15



(cf. sections 3.6.6; 5.16.4; 6.6.5; 7.7.3)

Annexure A16



(cf. sections 3.6.6; 5.16.4; 6.6.5; 7.7.3)

Annexure A17



Cables left in an area where the fence is damaged (cf. sections 3.6.6; 5.16.4; 6.6.5; 7.7.3)

Annexure A18



(cf. sections 3.6.6; 5.16.4; 6.6.5; 7.7.3)

Annexure 19



Cable theft crime scene (cf. sections 2.5.9; 5.16.4)

Annexure A20



Crime scene: Eskom project site affected by cable theft (cf. section 2.5.9)

Annexure A21



A picture of a cable drum that was removed from Eskom during a theft incident (cf. section 2.5.9)

Annexure A22



A picture of a crime scene of cable theft at an Eskom premises (cf. section 2.5.9)

Annexure A23



An Eskom security dog undergoing training (cf. section. 2.5.9; 4.3.1; 5.14.3; 7.3.5)

Annexure A24



An Eskom security dog training to jump through a hoop; once the dog is trained to jump through an ordinary hoop, it will be trained to jump through a fire hoop (cf. section 2.5.9; 4.3.1; 5.14.3; 7.3.5)

Annexure A25



Eskom security guards and their dogs after a training session (cf. section 2.5.9, 4.3.1, 5.14.3, 7.3.5)

Annexure A26



Eskom dogs and handlers on the parade ground (cf. section 2.5.9; 4.3.1; 5.14.3; 7.3.5)

Annexure A27



The Eskom security team with security dogs during training (cf. section 2.5.9; 4.3.1; 5.14.3; 7.3.5)

Annexure A28



An Eskom security dog performing a long jump over obstacles during training (cf. section 2.5.9; 4.3.1; 5.14.3; 7.3.5)

Annexure A29



Eskom security staff with their dogs display trophies from winning competitions (cf. section 2.5.9; 4.3.1; 5.14.3; 7.3.5)

Annexure A30



An imported German shepherd bred for security purposes at the Eskom Dog Centre in Arnot (cf. section 2.5.9; 4.3.1; 5.14.3; 7.3.5)

Annexure A31



An Eskom security guard on patrol with a patrol dog (cf. section 2.5.9; 4.3.1; 5.14.3; 7.3.5)

ANNEXURE B

FREQUENTLY STOLEN ESKOM MATERIAL

TRANSFORMERS



Figure A4.1: 11 kV Transformer



Figure A4.2: 315 kVA

These are transformers. They vary in size from 11kV to 500kV. Transformers are used to convert the electricity from overhead lines into a usable voltage for customers. These transformers are vandalised by thieves for the copper coils and oil inside. Thieves pull the transformers off the installations and then use cutting torches, hacksaws, etc. to open them to remove the coils and oil. The financial loss to Eskom is huge, as the cheapest transformer costs as much as R5 000. Power supply to the customer is lost when the transformer is vandalised or stolen.



Figure A4.3: Inside of a transformer



Figure A4.4: Inside of a transformer

Figures A4.3 and A4.4 (above) are transformers that were cut open and the copper coils removed.

OVER HEAD CABLE LINES



Figure A4.5: Overhead power lines

These are overhead power lines. These lines are strung with conductors composed of either aluminium or copper. These are high-voltage lines, which distribute the electricity supply to

customers. When the conductor is stolen, electrical supply is lost. Copper lines are more frequently targeted, due to the fact that the copper conductor is not uniquely marked. It can be identified through technical specs and forensics. Eskom aluminium conductor is marked with a unique identifier.

OVERHEAD LINES / PYLONS





Figure A4.6: Collapsed Pylons

This large steel structure is used to keep overhead high voltage power lines in the air. These lines are strung with copper or aluminium conductors and distribute electrical supply to customers. When overhead conductors are stolen, the tension on the pylon is unevenly distributed, resulting in the entire pylon structure buckling.

COPPER AND COVERED CONDUCTOR



Figure A4.7: Covered aluminium conductor.

This conductor is insulated with a fireproof PVC coating



Figure A4.8: Copper conductors are used on overhead power lines.

The copper conductor has an appearance of green discolouration to the naked eye. Unfortunately, this conductor is not marked, due to the age of the power lines.

REINFORCED CONDUCTOR

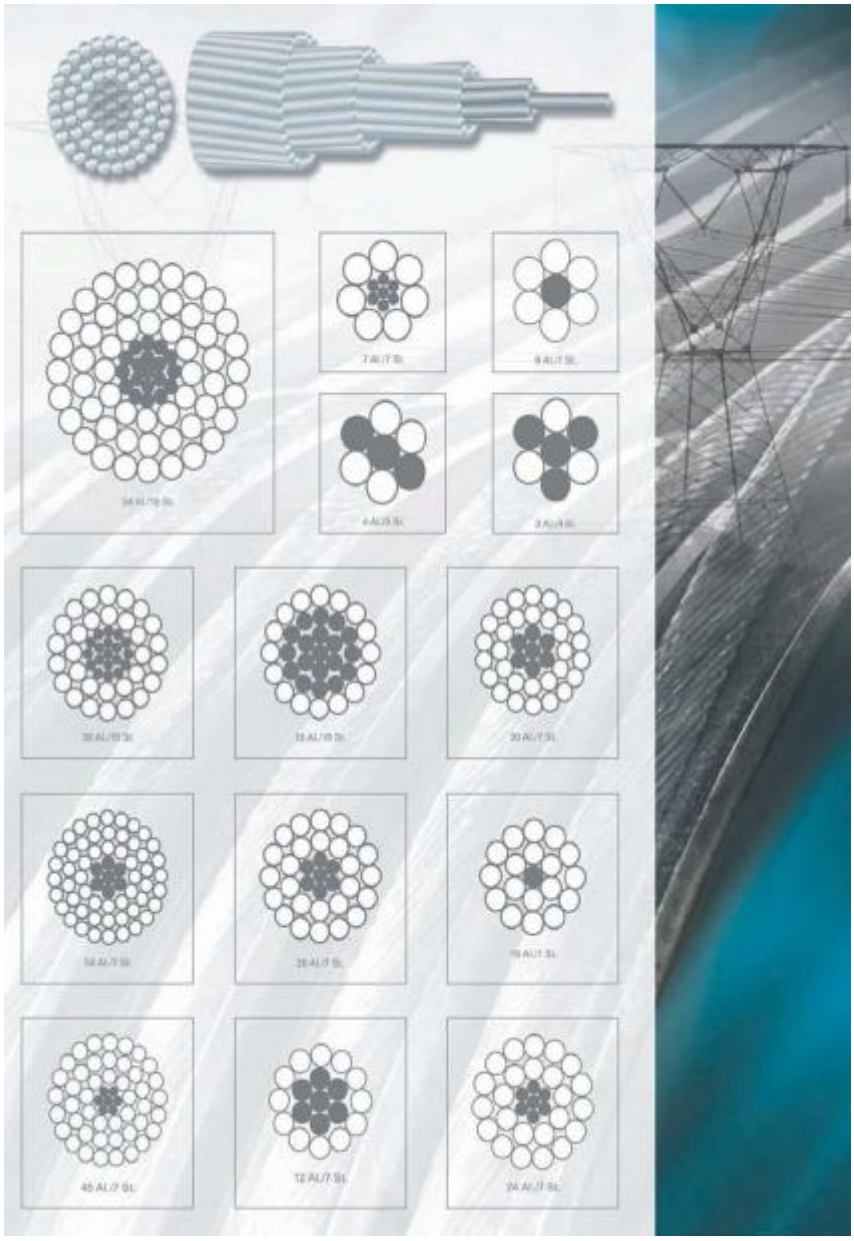


Figure A4.9: The composition of reinforced aluminium conductor – it is strengthened with strands of steel wire.

SUBSTATIONS





Substations are where various overhead lines meet and electricity is redistributed. They consist of transformers, voltage regulators, breakers, reclosers, VTs, CTs and various types of cables. Thieves target substations for the copper earthing, copper cables and copper coils found in the transformers, VTs and CTs. The oil spillage from vandalised transformers, VTs and CTs results in an environmental hazard.



Figure A4.10: A substation transformer that was vandalised and the copper coils inside stolen.



Figure A4.11: Vandalised substation (1)



Figure A4.12: Vandalised substation (2)

Figures A4.12 and A4.12 are photographs of substations that were vandalised by thieves and the copper cables, earthing and transformers stolen.

ESKOM SUBSTATION STRUCTURES

The following photographs depict various types of equipment found in substations that are vandalised for the copper inside.



Figure A4.13: VT (on the left) and CT (on the right)



Figure A4.14: Kiosk (on the left) and Voltage Regulator (on the right)



Figure A4.15: Mini Sub



Figure A4.16: NEC Transformer



Figure A4.17: Recloser



Figure A4.18: Breaker

COPPER EARTHING



Figure A4.19: Round Earthing



Figure A4.20: Flat earthing

These photographs depict round and flat copper earthing found at substations. The earthing is painted with a green-coloured coating.

AIRDAC AND BUNDLE THEFT



Figure A4.21: Various houses being electrified by means of airdac

Airdac runs from the pole-top box to the house and the bundle conductor from the transformer to the pole-top box. Airdac and bundles are stolen to do illegal connections and to sell the copper and aluminium for personal gain.

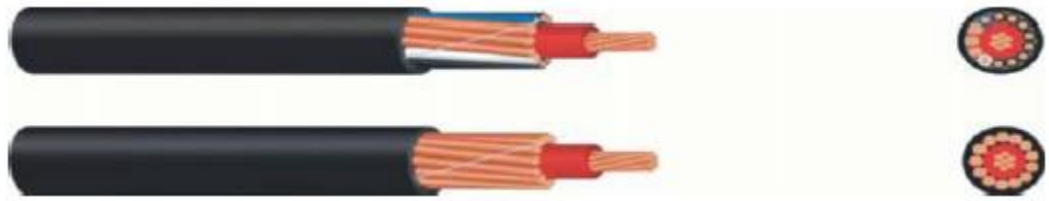


Figure A4.22: Airdac cable (1)



Figure A4.23: Airdac cable (2)

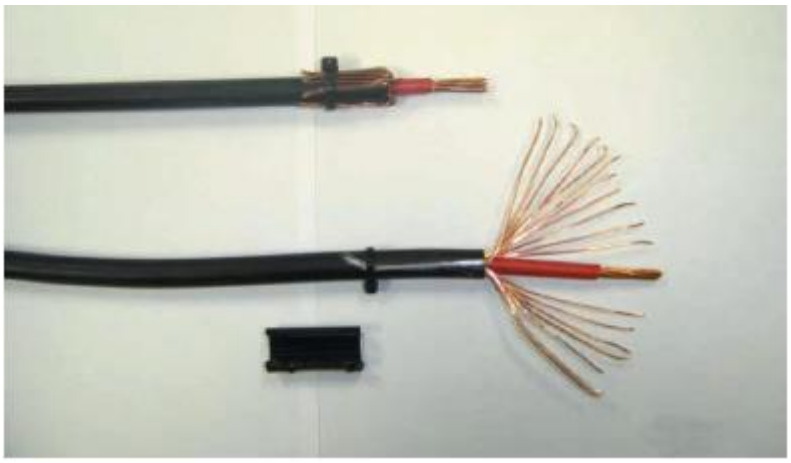


Figure A4.24: Airdac cable (3)

Figures A4.22, A4.23 and A4.24 depict three types of airdac cable. Airdac is used to supply electricity to a house – it is strung between the house and the pole-top box. The cable varies from 4 mm to 10 mm in diameter.

AERIAL BUNDLE



Figure A4.25: Aerial bundle (1)



Figure A4.26: Aerial bundle (2)



Figure A4.27: Aerial bundle (3)

The above three figures depict aerial bundles, which is used to supply electricity to a house – it is strung between the transformer and the pole-top box.

TYPES OF CABLE STOLEN

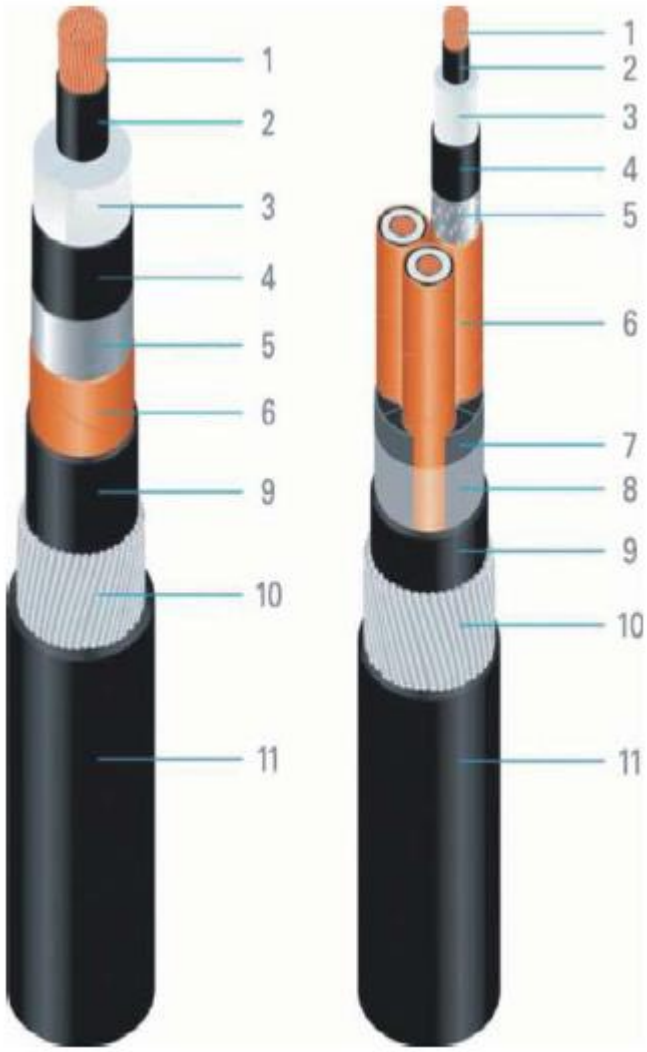






Regardless of where cables are stored or installed, they are stolen.

6.6kV – 33kV cable single / 3-core



1 – Conductor (copper / aluminium)

2 – Conductor screen – extruded semi-conductive layer integral width:

3 – Insulation – XLPE

4 – Core screen – extruded free strippable semi-conductive layer

5 – Semi-conductive numbered tape

6 – Metallic earth screen – copper tape(s)

7 – Fillers – pre-formed plastic material

8 – Binder tape

9 – Inner sheath (bedding)

10 – Armouring (steel wire or aluminium wire)

11 – Outer sheath



Figure A4.28: Single-core copper cable.

This cable varies in diameter from 1.5 mm up to as much as 400 mm. This is an insulated cable – covered with a PVC coating – and can be reinforced with armour wire, composed of either steel wire or aluminium wire, to make it stronger. This type of cabling is found within substations and at installations running from the transformer to the meter box, and from the meter box into the house / building.

3-CORE CABLE



Figure A4.29: 3-core copper cable

This cable varies in diameter from 1.5 mm up to as much as 400 mm. This is an insulated cable – covered with a PVC coating. There are three strands / cores, individually insulated, within the outer sheath.

4-CORE CABLE

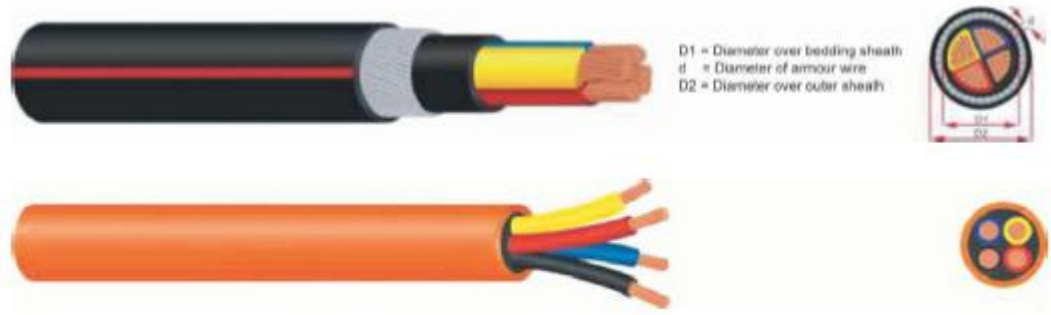


Figure A4.30: 4-core copper cable



Figure A4.31: 4-core copper cable

Figures A4.30 and A4.30 above depict 4-core copper cable. This cable varies in diameter from 1.5 mm up to as much as 400 mm. This is an insulated cable – covered with a PVC coating – and can be reinforced with armour wiring, composed of either steel wire or aluminium wire, to make it stronger. There are four strands / cores, individually insulated, within the outer sheath.

MULTI-CORE CABLE



Figure A4.32: Multi-core copper cable (1)



Figure A4.33: Multi-core copper cable (2)

Figures A4.32 and A4.33 depict multi-core copper cables. This cable varies in diameter from 1.5 mm up to as much as 400 mm. This is an insulated cable – covered with a PVC coating. There are multiple strands / cores, individually insulated, within the outer sheath.

EQUIPMENT USED TO STEAL CABLE



Thieves use an array of equipment to cut overhead lines and cables. The most common types of equipment used are hacksaws (mounted on a long wooden pole to cut overhead lines), pliers, bolt cutters and carpet knives.

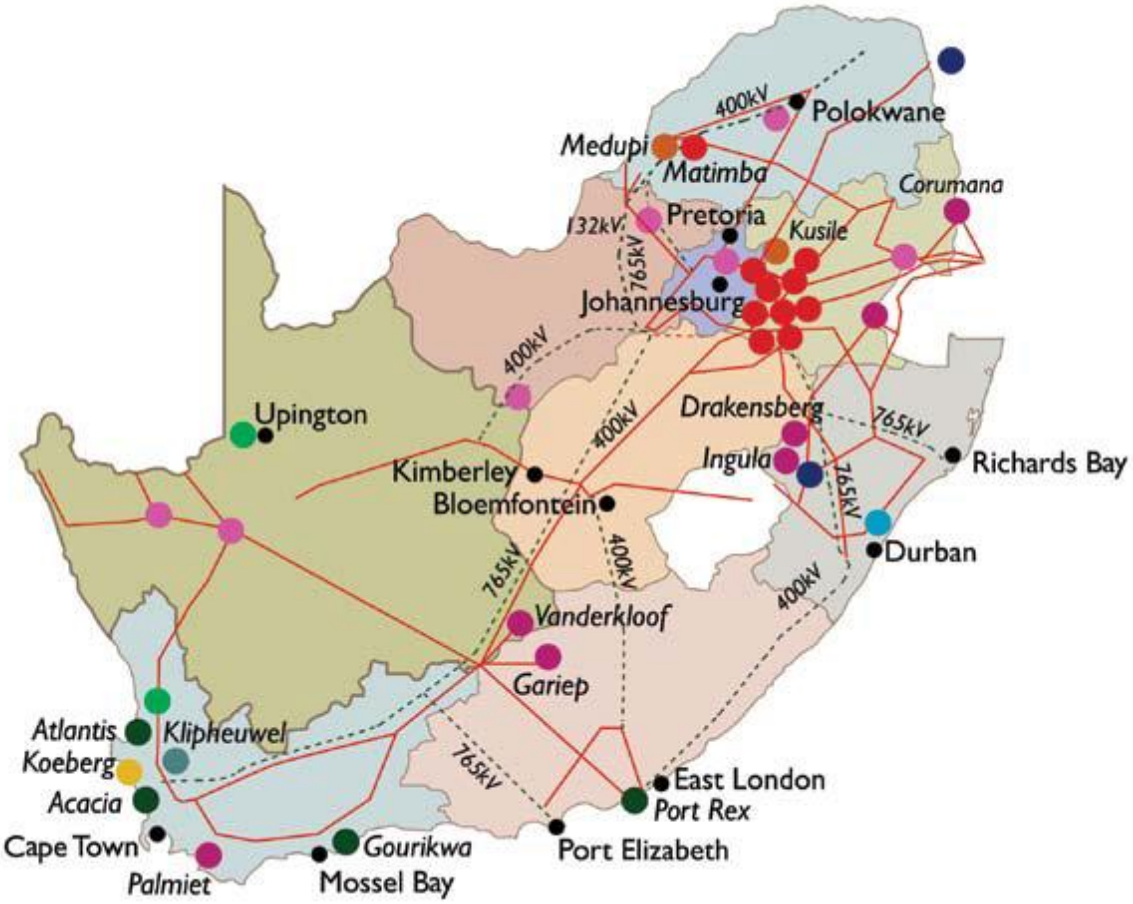
Reference:

Schultz, L. & Groenewald, C. Eskom Identification Guide. Frequently Stolen Material.

Mpumalanga Operating Unit, Eskom Distribution.

ANNEXURE C: MAPS

Annexure C1: ESKOM network in South Africa



This map indicates the South African power network (Source: Eskom integrated report 2011)

Annexure C2: Map of Africa (cf. section 1.10.1)



Source: <http://www.mapsofworld.com/africa/> [Accessed on 13 March 2015].

Annexure C3: Map of South Africa (cf. section 1.10.2)



Source: <www.ezilon.com> [Accessed on 13 March 2015].

Annexure C4: Map of Asia (cf. section 1.10.3)



Source: <http://www.worldatlas.com/webimage/countrys/as.htm> [Accessed 20 March 2015].

Annexure C5: Map of Europe (cf. section 1.10.4)



Source: <http://www.mapsofworld.com/europe/> [Accessed on 13 March 2015].

Annexure C6: Map of the United States of America (USA) (cf. section 1.10.5)



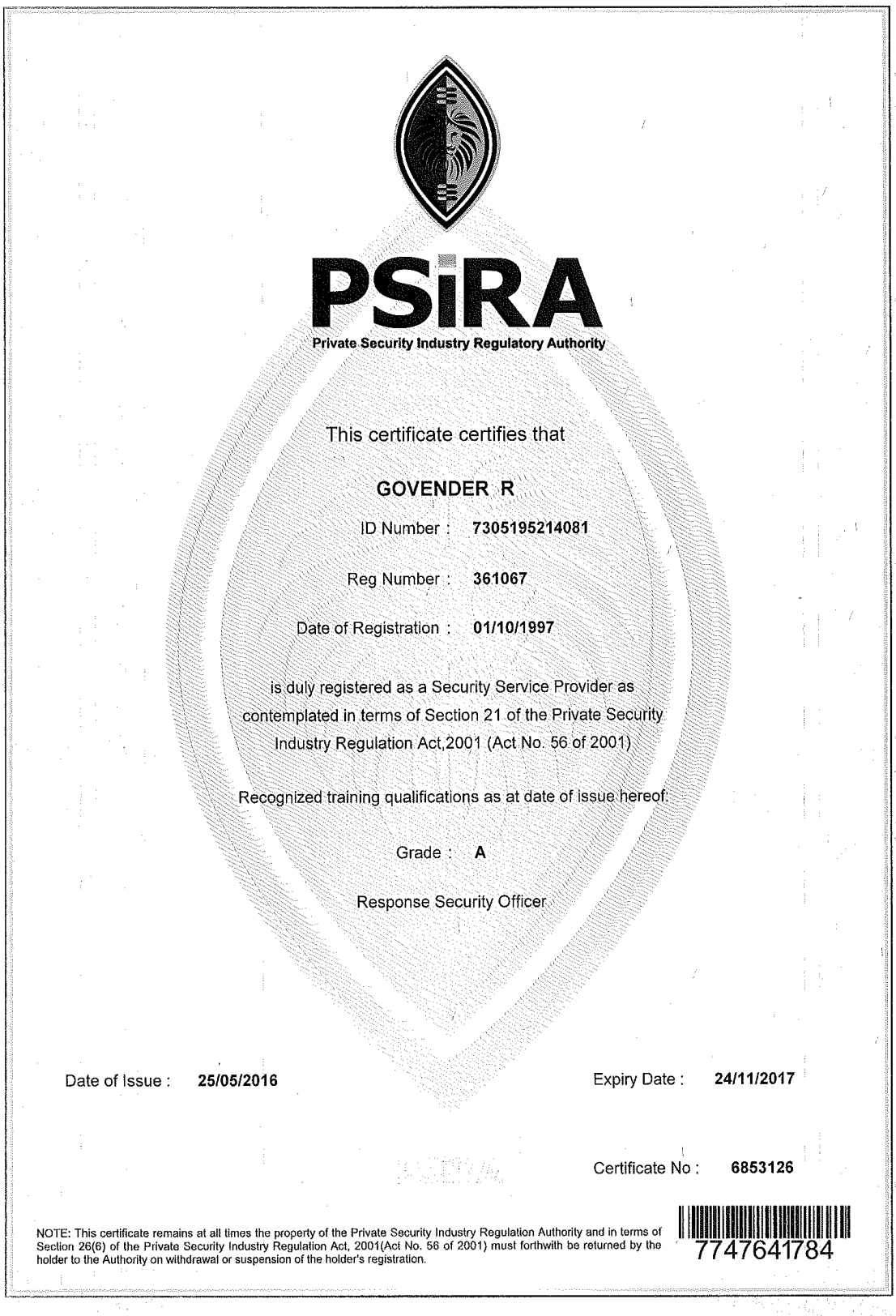
Source: <http://www.mapsofworld.com/usa/> [Accessed on 13 March 2015].

Annexure C7: Map of Australasia and New Zealand (cf. section 1.10.6)



Source: <http://www.aunztravel.com.au/australia-new-zealand-map> [Accessed on the 13 March 2015].

ANNEXURE D: PSIRA CERTIFICATION



PSiRA

Private Security Industry Regulatory Authority

This certificate certifies that

GOVENDER R

ID Number : **7305195214081**

Reg Number : **361067**

Date of Registration : **01/10/1997**

is duly registered as a Security Service Provider as contemplated in terms of Section 21 of the Private Security Industry Regulation Act,2001 (Act No. 56 of 2001)

Recognized training qualifications as at date of issue hereof:

Grade : **A**

Response Security Officer

Date of Issue : **25/05/2016**

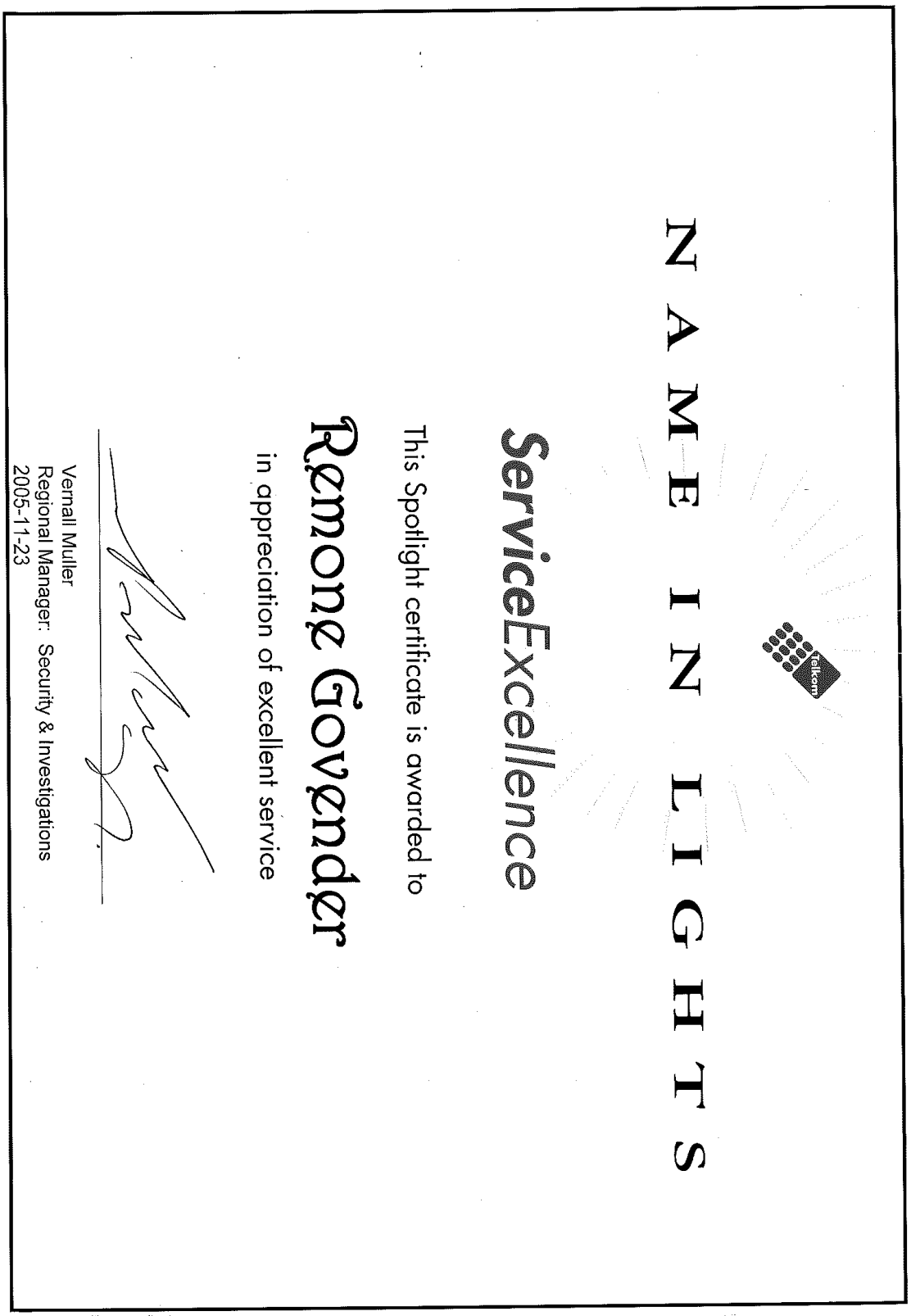
Expiry Date : **24/11/2017**

Certificate No : **6853126**

NOTE: This certificate remains at all times the property of the Private Security Industry Regulation Authority and in terms of Section 26(6) of the Private Security Industry Regulation Act, 2001(Act No. 56 of 2001) must forthwith be returned by the holder to the Authority on withdrawal or suspension of the holder's registration.

7747641784

ANNEXURE E: NAME IN LIGHTS CERTIFICATE



ANNEXURE F: MTECH DEGREE SECURITY MANAGEMENT

UNISA
UNIVERSITY OF SOUTH AFRICA

We certify that

REMONE GOVENDER

having complied with the requirements of the Higher Education Act and the Institutional Statute, was admitted to the degree of

MAGISTER TECHNOLOGIAE

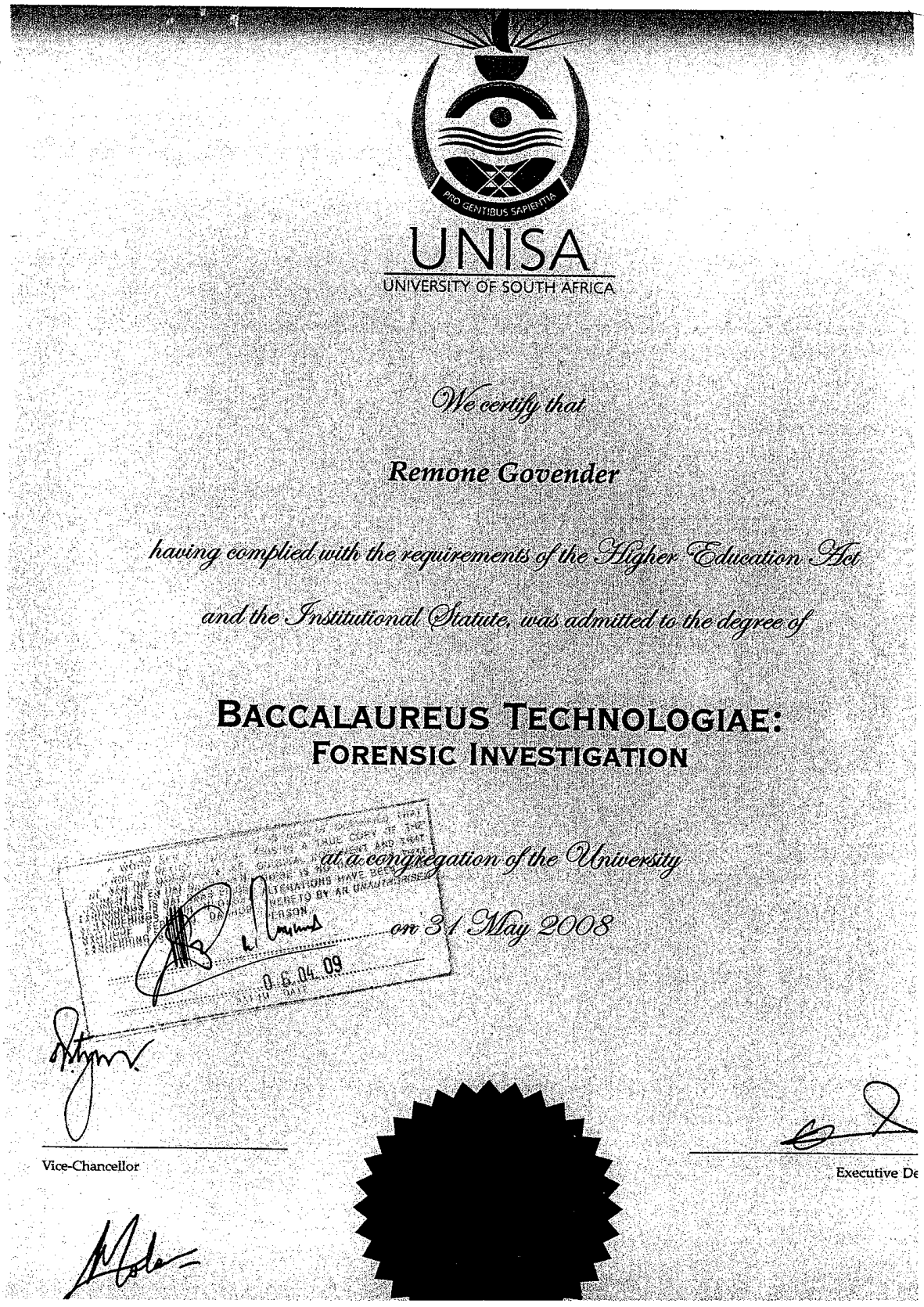
in Security Management

at a congregation of the University on 30 May 2014

Vice-Chancellor

Executive Dean

ANNEXURE G: BTECH DEGREE FORENSIC INVESTIGATION



UNISA
UNIVERSITY OF SOUTH AFRICA

We certify that

Remone Govender

having complied with the requirements of the Higher Education Act

and the Institutional Statute, was admitted to the degree of

BACCALAUREUS TECHNOLOGIAE:
FORENSIC INVESTIGATION

at a congregation of the University

on 31 May 2008

Vice-Chancellor

Executive De

ANNEXURE H: ADVANCED SECURITY MANAGEMENT PROGRAM

TECHNIKON PRETORIA

PROSPERITAS PER PERITIAM

TECHNIKON
SERTIFIKAAT CERTIFICATE

in

ADVANCED SECURITY MANAGEMENT PROGRAMME

Uitgereik aan Issued to

REMONE GOVENDER
7305195214081

Op grond van sy/haar sukses in die volgende: By virtue of his/her success on the following:

Corporate Risk Management
Strategic Management
Financial Management for Non-Financial Security Managers
Organizational Development and Leadership
Initiating and Managing Change
Cyber Crime
Counter Intelligence: Protection of Information
Forensic Techniques
Security Legislation

Opleidingstydperk Period of training

17 - 28 NOVEMBER 2003

SOCIAL DEVELOPMENT STUDIES
Fakulteit/Faculty

Dekaan/Dean

Departementshoof/Head of Department

K6746

2003-12-01
Uitreikingsdatum/Date of issue

ANNEXURE I: SAPS SWAT COURSE TRAINING CERTIFICATE

G.P.-S. 002-0131 SAP 292

SUID-AFRIKAANSE POLISIE SOUTH AFRICAN POLICE

Sertifikaat · Certificate

Hiermee word gesertifiseer dat This is to certify that

Nr.: / No.: 0247101-9 Rang: / Rank: Konstabel / Constable

Naam: / Name: R Govender

die / successfully completed the S.W.A.T. Course

and R5 Course

aangebied deur / presented by Internal Stability Unit No. 9 Point sukses-

vol deurloop het.

Duur van kursus: Vanaf / Duration of course: From 1993-04-17/18 tot / to 1993-04-22/23

Plek/Place Durban

Kursusleier/Course Leader
Lieutenant C De Wet

Bevelvoerder/Commander
Colonel E C Kennedy

Kommissaris van die Suid-Afrikaanse Polisie
Commissioner of the South African Police
Colonel R A Du Rand

ANNEXURE J: INTERVIEW SCHEDULE

Title: "*INVESTIGATION TOWARDS THE PREVENTION OF CABLE THEFT FROM ESKOM"*

INTERVIEW NO:……

SECTION A: WHY CANNOT THE PRIVATE SECURITY GUARDS PREVENT CABLE THEFT AT ESKOM?

1. Are the security guards adequately trained to protect Eskom facilities and identify Eskom's cables?
2. Are the security guards observant whilst on duty?
3. Are the guards reporting skills good enough to raise awareness immediately after an incident has occurred?
4. Do you think security officers are distracted by their mobile phones while on duty?
5. Do Security officers sleep on duty more especially between 23h00 to 03h00?
6. How effective and consistent are the security patrols during the shifts (mainly at night)?
7. Are vetting and screening done consistently prior to the deployment of security officers for Eskom facilities?

SECTION B: WHY CANNOT THE SUPERVISORS PREVENT CABLE THEFT AT ESKOM?

8. Are supervisor effective, dependable and reliable during routine supervision?
9. Are there disjointed relationships between supervisors and guards?
10. Are supervisors adequately trained to supervise Eskom facilities and identify Eskom's cables?
11. Are vetting and screening done consistently prior to the deployment of supervisors to Eskom facilities?
12. Should inspectors be lead investigators for crime incidents at Eskom?
13. Are there adequate support structures for supervisors to feel safe and committed to their jobs?

SECTION C: WHY CANNOT THE MANAGERS AND COMPANY DIRECTORS / OWNERS PREVENT CABLE THEFT AT ESKOM?

14. Does security managers and company directors / owners commitment remain consistent during the contract period?
15. Are vetting and screening done consistently prior to the deployment of managers to Eskom facilities?
16. Do you think security managers need to get involve in cable theft investigations?

17. Do you think security managers are adequately supported by company owners/directors?
18. Do security managers accept accountability for serious operational breaches?
19. Are the current security managers innovative enough and have the experience to manage large corporate contracts?

SECTION D: WHAT ARE THE REAL PROBLEMS WHY SECURITY CONTRACTED OUT TO ESKOM CANNOT PREVENT CABLE THEFT?

20. Is there a high turnover rate of security guards at Eskom facilities?
21. Is there an Eskom standard training entry requirement for private security employees to work at the Eskom facility?
22. Do you believe in the deployment of security patrol dogs for Eskom's high risk facilities?
23. Do you believe in the deployment of security patrol vehicles for Eskom's high risk facilities?
24. Do you believe that Eskom's security managers lack experience?
25. Is there a balance in security manpower numbers at Eskom facilities?

SECTION E: WHY CAN'T THE INTERNAL SECURITY MANAGEMENT TEAM STOP THEFT AT ESKOM?

26. Are Eskom's security structures properly aligned?
27. Is succession planning policies applied consistently in Eskom security division?
28. Do Eskom Security managers consider recommendations made by private security companies to improve security measures to reduce losses?
29. Are there disjointed relationships between security managers and in-house security officials (Area officers, sections officers, security officers working for Eskom)?
30. Are security contracts and oversight ownership structured evenly at Eskom?
31. Do you believe criminals are now adequately equipped and more determined to commit crimes at Eskom facilities?

SECTION F: WHAT ARE THE EXACT PROBLEMS WHY THE INTERNAL SECURITY MANAGEMENT TEAM STRUGGLE TO PREVENT CABLE THEFT AT ESKOM?

32. Is there an absence of a security information culture relating to cable theft at Eskom?
33. Does Eskom appoint security companies that establish strategic partnerships and develop crime prevention programs to prevent cable theft?
34. Are Threat and Risk Assessments (TRA) at Eskom conducted meticulously and accurately?
35. Are there expert witnesses available at Eskom to motivate for harsher sentences against criminals stealing Eskom cables?

36. Does poor housekeeping at Eskom facilities increase the risk of cable theft?
37. Does Eskom security use intelligent security systems to manage private security guards and supervisors?
38. Do Eskom in-house security officials work shifts to provide proper oversight management for security contractors?
39. If the president of South Africa instructs you to immediately stop cable theft at Eskom, what will you do within one month?
40. Do you have any further information you want share related to cable theft?
41. Do you have any remarks or recommendations on reducing cable theft at Eskom?

SECTION I: CLOSING

42. I appreciate the time you took for this interview. Is there anything else you think would be helpful for me to know?

    _____

43. I should have all the information I need. Would it be all right to call you if I have any more questions?

Thank you for answering my questions.

Reference number of participant**.....** Date**.....**

ANNEXURE K: PERMISSION LETTER

Eskom

University of Zululand
Corner Guldengracht & East Arterial Roads
RICHARDS BAY
3900

Date:
12 March 2015

Enquiries:
Tel +27 035 902 6950

Dear Professor Johan Ras

RESEARCH PROPOSAL (PHD) - THE PREVENTION OF CABLE THEFT FROM ESKOM: A QUALITATIVE APPROACH

The purpose of this study conducted by Remone Govender (student number: 201454924) is to gather relevant data to understand the extent of copper theft within Eskom in greater detail. It also will also look at the role of private security contractors and Eskom's security management team who are responsible within Eskom tasked to prevent these losses. In the final analysis the study will look at the action steps that need to be taken in order to prevent copper theft.

Emanating from the general research aim or goal of the study, the following specific research objectives are formulated:

- To establish why private security contractors cannot protect Eskom's copper.
- To see why Eskom's internal security team seems unable to stop copper theft.
- To determine what action steps must be taken by Eskom to ensure that no copper theft occurs.

Kindly be informed that approval for the proposed research on the above mentioned topic and purpose of the study, permission is hereby granted to Remone Govender on the basis that the research will be restricted to the non-disclosure of sensitive and confidential information of Eskom and that Eskom is permitted to review this information before the thesis is submitted for publication.

Yours sincerely

Martin Strauss
SENIOR MANAGER (GROUP SECURITY)

Sustainability Systems
Group Security
Megawatt Park Maxwell Drive Sunninghill Sandton
PO Box 1091 Johannesburg 2000 SA
Tel +27 11 800 3172 Fax +086 665 7369 www.eskom.co.za
Eskom Holdings SOC Ltd Reg No 2002/015527/30

ANNEXURE L: CONSENT FORM

AGREEMENT:

I hereby consent to:

- Be interviewed for the research project topic: "**INVESTIGATION TOWARDS THE PREVENTION OF CABLE THEFT FROM ESKOM"**
- Follow-up interviews if necessary;
- The use of data derived from these interviews by the interviewer in a research report as he deems appropriate.

I also understand that:

- My participation in this study is voluntary and I can refuse to participate, or withdraw at any time without stating a reason;
- Anonymity is guaranteed by the researcher and data will under no circumstances be reported in such a way as to reveal my identity;
- No reimbursement will be made by the researcher for information rendered or for my participation in this project;
- By signing this agreement I undertake to give honest answers to reasonable questions and not to mislead the researcher; and
- I will in no way derive any personal benefit from taking part in this research project.

I hereby acknowledge that the researcher/interviewer:

- Discussed the objectives, aims and goals of this research project with me;
- Informed me about the contents of this agreement; and
- Explained the implications of my signing this agreement.

In co-signing this agreement the researcher undertakes to:

- Maintain confidentiality, anonymity and privacy regarding the identity of the subject and information rendered by the interviewee.

(Interviewee signature) (Interviewer signature)

_____ _____

Date: _____ Date: _____

I, (interviewer signature)_____ certify that I explained the contents of the above document.

ANNEXURE M: CONSENT FORM FOCUS GROUP INTERVIEWS

University of Zululand
Private Bag X1001
KwaDlangezwa
3886

Dear Participant/Respondent

PARTICIPATION IN RESEARCH PROJECT: FOCUS GROUP INTERVIEWS

I am currently a student in the Department of Arts, School of Criminal Justice at the University of Zululand, busy with my studies for a ***DLITT et PHIL*** (doctorate) degree in Criminology. My research title is "***Investigation towards the prevention of cable theft from Eskom".***

I will be conducting a focus group interview with you on the problem of cable theft at Eskom and establish what needs to be done to prevent cable theft. The focus group interview should take about an hour to complete.

The objective of the study is:

- To establish the extent of cable theft at Eskom;
- To see what private security must do to prevent cable theft and;
- To determine what action steps must be taken by Eskom internal security management team and those responsible for the capturing of all relevant information related to cable theft

You are kindly requested to participate in the group interview, as honestly as possible. All the collected information will be collated and analysed in order to develop an accurate picture for this research project. If you have any queries please feel free to ask for an explanation. You are not required to provide your name or any other form of identification. All responses and information received will be treated as confidential and the respondent's identity will remain anonymous (i.e. anonymity is guaranteed, your identity will NOT be divulged to anyone). If you want to exit the group interview, you may do so at any time during the group discussion. If you need any further verification or clarity of any other information, you can contact my supervisor Prof. Johannes Marthinus Ras (RasJ@unizulu.ac.za) on 035-9026518.

Thank you for your time and participation!

Mr Remone Govender

Mobile: 0833786978

Email: remone.govender@eskom.co.za

ANNEXURE N: OBSERVATION GUIDE

OBSERVATION GUIDE		
CATEGORY	RESPONSE	RESEARCHERS NOTE
PERIMETER PROTECTION (FENCE, LIGHTS, GATES ETC.)		
SECURITY SYSTEMS CAPABILITY		
SECURITY OFFICER EQUIPMENT (TORCH, FIREARM, BULLETPROOF VEST ETC.)		
COPPER CABLES VISIBILITY ON SITE		
COPPER CABLES SAFE GUARDING CAPABILITY ON SITE		
SECURITY GUARD PATROL INTERVALS		
SECURITY SUPERVISION ROUTINE FOR FACILITY SECURITY		
SECURITY MANAGEMENT VISIT ROUTINE FOR FACILITY SECURITY		
SECURITY GUARD PERFORMANCE /CAPABILITY AND UNDERSTANDING OF ESKOMS CABLES		
ESKOM SECURITY MANAGEMENT CAPABILITY TO IDENTIFY SECURITY BREACHES AND PUT MEASURES IN PLACE. CHECK FOR HOLES IN THE FENCE, LIGHTING ETC.		
ESKOM EMPLOYEES PARTICIPATION IN THE ESKOM SECURITY PROGRAM		
MANPOWER CAPACITY AT THE FACILITY TO PROTECT ESKOM CABLES. SUFFICIENT OR INSUFFICIENT		
SITE PLANS, SECURITY OPERATIONAL PROCEDURES, THREAT AND RISK ASSESSMENTS, SITE PROCEDURES		

i Leon Van Den Berg is an Independent Forensic Investigations Consultant and former senior consultant at Eskom responsible for investigating and combatting network related crime, and chairperson of the multi-disciplinary Non-Ferrous Theft Combating Committee. The researcher was a colleague and worked closely with Mr Van Den Berg while he was employed at Eskom.

ii Mr Martin Strauss is the head of Group Security at Eskom.

iii Whoonga (also known as nyaope or wunga) is a street drug that has allegedly come into widespread use in South Africa since 2010, mostly in the impoverished townships of Durban, although it is claimed to be appearing in other places in South Africa as well.

iv 29 October 2014 in Simmerpan, Johannesburg