MANAGEMENT OF SECURITY INFORMATION IN THE SECURITY INDUSTRY

by

DORAVAL GOVENDER

submitted in accordance with the requirements
for the degree of

DOCTOR OF LITERATURE AND PHILOSOPHY

in the subject

CRIMINOLOGY

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: PROF A D V MINNAAR

JUNE 2012

COPYRIGHT

STATEMENT

Student number: **536-364-0**

I, **DORAVAL GOVENDER,** declare that this thesis: **MANAGEMENT OF SECURITY INFORMATION IN THE SECURITY INDUSTRY,** is my own work and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references.

_____ _____

SIGNATURE DATE

(D. Govender)

DEDICATED

TO MY MOTHER, MRS PARVATHY MURUGAN GOVENDER

AND MY LATE DAD, MR RAMSAMY MURUGAN GOVENDER

ACKNOWLEDGEMENTS

My honour goes to God the Almighty, who showed me the way and never let go of my hand. I also want to acknowledge and thank the following people for the support and assistance they provided during this study:

- My wife Chumpa, daughter Anusha, sons Kreesen and Kieron, son-in-law Savan and daughter-in-law Sal Sarika, for their never-ending love, support, patience and being there for me during difficult times. To my grandchildren Caitlin and Cameron for their love, understanding and patience.
- My promoter, Prof. Anthony Minnaar, 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.
- Prof. Johan Prinsloo, for his exceptional contribution in getting me on track.
- Prof. Cherita Morrison for her inspiration and editorial support.
- Ms Sarika Sewpersad, lecturer from the Programme Security Management for her technical support.
- To SAPS, SABRIC, PSI, CGRI in Gauteng, South Africa and ECU in Perth, Western Australia, for giving me written permission and support to conduct the case study research.
- Special thanks to Dr David Brooks and his team from ECU for making all the appointments for my interviews in Perth, Western Australia. The hospitality shown to me in Australia was wonderful.
- Mrs Suwissa Muchengetwa for her statistical support.
- All participants from the security industry in Gauteng who assisted me with the questionnaires, case studies, semi-structured interviews and focus group interviews.
- UNISA for affording me the opportunity to develop in knowledge and experience through this research.
- To the late Lieutenant General S Maharaj, Colonel Soobramani Pillai, Soobramoney Govender and (retired) Colonel Munsami Rungasamy for their support and encouragement to pursue academic goals.

SUMMARY

Incidents, threats and vulnerabilities have the potential to negatively affect an organisation's assets. Information on these incidents, threats and vulnerabilities are important to security. It is therefore necessary for this security information to be effectively and efficiently managed, so that correct decisions may be made on the implementation of security risk control measures. This study explored the management of security information in the security industry by undertaking the following:

- establishing the "*status quo"* of the collection and analysis of security information and the implementation of security risk control measures in practice;
- identifying the nature and extent of problems experienced in the collection and analysis of security information and the implementation of security risk control measures; and the
- discovery of a new Security Information Management Model (SIMM).

Mixed methods research was used to study the management of security information in the security industry. The explorative research design was used for this purpose. Semi-structured and focus group interviews were conducted with senior security managers and operational security officers, respectively. The grounded theory research design was used to analyse the qualitative data in order to generate a substantive grounded theory. The theory is that security officers operate without a standardised framework to manage security information.

The data from the semi-structured and the focus group interviews were used to design a questionnaire to conduct a survey using the quantitative approach. The non-experimental research design was used to conduct this self-administered questionnaire survey. The data from this questionnaire survey helped validate and confirm the substantive grounded theory. The study found that there was the need for a Security Information Management Model to manage security information in the security industry. Based on this finding the researcher recommended a new Security

Information Management Model for the management of security information in the security industry.

Key terms

Security Industry; Security information; Threat; Vulnerability; Incident; Collection of security information; Analysis of security information; Implementation of security risk control measures, Sharing of information, Information protection.

LIST OF ABBREVIATIONS

ATM	-	Automated Teller Machines
ASIAL	-	Australian Security Industry Association Liaison
ASIOBLU	-	Australian Security Intelligence Organisation Business Liaison Unit
BAC	-	Business Against Crime
BIS	-	Business Intelligence System
CAG	-	Council of Australian Governments
CAS	-	Crime Administration System
CCF	-	Crime Combating Forum
CCTV	-	Closed Circuit Television
CEO	-	Chief Executive Officer
CEOs	-	Chief Executive Officers
CGRI	-	Consumer Goods Risk Initiative
CGCSA	-	Consumer Goods Council of South Africa
CIAC	-	Crime Information Analysis Centre
CIMC	-	Crime Information Management Centre
CIOs	-	Crime Information Officers
CISF	-	Critical Infrastructure Security Forum
CIT	-	Cash-in-Transit
COB	-	Computerised Occurrence Book
COMPSTAT	-	Computer Statistics
CPA	-	Crime Pattern Analysis
CPF	-	Community Police Forum
CPFs	-	Community Police Forums
CPTED	-	Crime Prevention Through Environmental Design
CTA	-	Crime Threat Assessment
DSRM	-	Department of Security Risk Management
ECU	-	Edith Cowan University
GIS	-	Geographic Identification System
GISC	-	Global Information Security Company
ICT	-	Information and Communication Technology
IRIS	-	Incident Reporting Information Systems (IRIS)

ISCTISN	-	Industry Security Committee and Trusted Information Sharing Networks
IMS	-	Incident Management System
IPA	-	Incident Pattern Analysis
JOCOM	-	Joint Operational Committee
MANCOM	-	Management Committee
MISS	-	Minimum Information Security Standards
MOU	-	Memorandum of Understanding
NDPP	-	National Directorate of Public Prosecutions
NICOC	-	National Intelligence Coordinating Committee
NIM	-	National Intelligence Model
NPA	-	National Prosecuting Authority
OHS	-	Occupational Health and Safety
PPS	-	Physical Protection Systems
PSI	-	Petroleum Security Initiative
PSIRA	-	Private Security Industry Regulatory Authority
SABRIC	-	South African Banking Risk Information Centre
SAICB	-	South African Insurance Crime Bureau
SAPRA	-	South African Petroleum Retailers Association
SAPS	-	South African Police Service
SASOL	-	South African Synthetic Oils and Liquids
SIA	-	Security Industry Alliance
SIAU	-	Security Information Analysis Unit
SIMM	-	Security Information Management Model
SIU	-	Special Investigations Unit
SMS	-	Short Message System
SRMC	-	Security Risk Management Cycle
SRMM	-	Security Risk Management Model
SOP	-	Standing Operating Procedures
SWOT	-	Strengths, Weaknesses and Opportunities
TSA	-	Technikon South Africa
TA	-	Threat Assessment
UNISA	-	University of South Africa
UK	-	United Kingdom

US	-	United States (of America)
USA	-	United States of America
VA	-	Vulnerability Assessment
WA	-	Western Australia
WAP	-	Western Australian Police

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION AND MOTIVATION FOR THE RESEARCH

CHAPTER 4: SECURITY INFORMATION MANAGEMENT

APPENDICES

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION AND MOTIVATION FOR THE RESEARCH

1.1 INTRODUCTION

Over the last decade-and-half private security officials in South Africa have developed and increased their skills and body of knowledge. Some of this development has been necessitated by the increasing use of new (security) technologies and equipment and growing managerial sophistication within this specialised field of expertise (Minnaar, 2005: 85). Many of them have been employed as security officials at various government departments, i.e. not confined to the 'private' security sector. They safeguard and protect government assets just as in the private sector (Irish, 1999: 1-7). Owing to the aforementioned, the researcher decided to use the concept '*security service providers*', rather than '*private*' security service providers as the collective descriptive term of the target research population in this study.

Private security service providers commonly use security risk management processes to identify risks in organisations (Fisher, Halibozek & Green, 2008: 148). Based on the analysis of risks, security risk control measures are often designed to either overprotect a non-essential component or fail to adequately protect a vital portion of a facility. This misalignment is due to a lack of understanding of what is being protected and the surrounding environment. It is absolutely essential that a facility (site being protected) be fully understood in term of its constraints, expected performance, operations and the circumstances in which the facility exists. Garcia (2001: 15), calls this, the "characterisation of a facility". When characterising a facility, security information is collected on many different aspects of the facility and then reviewed and analysed.

The term '*security information'* relates to information on incidents, threats and vulnerabilities which has the potential to adversely affect an organisation's assets (Fischer et al., 2008: 149). Incident based information can be anything from an accident, anecdote (bird flies into a camera), violation of law or violation of company

policy (Opolot, 1999: 6-7). Threat information includes information on criminals, terrorists, foreign intelligence services, commercial or industrial competitors and people with malicious intent (to harm the organisation). Information on vulnerabilities is emphasised in specific security control measures, projected through people assets, information assets, physical assets/information and communication technology (ICT) (Talbot & Jakeman, 2008: 32-35).

This study explored the collection and analysis of security information and the implementation of security risk control measures in the security industry of the Gauteng province in South Africa.

This chapter introduces and provides the motivation for the study. It discusses the rationale for the study, problem statement, research questions, research goal, research objectives, definitions of concepts and the outline of the thesis.

1.2 RATIONALE FOR THE STUDY

In 2002, Ernest and Young's Global Information Security Company (GISC) from the United States (US) conducted a survey on information management at companies worldwide. The survey showed alarming gaps in their critical systems and data (Johnson, 2005: 331). The survey found that, of the companies surveyed:

- many do not conduct workplace investigations;
- some do not have security information strategies;
- personnel lack security information training; and
- there were no standard operating procedures relating to security information management (Johnson, 2005: 331).

According to Clark (2010: 1-4), the aftermath of the 11 September 2001 attacks on the World Trade Centre in New York and the Pentagon in Washington, D.C. identified many failures. Some of the common failures include:

- failure to share security information;
- failure to analyse security information; and
- failure to act on the information.

Focus group interviews[1] for this study indicated that many security service providers do not have:

- awareness programmes on security information at their facilities;
- security information collection units;
- security plans for the collection of security information;
- policy for security information management; and
- standard operating procedures (SOP).

1.2.1 Create awareness on the importance of security information

More needs to be done towards creating awareness on the importance of security information in reducing crime, increasing detection rates and preventing losses (Garcia, 2008: xvii). If all employees are contractually made aware of their role and responsibilities towards security information, they can be held accountable for any breach of security. Security service providers need to create awareness among all personnel and their clients on the importance of security information (Van Rooyen, 2008: 2). People should be made aware that information can come from a myriad of sources both internal and external of the organisation. It can be collected overtly or covertly, using different collection techniques. Information is available on everyone and everything. One just needs to know where to find it and how to find it. Information should be seen as the lifeblood of any organisational activity (Van Rooyen, 2008: 95). In the Western Australian (WA) casino industry, the collection of security information is everyone's responsibility. An information awareness culture is created by the distribution of pamphlets, holding awareness workshops and using a common code of conduct for all employees at the Casino. LCD television screens are also used to encourage the general public to provide information to specific control points (Interview no 23).

1.2.2 Intensify the collection of security information

Once the threat or vulnerability has been defined, then the planning of the collection of security information starts. Collection of the required security information will have

[1] Focus group interviews held on 10 April 2010 with security service employees from Gauteng at the University of South Africa.

to be intensified. Collectors will be tasked to collect the relevant security information. The collectors will have to ask questions of sources with knowledge of the defined threat or vulnerability (Clark, 2010: 10). The collection of the raw information is an important function in the entire security information management process. It requires understanding, knowledge, skills and courage. If adequate and proper information is not lawfully collected, the security information management process cannot be successful (Peterson, 1994: 270).

A total of 387 273 (registered with the Private Security Regulatory Authority (PSIRA) as active) security officers are currently employed in the Republic of South Africa. Of this total, approximately 151 991 work in the province of Gauteng. In comparison there are about 160 000 operational police officers employed in the Republic of South Africa. This equates to an approximate ratio of one 1 police officer for every three 3 security officers privately employed and/or on contract (PSIRA, 2012). This large number of serving personnel in the security industry can help intensify and grow the security information collection capacity.

1.2.3 Promote the sharing of security information

The Constitution of the Republic of South Africa provides for Community Police Forums (CPFs) and the National Intelligence Coordinating Committee (NICOC). The CPFs are used by both the community and the police to share incident based information on crime tendencies and patterns. Security Managers have a responsibility to become part of CPFs in order to share information on crime incidents and threats. The South African Police Service shares crime information on incidents and threats with private security service providers on a need-to-know basis (Abrie, 2008: 22). In terms of section 3 of the National Strategic Intelligence Act, No. 39 of 1994, crime intelligence may be provided to the SAPS in support of the SAPS' policing function in terms of section 205 (3) of the Constitution.

On 22 May 2007, in his departmental budget speech, the South African Minister of Safety and Security, Mr Charles Ngukala, announced that the private security industry had been drawn into partnership with the SAPS in the fight against crime. He indicated that talks between the police and private security had been initiated on

"partnership policing". The Minister stated that a partnership between private security and the SAPS would be based on information sharing. He called for the "alignment of Private Security with SAPS operations". He also stated that private security should make a start in enhancing their own information-gathering and sharing capabilities. Collected information should be directly shared with SAPS. On 15 November 2011, this statement was endorsed by the new Minister of Police,[2] Mr Nathi Mthethwa, at the 2011 Annual Conference of the South African Security Industry Alliance (SIA). He also stated that an ongoing review and measurement of crime statistics during 2010/2011 indicated a decline in both Cash-in-Transit heists and the cash loss as a result of these heists. He acknowledged that some of these successes were achieved through the contribution of the private security industry.

Constitutionally, SAPS is the custodian of all crime information and crime intelligence. Private security service providers have a legal obligation to share crime information on threats and incidents with SAPS. Security information related to vulnerabilities and incidents of policy violations may be managed by individual private security service providers.

Specific security information management companies which operate under the auspices of Business Against Crime (BAC) share information with SAPS. They include companies such as the:

- South African Banking Risk Information Centre (SABRIC);
- Petroleum Security Initiative (PSI); and
- Consumer Goods Risk Initiative (CGRI) of the Consumer Goods Council of South Africa (CGCSA).

However, this is limited to crime incident information, strategies and actionable crime information products. Information on vulnerabilities is managed by individual private security service providers (Maree, 2010).

[2] Ministry renamed in October 2010.

Working relationships and trust need to be established among security personnel and between law enforcement and security service providers. This will help promote the sharing of security information (Nemeth, 2010: 89-90).

1.2.4 Encourage workplace investigations

In two High Court cases (of the Witwatersrand and Natal divisions) the Judges expressed their acceptance that workplace investigations can occur [See *State vs Botha and others (1) 1995 (2) SACR 598 (W);* and *State vs Dube 2000 (1) SACR 53 (N)*]. In *State vs Dube 2000 (1) SACR 53 (N), a* private investigator set a trap for an employee of a vehicle manufacturer who was suspected of being involved in thefts. The investigator arranged for meetings and negotiations with the suspect to be photographed and tape-recorded. The court found that the private investigator acted within the law. In *State vs Botha and others (1) 1995 (2) SACR 598 (W)*, the court ruled that it had not been improper for a corporation's internal investigation unit to conduct an internal investigation (in this particular case in regard to the alleged defrauding of its pension fund). The court referred to the fact that various institutions conduct their own investigations and then hand the evidence over to the police for further action and possible criminal prosecution. This development has created new opportunities for all investigators whether in private, business (corporate) or government service. All indications are that the scope will increase.

Workplace investigations will include the investigation of all crimes, security breaches and policy violations as determined by management. The Private Security Industry Regulatory Act, No. 56 of 2001 provides for the functions of an investigator in the security service.

A workplace investigation is undertaken to establish whether an act, intention to act or omission may be labelled a crime or a policy violation (Newburn, Williamson & Wright, 2008: 426). There are two broad categories of investigation processes; reactive and proactive investigations. Reactive investigations are a traditional style of investigation. It includes the collection of information in search for evidence of a crime or irregularity. The primary focus is on identifying the perpetrators. This style of investigation requires the preservation and examination of the crime scene and the

search for witnesses. It also includes the evaluation of the collected information and the analysis thereof (Newburn et al., 2008: 426-427).

Proactive investigation on the other hand is common to workplace investigators. Here the attention is on the perpetrators rather than the crime or the policy violation. The focus is on collecting information by making use of informers, surveillance and undercover operations. This style of investigation is focussed on the recovery of the financial benefits of crime or irregularities (Newburn et al., 2008: 427). Information collected during workplace investigations will enlighten management on the extent of unlawful activities and misconduct in their organisation.

1.2.5 Encourage the analysis of security information

According to Gottlieb, Arenberg & Singh (1994: 140), the analysis of crime to identify suspects, crime patterns, etc. can be traced back to the 19th century. Analysis can be done manually or through the use of computer systems (Reuland, 1997: 12). Block, Dabdoub & Fregly (1995: xiii), argue that the change from manual analysis to automated processing is important. It supplements the expertise of an experienced official. It is also because the knowledge and techniques accumulated over the years do not retire with a veteran official. They are there for others to build on.

Analysis entails analysing the exact nature of the problem and the characteristics of the incidents. Important factors to consider include where the incidents are occurring, at what times, who is involved, how and why the problem is occurring and what solutions have been tried in the past. By determining the underlying causes of the problem through the collection of detailed information, more effective strategies can be developed. Such information can come from the police, outside agencies, experts and from the community itself and even from those offenders involved in the problem (Block, Dabdoub & Fregly, 1995: 3). If information is incomplete or inaccurate, then any subsequent analysis will be unreliable (Ainsworth, 2001: 59).

There are four types of analysis most often used by law enforcement analysts. They include crime analysis, intelligence analysis, operations analysis and investigative analysis. Crime information plays a significant role in producing intelligence through

the systematic collection, evaluation, analysis, integration, and dissemination of information on criminals, especially related to their associations and their identification with criminal activity of an organised nature (Gottlieb et al., 1994: 27).

Computerised techniques are used by qualified analysts for the analysis and evaluation of collected security information. These qualified analysts use these techniques to identify system deficiencies, evaluate improvements and perform cost-versus-effectiveness comparisons. This will assist the security service provider to implement well researched physical protection systems, strategies and/or actionable information products in line with the latest security trends. The computerised analysis capability will help in providing accurate analysis results. The use of accurate computerised analysis results to reduce crime, increase detection rates and prevent losses is not unique to modern times (Garcia, 2008: 8-9).

1.2.6 Investigate the development of a Security Information Management Model (SIMM)

Advances in information management in law enforcement during the 1970's gave rise to modern intelligence practices for law enforcement. The Chiefs of Police from England and Wales in the Baumber Report, made it clear that, "intelligence" has to be understood as something more than simply information. It was also noted that "intelligence" as a modern police concept required that all collected information be put together with others and that intelligence analysis be performed in order to produce intelligence. Intelligence has since been accepted in law enforcement as the end product of a process often complex, sometimes physical, and always intellectual, derived from information that has been collated, analysed and evaluated in order to prevent crime or secure the apprehension of offenders (Newburn et al., 2008: 32).

'Intelligence-led policing' (also known as 'intelligence-driven policing'), had its origins in the United Kingdom (UK) in the 1990s, when traditional reactive methods of policing failed to cope with the rapid changes in globalisation, which had increased opportunities for transnational organised crime. The UK, National Intelligence Model

(NIM) used four elements as its tactical tasking in the implementation of intelligence-led policing. These elements focus on:

- targeting offenders (especially targeting of active criminals through overt and covert means)
- management of crime and disorder hotspots;
- investigation of linked series of crimes and incidents; and the
- application of preventative measures,including working with local partnerships to reduce crime and disorder.

The spotlight was to target the criminal and not the crime. This is because research has shown that a small percentage of repeat offenders (recidivists), commit a large amount of crime [National Crime Intelligence Service (NCIS), 2000: 14].

In the late 1990s intelligence-led policing was implemented in Australia, driven by a number of police commissioners. The local adoption included a new accountability structure at a local level, a greater integration of intelligence and investigation, and improved targeting of daily police efforts through intelligence dissemination (Ratcliffe, 2003: 1).

Intelligence is a process, incorporating a continuous cycle of tasking, data collection, collation, analysis, dissemination and feedback, prior to the next or refined task. This intelligence process is responsible for the generation of an actionable threat analysis product, which is designed to shape the thinking of the decision makers (Ratcliffe, 2009: 92).

The production of intelligence in intelligence-led policing has different stages: this includes **direction to collect intelligence**, **evaluation, collation, analysis, dissemination and feedback**. These form part of the intelligence cycle with a regular flow, whereby disseminated intelligence triggers operational responses which in turn produce new information to be fed back to the intelligence unit for new analysis and so on (Newburn et al., 2008: 203 and Ratcliffe, 2009: 105).

In practice intelligence led-policing involves the collecting of information about crime and disorder problems and using a problem-oriented policing approach to analyse the information and apply reductive interventions. The strength of intelligence-led policing as a means of collecting, storing and analysing information is in the use of computerised techniques and software that enables large amounts of data to be collected, stored and analysed and minute detail on written or visual data that might be invisible or not decipherable to the human eye. Computer software plays a vital role, as it enables accurate links to be made between many different pieces of information or incidents that, when considered in isolation might not appear serious or relevant but when linked together might reveal a more serious crime and disorder problem (NCIS, 2000: 14)

According to Clark (2010: 260-261), a Security Risk Management Cycle (SRMC) is commonly used by security service providers as mandated by management. This cycle begins with the security risk manager identifying the assets to be protected. The risks associated with the asset are prioritised. It is followed by the analysis of the effects of the risks according to probability, impact and frequency. This results in the identification of alternative actions to reduce the risks.

During the period 1995-1997, the Programme Group: Security Management at the Technikon South Africa (TSA)[3] developed a Security Risk Management Model (SRMM) for their National Diploma in Security Management and for the newly instituted (1999) BTech degree in Security Risk Management. This Security Risk Management Model which specifically addresses crime risks was built on the work of other practitioners and customised to the security industry. It has since been applied by security risk managers within the South African environment. This model is based on the following steps:

- identification of the problem of security (crime risks);
- studying the policy of the organisation and obtaining a mandate;
- conducting an orientation exercise;
- undertaking a risk analysis exercise;

[3] In January 2004 the TSA merged with the University of South Africa (UNISA) and the Programme Group became the Department of Security Risk Management which in January 2009 merged with Criminology to become The Department of Criminology & Security Science.

- conducting a security survey;
- doing a return on investment exercise to implement security risk control measures; and
- submitting a crime risk management report to top management of the company for a decision on the implementation of security measures

(Rogers, 2008: 151-154).

The SRMM was further adapted to the residential security environment with an additional step namely ‘maintenance and upgrade’ (Olckers, 2007: 103). Kole (2010: 20), further adapted the SRMM with the addition of another step, namely ‘service level agreements’ which emanated from his masters research study on the protection of petrol stations.

The SRMM is only implemented on approval and request by security management (Rogers, 2008: 151-154). Security risks are then identified using the SRMM if the need arises or if the financial situation warrants such an exercise (Kole, 2010: 16).

A greater awareness of organised criminal activity in the world has led to the growth in uncertainty and risks confronting security service providers. Garcia (2006: 2-6), feels that reducing crime, increasing detection rates and preventing losses in organisations need effective and efficient security information management practices. Currently security information management is largely done on an ad hoc, situation or individual organisation basis and in a fragmented manner without any standardisation. There is an obvious need, not only nationally but also internationally, for the standardisation of the collection and analysis of security information and the implementation of physical protection systems, strategies and/or actionable information products (Nemeth, 2010: 87).

At agency level information in the law enforcement sphere is collected, analysed and implemented in a logical and structured manner using a crime information management model. Different types of analysis products are produced using the techniques of crime analysis, intelligence analysis, operations analysis and investigative analysis. Taking into consideration the advances made in information management and the different advantages derived from the systematic management

of crime information, the researcher is of the view that a security information management model will help the security industry to reduce crime, increase detection rates and prevent losses just as it assisted law enforcement. For this to be successful security information management should be standardised and regulated in the security industry (Newburn et al., 2008: 204; Reuland, 1997: 7).

Upon taking into consideration the abovementioned intelligence/information management approaches, this study identified a Security Information Management Model (SIMM), for the management of security information in the security industry. Hopefully, it will serve as a standardised framework for the security industry in Gauteng, South Africa (refer to Paragraph 7.3).

1.3 PROBLEM STATEMENT

An issue of concern that needs to be addressed in this study is the collection, and analysis of security information and the implementation of security risk control measures in the security industry.

The collection of security information by security service providers in Gauteng is not guided by a strategic plan, organisational security strategy, security plan or a collection plan. This results in the wastage of human resources and technology to collect security information which is not need by the client. According to Garcia (2006: 1) and Garcia (2008: 26), a security plan should be used to define threats and vulnerabilities. This should direct the collection of information on the potential threats, vulnerabilities and incidents related to the threat.

In the absence of a culture of information awareness, no specific effort is made by security officials to collect security information on specific matters within a specific context to address a specific threat. The flow of security information is not continuous. Security service providers gain some understanding of the state of security of the assets they protect through formal and informal sources of information. These sources include customer contacts, incidents at the workplace and information collected using human and technical means. Information from these sources is not always comprehensive in nature. The information may sometimes be

tacitly affected by the source's own perception, knowledge, and other psychological factors. They are often forms of fragmented information that provides an inaccurate picture of the state or status of security. A security service provider can gain a comprehensive understanding of the current state of security and its deficiencies by means of security information management. Security information management will ensure that all incidents, threats and vulnerabilities are managed according to organisational standards and objectives (Johnson, 2005: 335). It is important that all the employees, security officials and clients of the organisation get involved in the collection of security information. The collection of security information in the security industry does not seem to be part of the organisational culture.

The analysis function in the security industry is mostly left in the hands of security personnel. According to Garcia (2006: 1), for the sake of accuracy, reliability and validity analysts should be employed to organise the information into a threat assessment,[4] vulnerability assessment and incident pattern analysis documents,[5] so that it becomes usable as guiding instruments. Vulnerability assessment has been used by the United States Department of State for more than thirty years. Crime Pattern Analysis (CPA), consisting of all crime incident information, helps acquaint officers with the types of crimes being committed. CPA lists the days, times and location of a crime's occurrence. It provides officers with information on any known suspects, suspect vehicle, modus operandi and lost property (Gottlieb et al., 1994: 138).[6]

Analysed results should be directed at addressing specific threats or vulnerabilities according to the organisational security strategy. According to Johnson (2005: 334), collected security information should be analysed timeously and security risk control measures should be implemented as soon as the threat or vulnerability analysis result is known. The security risk control measures may take the form of physical protection systems, strategies and actionable crime information products (Fischer et al., 2008: 173).

[4] Threat assessment is used by the South African Police Service (SAPS) and the Western Australian Police (WAP) (refer to paragraphs 5.3.1 & 5.5).
[5] Incident registers for all incidents pertaining to violation of company policy is utilised by the WAP (refer to Paragraph 5. 5).
[6] CPA is used by SAPS, refer to Paragraph 5.3.1).

This study explored the existing practices carried out by security service providers regarding the collection and analysis of security information and the implementation of security risk control measures. The study identified problems in the collection and analysis of security information and the implementation of security risk control measures. Neither a strategic plan nor a security plan is used to manage the threats confronting the organisation being protected. A collection plan is not used for the collection of security information. An organisational security strategy is not considered in the implementation of security risk control measures. Many Security Service Providers have been doing informal collection, analysis and the implementation of security risk control measures for many years. However, they still do not have a standardised framework to guide them in this regard.

1.4 RESEARCH QUESTIONS

The following research questions were applied in this research:

- What is the "*status quo"* of the collection and analysis of security information and the implementation of security risk control measures in practice?
- What is the nature and extent of problems experienced in the collection and analysis of security information and the implementation of security risk control measures?
- Which solutions should be implemented to address the problems experienced in the collection and analysis of security information and the implementation of security risk control measures?

The research questions specify exactly what the researcher studied (security information). It clearly indicates on what the researcher wanted to focus on (collection and analysis of security information and the implementation of security risk control measures). The research questions were applied to establish the status quo of the collection and analysis of security information and the implementation of security risk control measures. To also identify the nature and extent of problems experienced by security officials and to find solutions to address the problems.

1.5 RESEARCH GOAL

Based on the problem statement and research questions there was a need to explore the management of security information in the security industry.

1.5.1 Research objectives

This study explored the management of security information in the security industry by undertaking the following:

- establishing the '*status quo'* of the collection and analysis of security information and the implementation of security risk control measures in practice;
- identifying the nature and extent of problems experienced in the collection and analysis of security information and the implementation of security risk control measures; and the
- discovery of a new Security Information Management Model (SIMM).

1.6 DEFINITIONS

In exploring a complex operational phenomenon, such as the 'Security Information Management', it is important to begin by developing an understanding of the various relevant concepts.

1.6.1 Private Security

Private security refers to those efforts by individuals and organisations to protect their assets from loss, harm or 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).

1.6.2 Security service

"Security service" means one or more of the following services or activities:

- protecting or safeguarding a person or property in any manner;
- providing a reactive response service in connection with the safeguarding of a person or property in any manner;
- giving advice on the protection or safeguarding of a person or property or the use of security equipment;
- providing a service aimed at ensuring order and safety on premises used for sporting, recreational, entertainment or similar purposes;
- manufacturing, importing, distributing or advertising of monitoring devices contemplated in Section 1 of the Interception and Monitoring Prohibition Act, No. 127 of 1992;
- providing services related to the functions of an investigator;
- providing security training or instruction to a security service provider or prospective service provider;
- monitoring signals or transmissions from electronic security equipment;
- installing, servicing or repairing security equipment;
- performing the functions of a locksmith; and
- managing, controlling or supervising the rendering of any of the above services [Private Security Industry Regulatory Act, No. 56 of 2001: Section 1 (1)].

1.6.3 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 2001).

1.6.4 Security

“Security implies a stable, relatively predictable environment in which an individual or group may pursue its ends without disruption or harm and without fear of disturbance or injury” (Fischer et al., 2008: 31).

1.6.5 Management

Management may be defined as the process of planning, organising, leading and controlling the resources of an organisation to achieve the stated organisational goals as productively as possible (Smit & Cronje, 2002: 9).

1.6.6 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.

1.6.7 Risk analysis

Addison (2002: 2), describes risk analysis as a form of security assessment. It focuses on the process of identifying the risks and their causes. It determines the consequences of the risks and their causes. It calculates the probability and impact of their occurrences**.**

1.6.8 Information

Information relates to any information, which you can hear (directly or indirectly), taste, smell, read, touch or see. It also includes rumours and so called “stories” (Van Rooyen, 2008: 218).

1.6.9 Security information

“Security information may be defined as any information on incidents, threats or vulnerabilities which has the potential to exploit an asset or group of assets and thereby cause losses to an organisation” (Blyth & Kovacich, 2006: 25).

1.6.10 Information collection

Information collection is the act of collecting information that will enable an analyst to make a recommendation on the implementation of physical protection systems, strategies and/or actionable information products to mitigate security risks (Peterson, 1994: 270).

1.6.11 Incident

Incident information refers to information of any event or occurrence resulting from a threat or policy violation (Allen, 1992: 597).

1.6.12 Threat

An individual or group with the motivation and capability for crime, terrorism, foreign intelligence, commercial or industrial competition and maliciousness or other malevolent acts that would result in loss of assets at a facility is a threat (Garcia, 2001: 302). A threat refers to anything that has the potential to prevent and hinder the achievement of objectives or disrupt the processes that support them (Talbot & Jakeman, 2008: 141).

1.6.13 Vulnerability

Vulnerability refers to an exploitable capability or an exploitable security weakness or deficiency at a facility of security interest. Exploitable capabilities or weaknesses are those inherent in the design (or layout) of the facility and its protection or those existing because of the failure to meet (maintain) prescribed security standards when evaluated against requirements for defined threats. If the vulnerability were detected

and exploited by an adversary, then it would reasonably be expected to result in a successful attack causing damage to the facility (Garcia, 2001: 303).

1.6.14 Analysis

Analysis is the reviewing of data and the comparison of it to other data to determine its meaning or relation to other data. This includes different forms of analyses such as evaluation, collation, threat assessment, vulnerability assessment and criticality assessment (Peterson, 1994: 270).

1.6.15 Evaluation (verification)

Evaluation (verification) of security information is the assessment of the reliability of the source and the quality of the information (Jordaan, 2003 (a): 59).

1.6.16 Collation

Information collation is the sorting, indexing and storing of information into a format from which it can be retrieved and analysed (Lyman, 1988: 153).

1.6.17 Threat analysis

It is a process in which information about a threat or potential threat is subjected to systematic and thorough examination in order to identify significant facts and derive conclusions there from (Garcia, 2001: 302).

1.6.18 Threat assessment

Threat assessment is a judgment, based on available intelligence, law enforcement and open source information, of the actual or potential threat to one or more assets (Garcia, 2001: 302). According to Le Roux (2004: 26), threat assessment is the identification of potentially undesirable events that could result in loss or harm.

1.6.19 Vulnerability analysis

Vulnerability analysis is a method of identifying the weak points of a facility (Garcia, 2001: 303).

1.6.20 Vulnerability assessment

It is a systematic evaluation process in which qualitative and/or quantitative techniques are applied to detect vulnerabilities and to arrive at an effectiveness level for a security system to protect specific targets from specific adversaries and their acts (Garcia, 2001: 303). A vulnerability assessment involves a process or outputs associated with reviewing assets and or security systems to identify weaknesses. Usually conducted from a baseline on how they could fail or be successfully attacked (Talbot & Jakes, 2008: 150).

1.6.21 Criticality assessment

Criticality assessment attempts to prioritise organisational infrastructure, assets or elements by the relative importance or dependence on that element. In practice this is often related to the magnitude of downstream impacts created by the element's destruction or disablement. Criticality assessment may be based on the magnitude of potential casualties, long term effects on organisational objectives and economic or socio-political impacts (Talbot & Jakes, 2008: 154).

"The term has been defined as the impact of a loss as measured in Rands". In addition to the cost of the item lost it also includes replacement costs, temporary replacement, downtime, discounted cash, insurance rate changes and the loss of market place advantage (Fischer et al., 2008: 157-158).

1.6.22 Physical Protection Systems

Measures implemented for the protection of assets or facilities against criminals, terrorists, foreign intelligence services, commercial or industrial competitors, malicious people or other malevolent attacks (Garcia, 2001: 298).

1.6.23 Strategies

Overall methods planned by the adversary to achieve objectives (Garcia, 2001: 301).

1.6.24 Actionable information products

Strategic actionable information products are generally research oriented, involving inferential and multivariate statistics; they include crime trend forecasts, resource allocation and situational analysis. Tactical actionable information products involves pattern detection, linkage analysis for suspect-crime correlations, target profiling and offender movement patterns (Goldsmith, McGuire, Mollenkopf & Ross, 2000: 5).

1.6.25 Dissemination

Dissemination is the release of recommendations for the implementation of physical protection systems/strategies and/or actionable information products to a client under certain conditions and protocols (Peterson, 1994: 269).

1.6. 26 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. For the purpose of this study it will include physical protection systems, strategies and actionable information products.

1.6.27 Feedback

Feedback is the informing of the analyst of the outcome of the implementation of specific physical protection systems/strategies and/or actionable information products (Reuland, 1997: 36).

1.7 OUTLINE OF THE THESIS

Chapter 1: Introduction and motivation for the research

This chapter introduced the rationale for the study, problem statement, research questions, research goal, research objectives, definitions of concepts and the outline of the thesis.

Chapter 2: Methodological exposition of the research design

This chapter discusses the methodological framework, guiding assumptions, limitations, value of the research and ethical considerations.

Chapter 3: Grounded theory: Generating categories and coding the data

This chapter focuses on the analysis of the data from the semi-structured and focus group interviews. The open, axial and selective coding procedures were used to generate a grounded theory.

Chapter 4: Security information management

This chapter provides a comprehensive literature study on the collection and analysis of security information and the implementation of security risk control measures.

Chapter 5: Case studies on security information management

In this chapter the case studies on Security Information Management in South Africa and Security Information Management in Perth, Western Australia are discussed. It identifies present-day standards.

Chapter 6: Data analysis of questionnaires

This chapter provides an analysis and interpretation of the survey questionnaires by using the univariate analysis process.

Chapter 7: Security Information Management Model: The Concept

This chapter discusses the development of a practical Security Information Management Model (SIMM). The model is aimed at providing a standardised framework for the collection and analysis of security information and the implementation of security risk control measures.

Chapter 8: Findings and recommendations

This chapter discusses findings and recommendations of this study.

1.8 CONCLUSION

This study took into account government departments and other private organisations where private security officials are employed to provide a security service. Security was considered from an objective, subjective and symbolic perspective within these environments. The management of crime information and crime intelligence served as pillars in understanding the importance of security information management. The intelligence and crime information cycles used by law enforcement was used as a source of theory, discipline and practice in the investigation of a Security Information Management Model (SIMM) for the security industry.

CHAPTER 2

METHODOLOGICAL EXPOSITION OF THE RESEARCH DESIGN

2.1 INTRODUCTION

The researcher followed the mixed methods approach using the exploratory mixed methods design in the research. The study explored the phenomenon (security information management) by using qualitative data and then testing it quantitatively in a questionnaire survey (Delport & Fouché, 2011: 441).

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

The grounded theory and case study research designs were used for qualitative data collection (Fouché & Schurink, 2011: 318-320). The data for the grounded theory design was collected using semi-structured one-on-one interviews and focus group interviews (Greef, 2011: 351-361). Semi-structured interviews were conducted using an interview schedule (See Appendices 1and 2). Senior managers from selected service providers and other stakeholders from the security services sector in the Gauteng province in South Africa were targeted for these interviews. Focus group interviews were conducted with security officers, supervisors and managers employed in Gauteng (See Appendix 5). This data was analysed using open, axial and selective coding procedures in an attempt to deliver a substantive grounded theory (Fouché & Schurink, 2011: 319-320). The researcher used interviews and focus groups to generate a substantive grounded theory. The purpose for using the case study design was to obtain a better understanding of security information management and the present day standards used by organisations. It facilitated the researcher's gaining of knowledge about security information management both nationally and internationally (Fouché & Schurink, 2011: 322). Interviews were primarily used in the case study design.

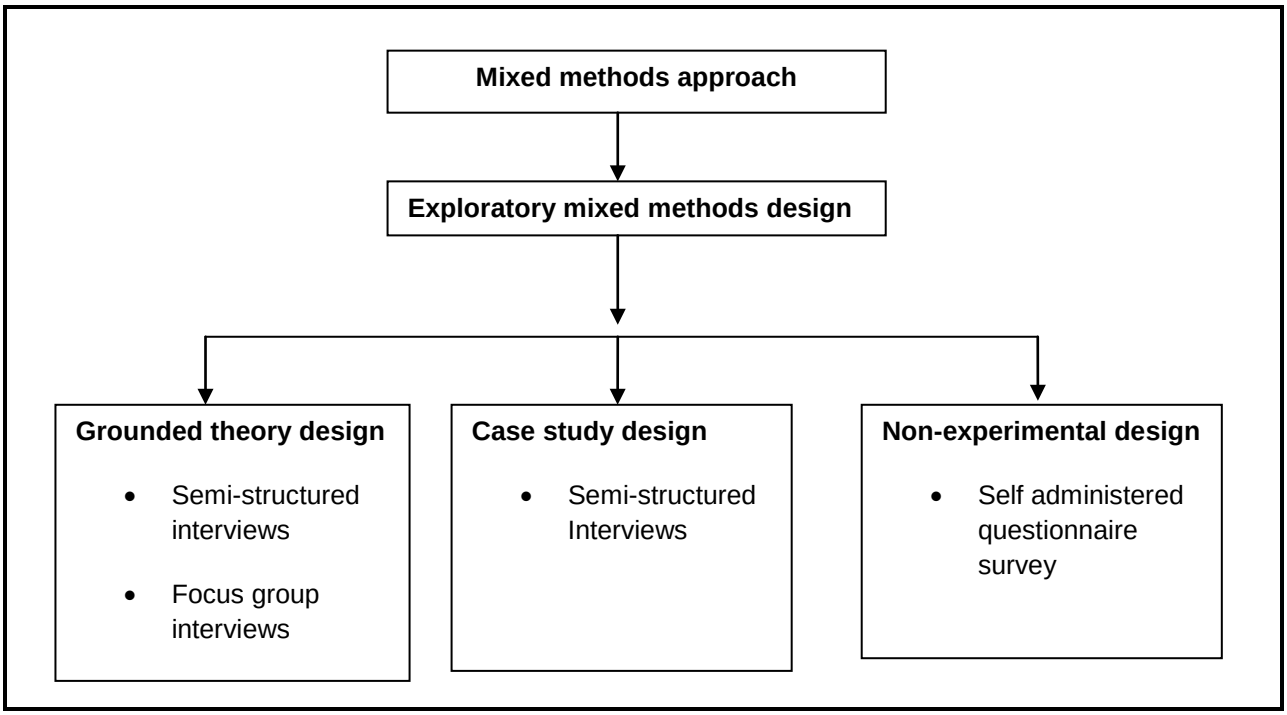
Surveys were used in the non-experimental research design to collect quantitative data for this study (Fouché, Delport & De Vos 2011: 155-156). The quantitative data was collected using a questionnaire as an instrument (See Appendix14). Responses from the semi-structured interviews helped to facilitate the development of the questionnaire with closed- and open-ended questions. The questionnaire was used to evaluate the collection and analysis of security information and the implementation of security risk control measures by security service providers in Gauteng. The data analysis of the questionnaires was done using the mixed method data analysis strategy. The univariate analysis process was used to quantitatively analyse and interpret the data in the questionnaires (Kruger, De Vos, Fouché & Venter, 2007: 217-245).

This chapter provides a discussion on the methodological exposition of the research design. It puts specific emphasis on the methodological framework, guiding assumptions, limitations and the value of the research.

2.2 METHODOLOGICAL FRAMEWORK

The researcher designed Figure 2.1 to provide an understanding of the methodological process used in this research.

Figure 2.1: Methodological process



The researcher used the mixed methods approach because it involved both the qualitative and quantitative approaches. The rationale for using the exploratory mixed methods design was to first explore the management of security information in the security industry before attempting to measure it quantitatively. It was used to seek convergence and corroboration of results from different methods and designs studying the same phenomenon. The exploratory mixed methods design was selected based on the research objectives, researcher's expertise and available resources. Consideration was also given to the timing and the weight of the quantitative and qualitative approaches as well as the approach in mixing the two data sets. The mixed methods approach enabled the researcher to simultaneously address a range of confirmatory and exploratory questions. The answers helped to generate and verify the grounded theory.

The sampling strategy stemmed logically from the research objectives and the research questions being addressed by the study (Delport & Fouché, 2011: 444-446). In planning this study it was important for the researcher to consider the different world views in the social sciences research process for both the qualitative and quantitative approaches (Fouché & Delport, 2011a: 70).

Three world views were used in this study, the world of everyday life, the world of science and the world of meta-scientific reflection (Mouton, 1996: 7-12). The mixed methods research encourages the use of multiple worldviews rather than the typical association of certain paradigms for quantitative researcher's and others for qualitative researchers (Delport & Fouché, 2011: 436).

Aspects important to the methodological framework are discussed. in the sections below

2.2.1 Exploratory mixed methods design

The exploratory mixed methods design was the most appropriate to explore the management of security information in the security industry. The exploratory mixed methods design worked well in this study, as the researcher needed to explore the concept "management of security information" in the security industry by using qualitative data before attempting to test it quantitatively. It was a two-phase design. Interviews and focus groups were used in South Africa as well as in Western Australia for the collection of information. The collected information was used to design the questionnaire for the quantitative study. The mixed methods design helped the researcher to find more accurate knowledge on how security information is managed in the security industry.

The researcher collected qualitative data from selected security managers, security officials and other stakeholders of their own description of security information management concepts; and their practical experiences with security information management. Data was collected through one-on-one interviews in the form of written and spoken language using semi-structured interview schedules and through focus group interviews. The data was analysed by identifying and categorising the data into generalised themes and categories. This allowed the researcher to study selected issues in depth, openness (transparency) and detail, as he identified and understood the categories of information that emerged from the data. The study was flexible; data collection was less structured and more accessible. This helped to dimensionally reduce the data into sub properties, for example the category 'sources used to collect security information'; its properties include open and closed sources

of information. Thus, open sources can include public documents and closed sources may include classified documents. Each of these documents can be further dimensionalised, if analysis calls for it. The researcher was able to make any necessary adjustments straight away. This allowed for the whole study to be more flowing, naturalistic, participatory and interpretive.

The grounded theory, the case study and the non-experimental quantitative research designs were used within the context of the exploratory mixed methods design. The qualitative data from the semi-structured and focus group interviews facilitated the development of a questionnaire. The questionnaire was used in the non-experimental design (Fouché et al., 2011: 144; Kerlinger, 1986: 294-295). The data from the grounded theory design and the non-experimental design together with the present day standards from the case study design and literature study were integrated, correlated and interpreted. This resulted in the findings and recommendations for this study.

2.2.1.1 Grounded theory design

The grounded theory design is concerned exclusively with the generation, rather than the testing of theory. It is positioned at the most extreme end of the continuum – after data collection (Creswell, 2007: 239). This required the researcher to collect and analyse data to generate a theory. According to Leedy & Omrod (2005: 140), the term “grounded” refers to the idea that theory is derived from and “grounded” in data that has been collected in the field. Patton (2002: 129), states that: “one of the strengths of the grounded theory is the inductive, naturalistic inquiry strategy of approaching a setting without any predetermined assumptions.” Grounded theory approaches aim to develop an often situation-specific emergent theory founded upon the interpretation and analysis of the actual research findings. In other words, as a research design, grounded theory seeks to generate a theory from (i.e. ‘grounded’ in) the empirical material through the ongoing interpretation of that material. However, the problem was how to approach the field of research in this study with an open mind by not having any pre-conceived theories or hypotheses. The sole purpose was to generate theory in this study by utilising the grounded theory design.

The researcher decided to use the grounded theory design within the interpretive research perspective of the qualitative approach (Straus & Corbin, 1990: 23). The reason being that this perspective makes the assumption that reality should be interpreted through the meaning that the research participants give to their life world. The ontology of the interpretive research perspective is that the real world can be discovered by means of a systematic, interactive methodological approach. Its epistemology is that knowledge will arise from the understanding of symbols and meaning through interaction. Ontology is the study of real world. In the qualitative approach the mind of a participant is referred to as the research domain (Mouton & Marais, 1990: 12). It has stocks of knowledge that we use in everyday life. It enables us to cope effectively with our daily tasks. This is the knowledge we have acquired through learning, experience, social interaction and self-reflection. Epistemology assumes that genuine knowledge must necessarily be certain and incorrigible knowledge. It should be subject to verification (Mouton & Marais, 1990: 14). Data for this study was collected according to this perspective by means of semi-structured and focus group interviews and systematically analysed and verified (Fouché & Schurink, 2011: 308-312).

The grounded theory design was used in this study to derive a general abstract theory of a process, action and interaction grounded on the views of participants. This process required the use of multiple stages of data collection and the refinement and interrelationship of categories of information. Data from the semi-structured and focus group interviews were simultaneously coded using the open coding, axle coding and selective coding procedures. This helped the researcher to reach a point where a theory emerged. Two primary characteristics of this design were the constant comparison of the data with emerging categories and the theoretical sampling of different groups to maximise the similarities and the differences of information (Creswell, 2009: 13).

2.2.1.2 Case study design

In contrast to the grounded theory design, the case study design was used to study present day standards in security information management both nationally and internationally. The researcher decided on using the collective case study type,

which according to Fouché and Schurink (2011: 322), “is an instrumental case study which may be extended to a number of cases.” The reason for using the collective case study type was to learn more about present day standards being used in other similar organisations. More specifically, to get to know how security information is managed both nationally and internationally. The case study design was used to explore, in-depth, the present day standards used by security service providers both in Gauteng, South Africa and in Perth, Western Australia. During the case study the researcher collected detailed information through interviews and observation. To do this, the researcher needed access to and the confidence of the participants. The end product of this exercise was an in-depth description of the processes used in security information management. The researcher conducted the case study research with sufficient background knowledge of the relevant security service provider, which helped to validate the responses.

2.2.1.3 Non-experimental quantitative research design

Fouché et al. (2011: 144), state that, “quantitative research designs may be classified into two main classes, namely experimental designs and non-experimental designs.” A researcher may carefully choose a research design to obtain appropriate data for investigating specific research questions. The non-experimental quantitative research design was chosen to conduct the self-administered questionnaire survey. Different categories of security service providers were selected to take part in the questionnaire survey. They were measured on all the relevant variables at a specific time and at a specific place. No manipulation of variables could take place, as a structured questionnaire was used to measure the variables. This design did not involve an experimental or control group.

2.2.1.4 Literature review

Literature review means locating and summarising the studies about a topic. The use of literature varies considerably depending on the research being conducted. There is no single way to conduct a literature review. Many students busy with literature research study proceed in a systematic fashion to capture, evaluate and summarise the literature (Creswell, 2009: 28-29). The review of literature has different purposes

and strategies depending on whether the researcher is conducting a quantitative or qualitative research project (Fouché & Delport, 2011: 133).

The researcher decided on doing literature review during the title choice, designing the research questions and to validate statements. This also included a search for present day practices and to verify knowledge. It is therefore important that the research produces statements that are highly probable and for which the highest standard of inductive support, substantiation or confirmation could be demonstrated.

The researcher searched different fields of study such as law, criminology, sociology, psychology, policing, private security, security services, investigation of crime and workplace investigations. The researcher also consulted within the Private Security Industry and at Crime Information Management Centre (CIMC) of the SAPS for literature on the same topic as the research. None of these sources revealed any literature on the same topic as the research.

The researcher then divided the research topic into key concepts namely: collection and analysis of security information and the implementation of security risk control measures and repeated the above processes. In doing this, the researcher found literature relevant to the study. The researcher studied this literature to search for best practices in the national and international arena. On finding literature relevant to collection and analysis of security information and the implementation of security risk control measures, the researcher created a literature map and then summarised the relevant articles, assembled them, structuring them thematically in an organised fashion. The researcher ended the literature review with a summary of the major themes and suggested how the particular study further adds to the existing pool of knowledge.

2.2.2 Demarcation

The Province of Gauteng in the Republic of South Africa was demarcated as the geographic area for this study. The reason was that most sectors of the security service are situated in Gauteng. They also operate as major security service providers in Gauteng with the highest number of operators nationally.

The study involved private and government security service providers in Gauteng. They were divided into different sectors according to the security service function they performed. They included security officials from the following sectors:

- protection services;
- in-house security;
- retail;
- public service entities;
- mining;
- contract companies;
- financial institutions;
- insurance companies;
- city and metropolitan councils;
- industrial sector; and
- transport.

Security managers, security officials and stakeholders from the security industry in the Province of Gauteng were sampled for the study. The research involved 12 senior managers and 114 operational security officials employed by these sectors. Three focus groups consisting of an average of 12 persons per focus group were selected from the different security sectors in Gauteng.

Three South African security information management companies from Gauteng and security representatives from Gauteng, South Africa and a comparative group from Perth, Western Australian were also sampled for the case study. Specific individuals were also identified for purposive interviews due to their experience and positions they hold in academia, professional bodies, security companies and law enforcement.

2.2.3 Research techniques

It was important to understand the reality in the security services environment. It was therefore necessary to study the collection and analysis of security information and the implementation of security risk control measures in all major categories of the

security service in Gauteng. Security information management was researched at a descriptive level using interpretive and application techniques (Mouton, Marais, Prinsloo & Rhoodie, 1985: 44).

2.2.3.1 Descriptive

The descriptive level was used to describe specific facts, observations and actions in this study. The study was focussed on the researcher's contribution to the science of security (Mouton et al., 1985: 44). According to Van Heerden (1982: 7), "the application of science is not science itself, but merely the utilisation of scientific information in practical circumstances. An applied science, in contrast, takes conclusions that have been researched in other sciences, processes them in a scientific context which is distinctively its own and makes the resulting scientific knowledge available to the professional practitioner." Since the security service function is a matter of fulfilling a specific social and economic function, the applied character of the subject is self-evident.

2.2.3.2 Interpretive

The study included the researcher's interpretation of the qualitative data during and after data collection. The researcher was assisted by a statistician in analysing and interpreting the quantitative data. The interpreted data was related meaningfully to the research objectives and the research questions. It was also used to make findings and recommendations.

2.2.3.3 Application

This evaluation inevitably focussed on the findings and recommendations for the purpose of application. Purposive conversations with fellow researchers, academics from the University of South Africa (UNISA) and Edith Cowan University (ECU), experienced security officials and members of professional bodies and regulatory agencies were used to support and confirm the findings and recommendations for the purpose of application.

2.2.4 Population and sampling procedures

According to Strydom (2007: 194), “a sample, thus comprises elements of the population considered for actual inclusion in the study. It can be viewed as a subset of measurements drawn from a population in which the researcher is interested.”

Whitt (1991: 410), is of the view that; “decisions about whom to interview or what to observe should be based not only on the aim of the research but also on the potential of the person or event to help the researcher gain insight and understanding about the phenomena”.

In order to establish the size of the research group the view is that it should be a proportional representative of the universe. The perception also exists that it is not the size of the research group that determines the reliability, but rather if the research group is representative of the universe (Van Vuuren, 1992: 9). Le Roux (2004: 12) agrees with Van Vuuren, that no guarantee can be given that the representative group are in all respects representative of the whole security community or that the results will stay unchanged unless the security community is involved with this investigation.

The entire number of security officials from the security service in South Africa was the universe of this study (refer to Paragraph 1.3.2 supra). According to Bailey (1987: 81-82), “universe includes all individuals or cases of a certain type.” Ideally, the researcher would have liked to study the entire universe, to give more weight to the findings. Due to financial, time and other constraints, the researcher could not study the entire universe. The researcher decided to choose the security officials from the security service in Gauteng as the study population for this research. Population, on the other hand, is a term that sets boundaries on 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, Meenaghan & Toomey, 1985: 235).

According to Steyn (2002: 71), results of a research study can be generalised to groups that participated in the research. 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 the security industry of the Gauteng province and not to generalise the findings to the security industry nationally. National generalisation was not of concern in this research, because there was clearly scientific value to gain from investigating some single category of individuals or group. However, whenever research is undertaken, the findings should not only be generalised to fit the specific individual; group or event studied but also to generally provide an understanding about similar individuals, groups and events. Since it is not a pure quantitative study with random sampling, generalisation is not at all an objective of the study (Berg, 2009: 330). The sample groups selected for the case studies and the interviews were valid, representative and selected without any bias.

The researcher used non-probability sampling together with the purposive, convenience (accidental) and snowball sampling methods, to select representative groups for this study (Strydom, 2007: 202). It can be said that the representative groups in this study are in all probability accurately representative.

2.2.4.1 Semi-structured interviews

It was decided to limit the study population by doing non-probability sampling using the purposive sampling method. Purposive sampling is based entirely on the judgment of the researcher (Strydom, 2007: 202). Researchers rely on their own experience, ingenuity and/or previous research findings to select participants in such a manner that the sample obtained may be regarded as representative of the relevant population (Le Roux, 2004: 12). In this study the researcher used two basic criteria to purposively sample security service providers for the semi-structured interviews. The first criterion was based on the kind of security service being provided by the security service provider. The researcher considered the security service provided in terms of the Private Security Industry Regulation Act, No. 56 of 2001, registration with PSIRA, reputation of the business entity, period of existence of the security service provider and the environment in which they provide security service/s. The second criterion was that of representativeness or typical attributes for

example, senior security officers in management positions. The judgment of the researcher was a prominent factor in this type of sampling.

Twelve security service providers were identified for the semi-structured interviews from the following sectors:

- protection services;
- in-house security;
- retail;
- public service entities;
- mining;
- contract companies;
- financial institutions;
- insurance companies;
- city and metropolitan councils;
- industrial sector; and
- transport.

The researcher also used his own judgment and identified police officers from the SAPS, other stakeholders and academics using the purposive sampling method. They were selected according to their official capacity, experience and their potential contribution to the study.

The concept “sufficiency” was used as the criteria to determine the number of participants as a sufficient number for the semi-structured interviews. A sufficient number was needed to reflect the range of participants and sectors that made up the population. This provided those outside the sample with a chance to connect to the experience of those in it (Greef, 2007b: 294).

2.2.4.2 Focus group interviews

Security officers from Gauteng were used as the population for the focus group interviews. It was decided to limit the study population by doing non-probability sampling using the purposive sampling method. The purposive sampling method

was used to select a representative sample of private security officials registered with PSIRA and employed as a security official in Gauteng. The sample group was considered representative of the population, because all private security officials are registered in terms of the same policy requirements, undergo the same or similar training and function according to the same policy and standards nationally (Private Security Industry Regulation Act, No. 56 of 2001). According to Strydom, (2007: 202) purposive sampling is based entirely on the judgment of the researcher. The sample group should be composed of elements that contain the most characteristics and representativeness or typical attributes of the population. In this case the sample group were all registered security officials, performing a security service in Gauteng.

The researcher held three collective interviews with focus groups consisting of at least 12 persons per focus group.

2.2.4.3 Case study

The semi-structured interviews were used to identify security information companies that manage security information (crime incidents, threats and vulnerabilities) for the specific security sector. This also helped to create a link with the specific security sector and the company identified for the case study. According to Baker (1988: 159), the snowball sampling method in non-probability sampling, involves approaching a single case that is involved in the phenomenon to be investigated in order to gain information on other similar cases. In turn this person is requested to identify further people who could make up the sample. In this way the researcher proceeded until he had identified a sufficient number of cases to make up the sample.

The researcher looked for companies' co-ordinating crime incident information, threats and vulnerabilities. The researcher could not find any company that manages security information on threats and vulnerabilities for security service providers. This function had to be done individually by the different security service providers, using their own in-house personnel (contracted individuals), resources and skills. However, there was several companies managing crime incident information for specific security service providers for example the banks, petroleum and oil companies,

insurance companies, tourism industry, retailers and casinos. Owing to a limited number of such companies being well established and organised only three security information management companies were selected for the case study. Non-probability sampling using the purposive sampling method was used to delimit the companies for the purpose of this study.

The identified companies were aligned to their clients in the semi-structured interviews. This was done to draw specific inferences on their line of communication and impact on crime relevant to the specific service provider; for example bank robberies, petrol station robberies and business robberies at retail stores.

The information received in the case studies also reached saturation, whereby any further case study with similar companies would have resulted in the repetition of the same practices. This is because all the security information management companies perform the same functions and provided the research with similar information on their practices for security information management.

2.2.4.4 Questionnaire survey

Security officials from Gauteng were identified to complete the self-administered questionnaires from the following sectors:

- in-house security at ‘security’ estates/villages;
- residential and commercial complexes;
- financial and insurance institutions;
- petroleum and oil companies;
- retail;
- mining;
- government departments;
- casinos;
- public service entities;
- university campuses; and
- contract security service companies.

It was decided to limit the population by doing non-probability sampling by using the accidental sampling method to interview security officials employed by the different sectors of the security industry in Gauteng. Strydom (2011: 232), refers to accidental sampling as a convenient, availability or haphazard sample and adds that the respondents are usually those who are nearest and most easily available. The accidental sampling procedure was applied to all security officials registered with PSIRA and employed by these security service providers, who were easily accessible to the interviewer. All such security officials were included in the sample until the desired number was obtained. The researcher used this procedure to ensure that the different groups or segments of the population acquired sufficient representation in the sample. The sample for this study consisted of security officials who were easily accessible to the interviewer.

2.2.5 Data collection

According to Leedy and Ormrod (200: 158), qualitative researchers may use multiple forms of data collection methods in any single study. Different kinds of data collection methods – interviews, case study and literature study were used in this study. Delport and Roestenburg (20: 171), state that: “quantitative data-collection methods often employ measuring instruments.” In the social and human sciences, “measuring instruments” refers to such instruments as structured observation schedules, structured interviewing schedules, questionnaires, checklists, indexes and scales. A questionnaire was used in this study as a quantitative data collecting method. All biases were acknowledged in the research report, so that readers could take them into account when reading the report. Mixed method research eliminates different kinds of bias, explains the true nature of the phenomenon under investigation and improves various forms of validity or quality criteria (Delport & Fouché, 2011: 436).

According to Greef (2007b: 293), qualitative studies typically employ different types of interviews in research. Since interviews are one of the most commonly recognised forms of the qualitative research method the researcher used the semi-structured interviews for one-on-one interviewing. Semi-structured interviews were also used in the case studies to identify present day practices in South Africa and Australia.

Focus groups were used for collective interviews. Self-administered questionnaires were used as a quantitative data collection method. A literature study was referred to for present day standards both nationally and internationally.

2.2.5.1 Semi-structured interviews

The semi-structured interviews were piloted with Chief Executive Officers (CEOs) of companies who had extensive national and international experience in the security service. Some of these CEOs are managing a chain of security companies in Gauteng. The pilot study helped to understand some of the practical aspects of establishing access, making contact and conducting the interviews, as well as becoming alert to one's own interviewing skills (Greef, 2007b: 294).

Twelve senior managers from the Security Service in Gauteng were identified by their CEOs for semi-structured interviews. Face-to-face interviews were conducted with the senior managers using an interview guide to direct the interview. Questions for the interview guide were derived from the research questions and literature study. The questions consisted of main questions, probing questions and follow up questions relevant to the research questions. The interview was focussed and discursive. It allowed the researcher and the participants to explore the collection and analysis of security information and the application of security risk control measures (Greef, 2007b: 293).

The semi-structured interviews assisted the researcher to obtain an understanding of the existing practices being used by security service providers in Gauteng. The interviewer had the advantage of building empathy between himself and the interviewee, resulting in greater involvement and better quality data (Robson, 2000: 90). Even if this did not occur, the interviewer was in a position to assess the degree of the interviewee's interest and involvement. Data obtained under these circumstances could be more easily compared, with less risk of bias occurring, as different people are asked the same questions.

Semi–structured, one-on-one interviews were used to gain a detailed picture of the nature and extent of problems being experienced in the collection and analysis of

security information and the implementation of security risk control measures. Interview guide used for the semi-structured interviews is attached (See Appendix 1). Consent forms were also completed by both the interviewee and the researcher, to conduct the semi structured interviews with the necessary confidentiality (See Appendix 2.

Purposive interviews were also carried out with the SAPS, other stakeholders from the security service environment and academia to determine individual perceptions, opinions, facts, forecasts and their reactions to initial findings and potential solutions (Greef, 2007a: 202). The purpose was to understand the experience of security managers and other stakeholders in the collection and analysis of security information and the implementation of security risk control measures (Greef, 2007b: 293). Letter requesting permission from SAPS together with approval letter are attached (See Appendices 3 and 4).

2.2.5.2 Focus group interviews

Focus groups were used to evaluate the collection and analysis of security information and the implementation of security risk control measures in the security service. Participants were selected from among security officers registered with PSIRA and employed by security service providers in Gauteng. The researcher decided to hold focus group discussions at a neutral setting. It is believed that this type of setting would motivate respondent participation. The focus group discussions were held at the UNISA campus in Pretoria, Gauteng.

The focus group discussion was facilitated by the researcher, with the assistance of a scribe who took notes. The focus group discussion started by the researcher introducing himself as the facilitator. The scribe was introduced to the participants. The facilitator outlined the purpose of the focus group discussion. All participants introduced themselves and mentioned the security service provider they work for in Gauteng. Participants were informed that if they felt uncomfortable or felt the questions were becoming too sensitive, they could exit the focus group discussion at any time.

The researcher used questions, consisting of main questions, probing questions and follow-up questions relevant to the research questions (Greef, 2007b: 293). The questions posed to the participants were in everyday, non-professional language to generate rich descriptions and authentic data. The focus group discussions were also audio-taped for future reference. Throughout this process the researcher's essential motivation was a desire to listen and learn from the participants. It helped the researcher to explore the collection and analysis of security information and the application of security risk control measures. It also helped uncover new facts and to understand the practices within the security environment. The researcher also understood how security officials interpreted security information management concepts in practice. There was an atmosphere of trust and openness. Participants shared their experiences voluntarily.

Focus group responses were used as a supplementary source of data to the semi-structured interviews conducted with an interview guide (Morgan, 1997: 2). This method of collective interviewing with security officers from Gauteng was used to validate the semi-structured interviews.

According to Greef (2011: 370), pilot testing focus group questions is difficult, because questions used in focus group interviews are hard to separate from the environment of the focus group. A pilot test was still conducted by testing the first focus group with the participants. There were no shortcomings identified.

Interview guide used to facilitate the focus group interviews is attached (See Appendix 5).

2.2.5.3 Case Study

In conducting semi-structured interviews with senior managers from the security industry in Gauteng, all information was recorded using a tape recorder and in the field journal of the researcher, for easy reference during the interpretation and analysis phase of the research. Further meetings were held to clear ambiguities or to request any additional documentation. During the course of conducting these interviews, the researcher learnt of specific security information management

companies in South Africa. These are security information management companies such as the South African Banking Risk Information Centre (SABRIC), Petroleum Security Initiative (PSI) and the Consumer Goods Risk Initiative (CGRI). These security information management companies provide strategies and/or actionable crime information products to clients, partners and stakeholders to mitigate specific security risks. There are a limited number of such companies in South Africa. Many of them are in their infancy, not fully established and organised. This made it difficult for the researcher to obtain approval to conduct research at such companies. Some of the companies refused to assist in this study, because of the sensitive nature of the information handled by them.

It was decided to conduct case studies with well-established companies who manage security information on incidents, threats and vulnerabilities. Specifically those that have been in existence for a reasonable period of time. Interviews were arranged with specific managers of the companies with written permission from the respective CEOs. Semi-structured interviews were conducted. Documentation such as policies and operating procedures, information flow documentation and actionable crime information products were also reviewed. Site observation was also conducted at the facilities, checking on how information is received, analysed and prepared for application in the form of strategies and actionable crime information products. These companies managed security information on crime incidents and not on threats and vulnerabilities.

The case study strategy was used to explore the activities of such companies for best practices, processes and models. It helped obtain a better understanding and insight of the current practises in security information management companies.

It is not the primary responsibility of these security information management companies to collect crime information. However, some of the information management companies collect information to enrich the data on hand. The responsibility to provide information on crime incidents rests with their clients. The security information provided to these companies is on daily crime incidents that take place at the business sites of their clients. These security information management companies are responsible for security information management, analysis and

providing strategies and/or actionable crime information products for application by their clients, partners and stakeholders.

The case studies were general in scope, offering approximately equal weight to information management, analysis and implementation processes.

The case studies provided an understanding of the security information management concepts used by the companies. The concepts were fully explored within the parameters of the security information management company policies. It also provided details on security information management, crime analysis and application processes in practice. The nature and extent of the problems experienced and the steps implemented to address the problems were also discussed for consideration as best practices.

Semi-structured interviews with the clients of the specific companies assisted in understanding the flow of information from the clients to the security information management companies. Some of these clients were, for example South African Synthetic Oils and Liquids (SASOL), Pick-and-Pay and Nedbank.

Due to legislative imperatives, these security information management companies are not allowed by law to manage and implement crime intelligence. Their focus is only on crime incident information reported by their respective clients. Letters requesting permission from the security information companies together with approval letters are attached (See Appendices 6, 7, 8, 9, 10 and 11. Interview guide used for the case study is similar to that used for the sem-istructured interviews (See Appendix 1). Consent form used for the case study is similar to that used for the semi-structured interviews (See Appendix 2). The consent forms were completed in order to conduct the case study research with the necessary confidentiality.

The researcher also attended the SAPS Provincial Crime Combating Forums in the Province of Gauteng. Security information management companies are also represented at these forums. The security information companies managed crime incident information, analysed them and formulated strategies and actionable crime information products to share with their clients, partners, the SAPS and other

stakeholders. This security information is shared with the SAPS in order to reduce crime rates, increase detection rates and prevent losses in businesses (Mzwandile, 2011: 28-29; Reddy, 2010).

The researcher also visited Edith Cowan University (ECU) at Joondalup, Perth, Western Australia. Semi-structured interviews with academics, researchers and security service representatives were conducted in Perth. These interviews were arranged by the School of Computer and Security Sciences in the Faculty of Computing, Health and Science. The semi-structured interviews were conducted using an interview schedule to explore how security information on incidents, threats and vulnerabilities is managed. Observation was also conducted at facilities, checking on how information is received, analysed and prepared for application in the form of strategies and actionable information products. The aim was to look at present day standards for security information management as used by security service providers in Western Australia. Letter requesting permission from ECU together with approval letter is attached (See Appendices 12 and 13). The interview guide used for the case study in Western Australia is similar to that used in the case study in South Africa (See Appendix 1). Similar consent forms to that used in South Africa was used for the case study in Western Australia (See Appendix 2). The consent forms were used in order to conduct the case study research with the necessary confidentiality.

2.2.5.4 Questionnaire survey

One-hundred-and-fifty questionnaires were prepared and handed out to security officials employed by the different sectors of the security industry in Gauteng. Only 114 were received back from the respondents.

The discussions from the focus group interviews, the responses to the semi-structured interviews and the literature study were used to design the questions for the questionnaire. The questionnaire was designed to guide the respondent and the researcher. This guided the researcher to understand the construct at hand and to know what additional clarification questions to ask to cover the construct. The questionnaire provided for closed and open-ended questions as required by the

mixed methods approach (Creswell, 2009: 17). The questions were focussed to ensure that the respondents gave the specific information required to answer the research questions (Greef, 2007b: 296-297).The questionnaire was divided into six sections. The sections were divided as follows:

- first section covered the respondent's demographic details,
- second section was about the security service details,
- third was on the collection of security information,
- fourth on the analysis of security information,
- fifth on the application of security risk control measures; and
- sixth section was on general issues the respondent intended to discuss.

The following was kept in mind when developing the questionnaire:

- biased and leading questions were avoided;
- negative questions were avoided;
- length of the questions and the questionnaire were considered, giving preference to shorter questions;
- loaded phrases that suggested certain responses were avoided;
- response categories were made easy to remember; and
- ensured that the response categories offered a real range of alternatives

(Delport & Rostenberg, 2011: 192).

The researcher personally took the questionnaires by hand to the relevant security service providers. At the start of the survey the researcher explained to the respondents the nature and purpose of the study, the duration of the questionnaire as well as what will be done with the data. The importance of each individual's contribution to the study, was emphasised, the sampling method used and why they were chosen and that they were free to ask questions at any time during or after the completion of the questionnaire. They were assured that all the information would be treated as confidential and anonymous. The researcher was open and honest about the purpose of the research and strived to maintain high levels of competence throughout the research (Whitt, 1991: 414).

Due to the practical nature of the work being performed by the security officials at different facilities in Gauteng, it was also financially viable and appropriate to use their senior managers to conduct the survey. In these instances, the researcher made appointments with the senior managers of the security companies, so that the questionnaires could be completed by security officials at the respective companies/plants. The managers who assisted with the interviews were given a full description of what the study was all about. General guidelines and procedures were discussed. Each question in the questionnaire was handled separately, with the senior manager. The researcher gave the senior managers specific guidelines on how to conduct the survey. The senior managers' efforts were carefully controlled by the researcher. All these questionnaires were collected not more than 48-hours after completion.

A pilot study was carried out on the questionnaires with persons other than the sample group. The respondents in the pilot study were asked to complete the questionnaires rather than to read through it for errors. The pilot study achieved two objectives: it improved the face and content validity of the instrument and secondly, it estimated how long it would take to complete the questionnaire. The questionnaire was presented to the full sample after the necessary modifications were made following the pilot test (Greef, 2007b: 294).

The self-administered questionnaire used in the quantitative survey is attached (See Appendix 14). Consent form used in the quantitative survey is attached (See Appendix 2). The consent form was used to conduct the quantitative survey with the necessary confidentiality.

2.2.6 Data analysis

According to Delport and Fouché (2011: 447), data analysis in mixed methods research consists of analysing the quantitative data using quantitative methods and procedures and the qualitative data using qualitative methods and procedures. The mixed methods research has seven data analysis stages that a researcher should follow when analysing mixed methods research data, namely:

1. data reduction (reducing the dimensionality of the of the qualitative data);

2. data display (describing pictorially the qualitative data and quantitative data);
3. data transformation (where qualitative data is converted into narrative data that can be analysed qualitatively, where quantitative data are converted into numerical codes that can be represented statistically);
4. data correlation (quantitative data is correlated with the qualitative data and vice versa);
5. data consolidation (both qualitative and quantitative data are combined to create new data sets);
6. data comparison (comparing data from the qualitative and quantitative data sources); and
7. data integration (quantitative and qualitative data is integrated into a coherent whole or two separate sets).

Qualitative data analysis transforms data into findings. It brings order, structure and meaning to the mass of collected data (Patton, 2002: 432). Qualitative data analysis is a search for general statements about relationships among categories of data; it builds grounded theory (Marshall & Rossman, 1999: 150). The aim of this analysis was to come up with a detail and systematic recording of the themes and issues, which had been addressed during the interviews and to link themes together within a category system.

According to De Vos (2007: 340) open coding, axial coding and selective coding are used in conducting data analysis on the grounded theory design. The analysis of data using the grounded theory is limited to the use of logic, sensitivity and three basic types of coding procedures. The codification process will be discussed, so that it can throw light on how it related to this study (Strauss & Corbin, 1990: 180).

Step 1: Open coding

Open coding is an interpretation process during which the data is separated through analysis. Open coding creates opportunities for the researcher to obtain new insight by looking at data in another way. The purpose of using open coding was to discover new phenomena, to develop themes in terms of features and dimensions and to provide names for the themes. Concepts of similar or concurrent happenings and

interactions are grouped together to form a category or sub-category (Creswell, 2009: 184). An example of such categorising and sub-categorising in security information collection is to check on the availability of guards and the cameras on the facility. The researcher conceptualised this happening for the ‘Collection of security information’, which may be subdivided into specific activities and dimensions. ‘Methods of collecting security information’ as a category may be sub-categorised into CCTV cameras and spotters.

Step 2: Axial coding

Axial coding was used to directly bring together the categories and sub-categories which were developed in the open-coding and positioning it under one category within a theoretical model. As this process goes ahead, new categories are developed. The researcher must be continuously on the lookout for such indications. If the researcher does not collect and analyse the data on the turn, it may result in the theory consisting of gaps (Creswell, 2009: 184). It is therefore important to conduct follow-up interviews to address the gaps. In the light of the aforementioned discussion the following example is provided. In this study the sub-category “CCTV cameras” is connected with the category ‘Methods of collecting security information’. The question is whether there is a connection between CCTV Cameras and ‘Methods of collecting security information’. If this question is verified and supported by the data the question changes into a hypothesis/proposal, namely: CCTV Cameras are used covertly as a method of collecting security information. Axial coding refers to a set of procedures whereby data is put back together in new ways after open coding, by making connections between categories, utilising a coding paradigm involving conditions, context, action or interactional strategies or consequences.

Step 3: Selective coding

Selective coding refers to the process of selecting the core category, systematically relating it to other categories, validating those relationships and filling categories that need further refinement and development. The purpose of selective coding is to integrate the themes, or categories on a dimensional level in a way that a

substantive theory (low order) is developed. To validate the integration of the relationship, all identified gaps need to be addressed. This relationship is tested with data by the development of an assumption, which is continuously compared with data and adjusted where necessary. The assumption which repeatedly appears in the data will be reflected in the substantive theory. Contradictory data must not be excluded, because it may indicate a possible variation. Selective coding is a process which consists of different steps. The first step is to allow a story line to unfold. Secondly, additional categories may be connected to the core category by way of paradigms. The third step indicates the relationship between categories on a dimensional level. Fourthly, the relationship between the core category and other categories are validated by data. The fifth step consists of incorporating further categories, with the aim to further refine and develop a theory. The core category represents the central theme of the phenomenon under study. The other categories are kept connected with the core category in relation to circumstances, actions/interactions, strategies or consequences. Every category and sub-category of a declared theory must have conceptual depth. If this is not the case, the researcher must go back to the field or field notes in order to obtain data to fulfil the gaps (Creswell, 2009: 184). The development of a grounded theory according to Strauss and Corbin (1990: 424), is limited to the controllability thereof.

In this study, the researcher applied open, axial and selective coding of the data collected during the semi-structured interviews and focus group interviews. The application of the selected coding method resulted in the selection of the core category; ‘management of security information’. The themes, concepts, categories and processes led to the unfolding of a substantive grounded theory in relation to security information management. The theory is that, ‘security officers operate without a standardised framework to manage security information’.

The challenge facing security service providers in Gauteng, is simply whether or not security information management can be approached in a much more structured, integrated and user friendly manner. Threats have an impact not only on economic loss, but also on human suffering through injury. According to Valsimakis, Vivian and Du Toit (1996: 12), a need exists for a different approach to manage security

information more effectively – with the objective of eliminating the causes of the threats and the vulnerabilities.

According to Kruger et al. (2007: 217-245), the simplest form of data analysis is univariate analysis. The univariate analysis process was used to analyse the variables from the questionnaires, mainly with the view to describing them. All the data gathered on the variables were summarised. The summary was displayed in a tabular form. Frequency distributions were used to describe the data. This summary displayed useful information to the researcher and provided the foundation for more sophisticated analysis at a later stage.

2.2.7 Guiding assumptions

The seven analysis stages that a researcher should follow in analysing mixed method data were followed. The findings of the grounded theory design were validated against the findings of the non-experimental quantitative research design.

According to Mouton and Marais (1990: 157), what is called hypothesis in quantitative research may be termed suppositions/assumptions, expectations or statements concerning anticipated results in qualitative research. Qualitative researchers use assumptions in their studies as a broad explanation for behaviour and attitudes and it may be complete with variables, constructs and hypothesis (Creswell, 2009: 61). The researcher made assumptions during the development of a substantive grounded theory. These assumptions were considered when determining the findings and making recommendations

2.2.8 Reliability and validity

According to Bless and Higson-Smith (1995: 129), reliability is the extent to which the observable measures that represent a theoretical concept are accurate and stable when used for the concept in several studies. Reliability of data is influenced by four variables: the researcher, the participant, the measuring instrument, the research context and the circumstances under which the research is conducted (Leedy & Ormrod, 2005: 92).

To achieve reliability, the researcher ensured that the interviews were carried out in a consistent manner, without any bias. The researcher ensured that the questions on the interview guide and the questionnaire were standardised from one situation or person to the next. All the items in the interview guide and the questionnaire were tested (piloted) to check whether it was consistent to yield similar results.

Validity means that the data and the methods must be right. The research data must reflect the truth and reality and cover crucial matters (Denscombe, 2002: 301). Face-and-content validity (Leedy & Ormrod, 2005: 92) of the questions on the interview guide and the questionnaire were tested. These were checked to see if the questions reflected on the collection and analysis of security information and the application of security risk control measures in appropriate proportions. Respondent validation was obtained from the participants in the purposive interviews by simply asking if they agreed with the conclusions. The researcher made sure that the data collection methods were administered in a consistent fashion and that the methods used to collect the data were accurate, honest and on target.

Criterion validity was used in this regard to test whether the results of the interviews and case study correlated with the literature review (Leedy & Omrod, 2005: 92).

Specific criteria were established to dictate the kinds of judgments the researcher made. One can measure something accurately only when one can also measure it consistently. In other words, in order to have validity one must also have reliability. The researcher ensured that each of the methods used was carefully monitored to prevent bias. Steps were taken to make sure that reliability became the central consideration of validity during the process of data collection. Opinions of experienced and skilled personnel from the security service and SAPS were obtained whenever subjective judgments were made of the data. The researcher remained as objective as possible throughout the research.

2.2.9 Field notes (Journal)

Noak and Wincup (2004: 171), state that: “the process of data collection, analysis and writing are intricately bound”. In line with the qualitative elements of the

research, field notes were kept from the beginning of the research. The field notes included a description of the events, the researcher's own feelings and responses to it and linkages to potential research themes. They also contain the researcher's thoughts regarding connections to the literature and prompts for future research and investigation. Regular face-to-face meetings were maintained to keep day-to-day contact with the activities of the security officials. According to Denscombe (2002: 274), this is sometimes called an audit trail to test reliability.

Taking down field notes or writing in a 'field journal' is an important vehicle for the researcher, as some of the information relayed on the tape might be lost for example during an interview if the telephone rang or people came to make enquiries and the researcher had to turn the tape recorder off. The researcher took notes during the case studies and during all the interviews in the event of data being lost. This procedure was explained to the respondents and they had no objections. In this way data could be verified at a later stage (Morrison, 2004: 13).

2.2.10 Limitations of the study

2.2.10.1 Limited literature

The researcher conducted a literature search on information concerning security information management in the security industry. Security service providers and the SAPS were consulted. None of these sources revealed any literature specifically on the same topic as the research. The researcher had to divide the research topic into concepts such as collection and analysis of security information and the application security risk control measures. This helped to find literature relevant to the concepts.

Sufficient literature was not available on the collection and analysis of security information and the application of security risk control measures. This research had to draw data using a combination of methods namely; interviews, case studies and literature study.

2.2.10.2 Sensitivity of information

The researcher was personally responsible for the gathering of data. Being an academic, respondents were not always keen on sharing security information. This was especially so in the case of information on collection methods, security products, security technology, strategies and actionable information products. Some respondents did not want to comment on undercover and surveillance methods used to collect security information, because of the sensitivity of the information.

Initially the researcher decided to do semi-structured interviews with security officials at grassroots level using an interview schedule. After, piloting several such interviews, it was found that the security officials could not provide all the required information. It was then decided to first conduct semi-structured interviews with senior managers from the security industry to help in designing a questionnaire. The questionnaire was designed consistent with the responses from the senior managers. The senior managers also facilitated the interviews with the security officials at grassroots level. This helped to obtain an authentic picture from the security officials at grassroots level.

2.2.10.3 Non-participation in case study

Initially it was planned to conduct a case study with the Special Investigations Unit (SIU) situated within the office of the National Prosecuting Authority (NPA) for best practices on the collection and analysis of security information and the implementation of security risk control measures. Although SIU granted permission, the case study interviews did not materialise because of their unavailability. One meeting was arranged by SIU, but cancelled at the last minute. According to Montesh (2007: 140), the SIU does not have intelligence collection powers and functions. Based on this finding it was decided not to pursue the SIU for a case study. They were subsequently replaced with the Consumer Goods Risk Initiative (CGRI) and the Petroleum Security initiative (PSI), who were better suited for the case study.

2.2.11 Value of the research

This research was able to establish the status quo of the collection and analysis of security information and the implementation of security risk control measures. It identified the nature and extent of problems experienced by security officials in the collection and analysis of security information and the implementation of security risk control measures. Solutions were also identified to address the problems. The findings and recommendations of this research will benefit the security industry. The security service provider will benefit in terms of knowledge, skills and attitudes in the collection and analysis of security information and the implementation of security risk control measures. The South African community will benefit from a much safer and more secure environment.

2.2.11.1 Operational clarification value

It is hoped that this research will lend itself to and facilitate the creation of an "information awareness culture" in organisations, companies and other agencies. Such would then lead to every member of staff (including contracted personnel), as well as security officials, to look out for security information with operational clarification value. Security officials to then follow proper procedures and ethics in security information management. Security service providers will ensure that the information is legally collected, entered timely into a database and analysed by qualified analysts. Recommendations by analysts will be valued by management and considered for the application of security risk control measures.

2.2.11.2 Original contribution to the disciplinary field of study

The relevance of this study is to provide a standardised framework to the security industry for security information management (Mouton & Marais, 1990: 14). The purpose will be to enhance the present crime combating strategies and create new opportunities for research. Security information is not always lawfully and ethically collected keeping in mind 'a service standard of excellence', neither is it correctly evaluated/verified, collated, analysed and implemented to mitigate security risks. It is

not shared in a regulated manner with all security service providers, the SAPS and other stakeholders in the security services industry either.

Although security service providers are regulated through PSIRA, the functioning of the security service provider in terms of his/her activity as an investigator, guard, etc. is not always information driven. Information collection is the starting point for a successful prosecution in a court of law or a disciplinary hearing. This research is important to empower the security official in this regard.

Much of the security information is being collected on an ad hoc basis. The information is mostly handled in an unregulated manner. Information is sometimes passed onto the SAPS. Information is also passed onto security officers and human resource managers for disciplinary purposes.

Emanating from this research was a practical Security Information Management Model (SIMM) designed and developed for the better management of security information in the security industry. The new model considers the implementation of physical protection systems, strategies and actionable information products to mitigate security risks. It will also leave a paper trail for monitoring and evaluation purposes.

2.2.12 Ethical considerations

Participants were not exposed to physical or psychological harm. Potential interviewees were informed of the nature of the study to be conducted and given the choice of either participating or not participating. Permission was also obtained from security service providers to conduct interviews and to carry out case studies. Interviewees were requested to sign a consent form. Participants had the right to withdraw from the study at any time. Participation in the study was strictly voluntary. Each participant's right to confidentiality and privacy was respected. All findings were done in a complete and honest fashion, without misrepresenting what had been done or intentionally misleading others as to the nature of the findings (Leedy & Omrod, 2001: 107-108). No confidential information shared by respondents with the researcher was revealed.

2.3 CONCLUSION

This chapter provides a methodological exposition of the research design by discussing mixed methods research, exploratory mixed methods research design, the grounded theory design, case study design and the non-experimental quantitative research design. Special emphasis was placed on the population and sampling techniques, data collection and data analysis procedures used. The exploratory mixed method research design helped integrate the qualitative and quantitative data for interpretation. It brought out the philosophical worldview assumptions of both the ontological and epistemological dimensions of this study taking into consideration the limitations, values of the study and the ethical considerations. The approaches, design and data collection methods followed in this research were found to be reliable. Triangulation of the information collected using different data collection methods helped to build a coherent justification for validity.

CHAPTER 3

GROUNDED THEORY: GENERATING CATEGORIES AND CODING THE DATA

3.1 INTRODUCTION

The researcher held a social constructivist worldview that security officials understand the world in which they live and work better than anyone else not specifically working in this industry or allied services like the police. Therefore the researcher relied as much as possible on their responses. Accordingly, there was a need to understand the problems identified by the participants and to interpret their meaning, so that a theory or pattern of meaning may be generated and inductively developed (Creswell, 2009: 8). The grounded theory design was used so that a grounded theory could be inductively developed to contribute to the scientific body of knowledge for this specific discipline. Semi-structured interviews were used to collect data from selected security managers. Focus group interviews were used to collect data from grassroots security officials and supervisors. The reason for using two different interviewing techniques, targeting two different echelons of the security service was to obtain meanings that are varied, diverse and multiple. This helped the researcher to look for a complexity of views rather than narrowing meanings into a few categories or ideas. The purpose was to obtain the everyday life and lay knowledge of how security information is collected, analysed and implemented as security risk control measures.

This chapter focuses on the conceptual construction and the categorisation of the data from the semi-structured and focus group interviews. The open, axial and selective coding procedures were used to generate the grounded theory.

3.2 CONCEPTUAL CONSTRUCTION AND CATEGORISATION OF DATA: A THEMATIC EXPOSITION

According to Patton (2002: 14), the researcher is the instrument and the methods used are part of the process. Qualitative research, under which the grounded theory resorts, required the researcher to personally collect and analyse the data (Whitt,

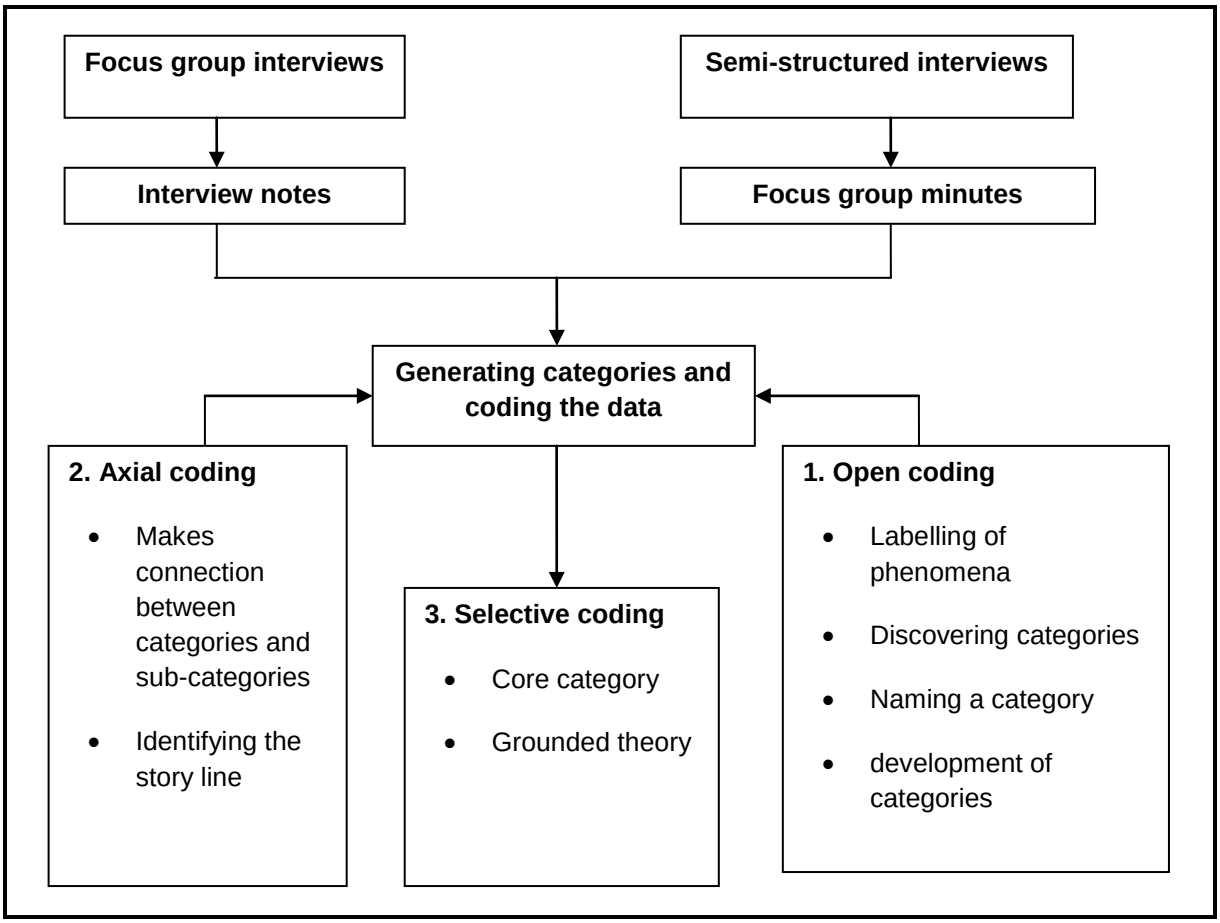
1991: 408). Semi-structured interviews together with focus groups were used as data collection techniques for this purpose. The researcher conducted semi-structured interviews and focus group interviews with two different sample groups to achieve an unbiased outcome. Reliability and validity was obtained by asking respondents in the semi-structured interviews and the focus group interviews similar questions and comparing the responses during categorisation. The researcher processed data immediately, clarified and summarised data as the study evolved and explored inconsistent responses. This also contributed to the reliability and validity of the data (Merriam, 1988: 19).

The researcher found the grounded theory design to be a systematic way of developing and integrating scientific knowledge and information. This involved generating themes and categories of information, selecting subcategories and positioning it within specific categories and themes within a theoretical model. It then involved explicating a story from the interconnection of these themes and categories and establishing a core category. The grounded theory was generated from the themes, categories and the story line.

3.2.1 Open coding, axial coding and selective coding process

The researcher designed Figure 3.1 to provide a structure of coding frame.

Figure 3.1: Structure of coding frame



The grounded theory was generated using the following steps:

- generating themes and categories of information (open coding);
- selecting sub-categories and positioning them under specific categories and themes within a theoretical model (axial coding);
- explicating a story line from the interconnection of these categories and themes resulting in a core category (selective coding); and
- by studying the different themes, categories and the story line a substantive grounded theory was generated (Creswell, 2009: 184).

During open coding, the researcher read through all the data from the semi-structured interviews (See Appendix1) and the focus group interviews (See Appendix 5). The researcher obtained a general sense of the information and reflected on its overall meaning, according to what was said by the respondents. This involved the process of breaking down, examining, comparing, conceptualising and categorising

data. The data from the semi-structured interviews and the focus group interviews were closely examined and compared to each other for similarities and differences, and questions were asked about the phenomena as reflected in the data. Specific themes and categories were developed with this scientific information

According to Straus & Corbin (1990: 96-97), in axial coding, subcategories are linked to a category in a set of relationships denoting causal conditions, phenomena, context, intervening conditions, action/interaction strategies and consequences. Axial coding was followed by putting together data in new ways, by making connections between categories and sub-categories using a coding paradigm involving conditions, context, action or interactional strategies and consequences. This process enabled the researcher to think systematically about data and to link them in more complex ways.

After some time of collecting and analysing the data, the researcher was confronted with the task of integrating the categories to form a core category. Selective coding was used to select the core category by systematically relating it to other categories, validating those relationships and filing in categories that needed further refinement and development.

Practically, the open coding, axial coding and selective coding process was used for coding and analysis of the scientific data in the grounded theory design. The semi structured interview guide (See Appendix1) and the focus group interview guide (See Appendix 5) were used to gather scientific data. For the sake of reliability and validity the questions were similar on both Appendices 1 and 5. The same items were being measured using two different instruments and groups. The respondents in the semi-structured interviews were senior managers from different sectors of the security industry. The respondents for the focus group interviews were security officers from different levels of the security industry. Both the measuring instruments proved to be reliable as they produced similar measurements. The responses from both the semi-structured interviews and the focus groups were broken down, examined, compared, conceptualised and categorised manually. Flip chart sheets were used to thematically categorise and sub categorise properties belonging to the same category. Subcategories were linked to categories in a set of relationships denoting

causal conditions, phenomena, context, intervening conditions, action/interaction strategies and consequences. The process unfolded into three main themes and categories which were aligned to the research questions. This conceptual construction and categorisation helped determine underlying processes in relation to the three themes, which resulted in the emergence of specific storylines (assumptions) for the three themes. The thematic exposition, categories and the storyline was used to develop a core category, which eventually gave rise to a grounded theory.

The data collected during the semi-structured interviews (See Appendix1) and focus group interviews (See Appendix 5) was broken down and conceptualised. Each piece of information was taken apart and given a name, something that represents a phenomenon. According to Straus and Corbin (1990:63) this is called the labelling phenomena. The next step was to group concepts around the phenomenon. This process of grouping concepts that pertains to the same phenomenon is called categorising. Categories have conceptual power because they are able to pull together other groups of concepts, processes or subcategories. This is how categories were discovered. The researcher gave the categories names that seemed most logically related to the data it represented and which is commonly used in the security industry.

A category was developed in terms of its properties which were then dimensionalised. Properties are the characteristics or attributes of a category, and dimensions represent locations of a property along a continuum (Straus and Corbin, 1990: 63). Open coding stimulated the discovery of categories, properties and dimensions. Properties also had sub-properties; each inturn was dimensionalised as directed by the analysis process. The researcher in this study decided on doing word for word analysis of the interviews by closely examining each response as recorded in the interview notes and field journal. Open coding may be done in various ways. Each person must find the method that works best for him (Straus and Corbin, 1990:67).

During the axial coding process the open coded data was put in new ways by making connections between categories and sub-categories. This was done by

giving consideration to conditions, contexts, action/interactional strategies and consequences. The open and axial coding process is outlined hereunder:

3.2.1.1 Theme 1: Collection of security information

Security information collection is not about collecting information at random. The collection drive must provide a plan and a focus so that that security information is collected to address specific threats, vulnerabilities and risks confronting the organisation/company. It is essential that the sources for the collection of security information should be approached with a description of the security information, which is likely to be useful in analysis. The integrity and quality of the information collected should always be borne in mind (Ekblom, 1988: 11).

Category 1: Sources used for the collection of security information

Conceptual construction in relation to the sources used for the collection of security information:

1. Information reports from organisations, companies, forums and networks
2. Risk assessment reports
3. Internal incident statistics
4. Hotline (telephone)
5. Whistle blowing
6. Community police forums
7. Loss reports
8. Investigation reports
9. Media reports
10. Suggestion boxes
11. Public/Staff
12. Security staff are expected to record all suspicious activities
13. No structured way of collecting information
14. External sources
15. Internal sources

The responses in **Category 1** indicate that security officials use different sources to collect security information on various aspects.

Information is the lifeblood of any organisation. Information is available on everyone and everything. One needs to know where and how to find it (Van Rooyen, 2008: 95). According to Van Rooyen (2008: 218), a source is the actual point from where information is obtained. First hand information may be sourced from a person, publication, thing or activity. The collection of security information must cover the organisation in totality. There should be no shortcuts. Security information is usually collected by accessing internal and external sources of information (Fischer et al., 2008: 148-156).

Category 2: People tasked to collect security information

Conceptual construction in relation to people tasked to collect security information:

1. Security managers
2. Security supervisors
3. Investigators
4. Crime risk officers
5. Security officials at grassroots level are not entrusted with investigations
6. No security information collection units exist
7. Management do not listen to security officials at grassroots

The responses in **Category 2** indicate that only specific individuals such as managers, supervisors, risk managers and investigators are tasked to collect security information. In some security companies grassroots level security officials are not entrusted with workplace investigation neither are they tasked to collect security information. Collection units do not exist in some companies.

According to Van Rooyen (2008: 95), successful investigators are seen as effective information collectors. In countries such as China, France, Russia, the United Kingdom, information collection units have been set up by government departments

to collect information on security related issues from specific sources (Clark, 2010: 88).

Category 3: Types of security information commonly collected

Conceptual construction in relation to the types of security information commonly collected:

1. Information on crimes/criminals
2. Security breaches
3. Policy violations
4. Information on marches/demonstrations/strike action
5. Information on technical problems
6. Auditing information
7. Security information on special events
8. Information on contractors
9. Occupational Health and Safety
10. Information on cheating
11. Information on physical protection systems

The responses in **Category 3** indicate the types of security information commonly collected in the security industry. Mainly incident and physical protection systems related information is collected. It is clear that security officials do not collect information on potential threats and existing vulnerabilities. Reactive information on incidents is prioritised for collection.

Categories of incidents which are commonly investigated to gather evidence includes the following:

- Violation of law (an example of an incident of rape);
- Accidental (an example of an incident where a customer falls on a slippery floor in a retail store);
- Anecdote (an example of an incident of a guard on night patrol at the back of the plant, surrounded by woods, where a bat swiped onto his bald head almost dropping him to the ground. It caused bruising to his head); and

- Violation of policy (an example of an incident of a security guard who fell asleep at 03:00 am in the morning while on access control duty. He was reported to the supervisor) (Opolot, 1999: 6-7).

Security information of any circumstances or event with the potential to cause harm to the systems, personnel, assets, facilities and viability of a business, industry or institution by destruction, disclosure or denial of service is referred to as threat information. It may require proactive or reactive action (Simonsen, 1998: 203). Security information on any weakness or flaw in the physical layout of an organisation, procedures, management, administration, hardware or software that may be exploited to cause harm to the institution, business or activity is referred to as vulnerability information. It may require proactive action (Simonsen, 1998: 202)

Category 4: Methods used to collect security information

Conceptual construction in relation to the methods used to collect security information:

1. CCTV cameras
2. Interviews
3. Collection methods are not always used to collect security information
4. Overt and covert methods are used to collect security
5. Forensic auditing is used to collect information in fraud investigations
6. Informers
7. Spotters
8. Section 205 of the Criminal Procedure Act
9. Obtaining statements in investigations
10. Networking

The responses in **Category 4** indicate that technical and human methods are used to collect security information.

According to Ferraro and Spain (2006: 13), physical surveillance, electronic surveillance, undercover operations, interviews and interrogations, forensics,

research and internal audit are the most commonly used methods for collection of information.

Category 5: Steps followed for the collection of security information

Conceptual construction in relation to steps followed for the collection of security information:

1. Receive voluntary information from third parties
2. Information is recorded in pocket books
3. Supervisor is informed verbally.
4. Supervisor enters the information in a register (occurrence book) in the control room
5. Forward to intelligence unit
6. Supervisor informs management of the information
7. Store security information in electronic systems

The steps in **Category 5** show that security information is collected, but not referred to qualified analysts (trained analytical and experienced experts). Some of the respondents mentioned that it is referred to intelligence units. The intelligence unit referred to in this context includes SABRIC, PSI and CGRI.

According to Reuland (1997: 7), information management includes the collection of information, collation of the information, analysis, dissemination, implementation and feedback. The outcomes of the collection of security information should be inextricably related to the focus areas in the security plan. In fact, it is the potential and intended outcomes that largely determine the focus areas (Ferraro & Spain, 2006: 79).

This security information is usually collected by conducting an asset assessment, threat assessment, security risk analysis, security survey, general departmental evaluations, operational audits or site visits as determined by management (Fischer et al., 2008: 148-156).

Category 6: Levels of classification used for the protection of security information

Conceptual construction in relation to the levels of classification used for the protection of security information:

1. Management do not want anyone to know about the information so they sometimes do not record it
2. Information access is restricted to most security personnel
3. Management do not trust security personnel working at grassroots level
4. Information is classified, using confidential, top secret, secret, restricted and not allowed access

The responses in **Category 6** indicate that security service providers utilise means to protect security information, even at the expense of not informing their grassroots level officials. Sometimes information is not recorded due to mistrust among security officials. No mention is made of any minimum information security standards framework used for the classification of security information.

Category 7: Advantages in collecting security information

Conceptual construction in relation to the advantages of collecting security information:

1. Eliminates or reduces risks
2. Provides investigators with information to solve cases
3. Gives businesses a competitive edge
4. Encourages the sharing of information
5. Decision makers can provide appropriate resources to address problems
6. Makes management aware of risks and trends
7. Reduces losses
8. Ensures safety of employees
9. Makes personnel alert
10. Creates security awareness

The responses in **Category 7** are widespread. It reflects on many different advantages for the organisation being protected. The most important advantage is the reduction of losses.

Category 8: Disadvantages in collecting security information

Conceptual construction in relation to the disadvantages of collecting security information:

1. Cost of collecting security information
2. Information is not operationalised
3. Time consuming
4. Infringement on human rights and privacy
5. Disinformation and information trade offs
6. Risky, can be assaulted or killed
7. Clients do not want to fund information collection
8. Mistrust among personnel
9. Leakage of information
10. Misleading information

The responses in **Category 8** indicate that many of disadvantages are related to poor management and control in the absence of standing operating procedures.

Category 9: Problems experienced in the collection of security information

Conceptual construction in relation to problems experienced in the collection of security information:

1. Personnel do not have skills to identify risks
2. Unable to take down statements
3. Poor communication skills
4. Legal restrictions on the collection of intelligence
5. Staff are reluctant to provide information due to intimidation and fear of being labelled as an *'impimpi'* (derogatory Zulu term for informer or 'sell-out' from the pre-1994 era of political contestation in the townships)
6. Infringement of people rights

7. No policy for the collection of security information
8. External databases not accessible
9. Personnel shortage to collect information
10. Do not get feedback
11. Management do not trust security personnel working at grassroots level
12. Not all information is stored and maintained in a computer database
13. Information is retained by people rather than by systems
14. Investigators possess wealth of information.

The responses in **Category 9** indicate that many of the problems are management related and relevant to human and physical resource support.

Category 10: Solutions to overcome the problems in the collection of security information

Conceptual construction in relation to solutions to overcome the problems in the collection of security information:

1. Personnel to be trained to collect security information
2. Improve communication skills of personnel
3. Closer working relationship with SAPS and NPA
4. Create awareness on the importance of information
5. Identity of information source to be protected
6. Motivate personnel on the collection of information
7. Improve networking with service providers
8. Information sharing to be encouraged
9. Accessibility to external databases to be negotiated
10. Payment of incentives for information
11. Provide the required human, physical and financial resources
12. Proper rewarding of informers
13. Keep track with new technology and advancement
14. All collected information should be placed on a database
15. Disciplinary action with penalties for non compliance
16. Collection of security information should be included in service level agreements and job descriptions
17. More academic research is essential to improve on the collection of security information

The responses in **Category 10** indicate management related solutions relevant to financial, human and physical resources. Memorandum of understanding may be used to improve networking with service providers.

3.2.1.2 Theme 2: Analysis of security information

When an incident is reported or a threat is identified, the next stage is to analyse the incident or threat information. Many corporate managers leave this important function to law enforcement, which presumably has sufficient resources to deal with these issues. In reality this is not always the case. Many law enforcement departments have neither the resources nor the capability to effectively examine incident or threat information as thoroughly as is needed. It is therefore important for security service providers to have their own analysis capabilities (Montgomery & Majesky, 2005: 612).

Category 1: Analysis of security information

Conceptual construction in relation to analysis of security information:

1. Investigators are tasked to do analysis on information received
2. In many instances analysis is done manually by management
3. Computer software programs for analysis is only used by big security service providers
4. Clerks are used as data analysts
5. Unaware of any analysis centres established by security service providers to analyse security information
6. Information is analysed to calculate risks
7. Special investigation units are used as analysis centres

The responses in **Category 1** indicate that trained analysts are not used to analyse security information. It would seem that there is more use being made of clerks and investigators than trained analysts to carry out the analysis functions. Knowledge of analytical concepts and methods in information management and crime analysis equips security officials better to perform security information management tasks, duties and responsibilities. This is why the majority of the people who undergo

analytical training are investigators. They are not interested in analytical career paths but want to utilise the proven techniques of analysis in their cases under investigation (Peterson, 1994: 6). According to Ratcliffe (2009: 160), it is increasingly accepted that analysts should make recommendations for future courses of action or activity based on the findings of the assessment undertake. Analysts are not merely data-entry clerks, nor do they work in or for quality control. Data cleaning should always be the norm (Reuland, 1997: 27).

Category 2: Steps followed in the analysis process

Conceptual construction in relation to steps followed in the analysis process:

1. Verify the information
2. Interpret the information
3. Decide on action
4. Discuss with management for implementation
5. Security officials who provided information are not involved in the analysis

The steps in **Category 2** do not indicate an analysis capability. This implies that security information is not analysed by qualified analysts.

According to Gotlieb et al. (1994: 137), analysis is the examination and processing of information which is directed at providing timely and pertinent information products relative to patterns and trend correlation. It is done by trained and qualified analysts using analytical computer software.

Category 3: Analysis products commonly used by security service providers

Conceptual construction in relation to the analysis products commonly used by security service providers:

1. Statistical information on incidents
2. Specific and recurring modus operandi patterns
3. Geographic concentration patterns on incidents
4. Security risk analysis report
5. Security assessments

6. Criminal reports
7. Alerts
8. Profiles

The responses in **Category 3** indicate that security service providers commonly use security risk assessments, risk analysis reports and actionable information products. No mention has been made of tactical strategies or physical protection systems to avert threats and vulnerabilities.

Engaging in the process of analysis suggests that patterns of crime can be identified among offenders, offences, victims and places (Newburn et al., 2008: 208). Analysis of information by experienced analysts will be able to assist the police and security officials with the most appropriate analysis results that will enable them to tactically plan operations to reduce crime, increase detection rates and prevent losses

In the majority of cases analysis products are never obtained directly from analysts, instead they are obtained from supervisors and managers. Security officials are not always given the opportunity to directly task the analyst on their analysis needs. This breakdown in communication between a security official and an analyst leads to misunderstanding and mistrust, specifically when requesting additional information for the enrichment of the information on hand. These are some of the many problems that confront security officials on a daily basis, which require managerial interventions. These problems have to be addressed directly by management (Ratcliffe, 2009: 129).

Category 4: Advantages in the analysis of security information

Conceptual construction in relation to the advantages in the analysis of security information:

1. Identify vulnerability areas
2. Provides risk mitigation strategies
3. Provides operational responses to crime
4. Directs investigations
5. Improves security measures

6. Directs training
7. Helps us to understand the collected security information

The responses in **Category 4** indicate that there are many advantages for the organisation which is being protected, if security information is analysed by trained and experienced analysts.

Category 5: Disadvantages in the analysis of security information

Conceptual construction in relation to the disadvantages in the analysis of security information:

1. Time consuming
2. Incorrect recommendation by analysts
3. Inexperienced analysts
4. Costly exercise
5. Inaccurate information is provided to analysts
6. Validity and source of the information is not tested
7. Insufficient information is given for analysis

The responses in **Category 5** indicate that management does not do much to manage data integrity and quality control the analysis result before it is passed onto the security officials for application.

Category 6: Problems experienced in the analysis of security information

Conceptual construction in relation to problems experienced in the analysis of security information:

1. No indexing, sorting and storage of collected security information takes place
2. Information is manually recorded in registers by supervisors
3. No policy framework for the analysis of security information
4. Many security service providers do not have analysts in their employ
5. Shortage of trained analysts
6. Shortage of computers
7. Shortage of computer software programs to do specific analysis

The responses in **Category 6** indicate to management related problems relevant to the absence of a policy framework and the need for human and physical resources.

Category 7: Solutions to overcome the problems in the analysis of security information

Conceptual construction in relation to solutions to overcome problems in the analysis of security information:

1. Need for analysis computer software programmes
2. Qualified experience personnel should be used to do analysis
3. Training of analysts
4. Develop collection plans in consultation with analysts
5. Establish a data analysis centre to monitor incidents
6. Analyse information in a structured way

The responses in **Category 7** indicate to management related solutions which will need the formulation of a policy framework to handle analysis in a structured way and physical and human resource interventions.

3.2.1.3 Theme 3: Implementation of security risk control measures

The security officer responsible for the implementation of the specific security risk control measure should be in the best position to reach a reasoned conclusion on the most likely security risk control measure, to obviate or minimise the identified threat (Montgomery & Majeski, 2005: 598).

Category 1: Implementation of security risk control measures

Conceptual construction in relation to the implementation of security risk control measures:

1. Prevent crimes
2. Mitigate risks
3. Reduce and recover losses
4. Apprehend perpetrators

5. Future planning
6. Corrective action
7. Supervisor makes a decision on how to handle the information
8. Physical security is improved if the budget is available
9. Supervisors investigate the report
10. Forward to SAPS for action
11. Investigate disciplinary irregularities
12. Use in awareness programme
13. Forward to information management companies such as SABRIC, CGRI and PSI.

The responses in **Category 1** indicate that implementation of security risk control measures is operationalised on the decisions made by a supervisor. Security risk control measures are implemented for a variety of reasons and not related to a specific organisational security strategy. It is clear that there are no standing operating procedures on which decisions may be made by security officials at grassroots level for the implementation of security risk control measures.

The decision by a supervisor to implement a specific security risk control measure or solution is subjected to a rigorous return-on-investment exercise, during which process the financial benefits of the security measure is quantified. This exercise assists in identifying and in isolating the most cost-effective security measure for possible intervention. This is important in order to contribute to the decision-making process and to overcome resistance from top management in terms of obtaining their approval for funding and implementation of the recommended security risk control measures (Rogers, 2008: 152-153). The implementation of the security risk control measure is more quantitatively driven in terms of cost than the qualitative designing of the security risk control measure to deter, detect, delay and respond to the intruder.

Category 2: Intended users of the security risk control measures

Conceptual construction in relation to the intended users of the security risk control measures:

1. Security personnel
2. Investigators
3. Police
4. Auditors
5. Legal services
6. General personnel
7. Visitors to facility
8. Management

The responses in **Category 2** indicate that the intended users of the security risk control measures include security personnel, staff from the organisation/company being protected and police personnel.

To promote a culture of applying creative strategies, the American policing agencies have introduced an increasingly popular strategy of providing police officers with crime analysis information in the form of crime maps. The aim is to encourage officers to use crime information, determine problem areas and modify their strategies accordingly. This goes together with training and resources to allow for the full capability of crime mapping to be realised (Paulsen, 2004: 234).

Category 3: Dissemination of recommendations for the implementation of security risk control measures

Conceptual construction in relation to the dissemination of recommendations for the implementation of security risk control measures:

1. Reports
2. Meetings
3. Emails
4. Handouts
5. Telephonic conversation

6. It takes about 24hours to disseminate recommendations for operationalisation
7. The outgoing shift disseminates information to the incoming shift, so that they become aware of any incident that occurred.
8. Information is disseminated on a need-to-know basis

The responses in **Category 3** indicate that verbal and written communication methods are used to disseminate recommendations for the implementation of security risk control measures. The cause for concern is that information takes about 24hours to be operationalised. There seems to be no regulated way in which security information is disseminated for application.

Jordaan (2003a: 59) refers to dissemination as vital, as it encompasses information that was gathered and analysed and which must be packaged and delivered to the clients who can use it. Dissemination of the recommendation for application of specific security risk control measures is the first stage of the application process. Dissemination can be carried out in several different ways, namely, by attending briefings and strategy sessions, presenting verbal reports, providing written reports, having face-to-face contact with investigators and whenever the need arises. Public information systems – both the written and electronic media may also be used to disseminate security risk control measures (Reuland, 1997: 35).

Category 4: Feedback on the implementation of the security risk control measures

Conceptual construction in relation to feedback on the implementation of the security risk control measures:

1. Reports
2. Meetings
3. E mail
4. Telephonic communication
5. In many instances no feedback is given
6. In urgent cases feedback is given over the phone and followed up with a written report
7. Feedback is important
8. Feedback to be given in a form of a memo

The responses in **Category 4** indicate that verbal and written communication methods are used to give feedback. It would appear as though feedback is given as determined by individual end-users of the security risk control measures

According to Reuland (1997: 36), feedback is the informing of the crime analyst of the outcome of the information or crime analysis product.

Category 5: Advantages of the implementation of security risk control measures

Conceptual construction in relation to advantages of the implementation of security risk control measures:

1. Helps planning on operational and strategic levels
2. Planning budget for future year
3. Keeps abreast with trends and methods
4. Gives competent edge
5. Adds value to customer needs
6. Protects own interest
7. Reduces security risks
8. Keeps facility safe

The responses in **Category 5** indicate that there are many advantages, for the organisation being protected, in the implementation of security risk control measures. The most important advantage is the reduction of risks.

The implementation of the security risk control measures should benefit the organisation by being able to detect an adversary, delay the adversary and be able to provide timely responses by security personnel (Garcia, 2008: 5).

A layered security strategy built around all aspects of an organisation will make sure that security risk control measures are applied accordingly (Johnson, 2005: 334).

Category 6: Disadvantages of the implementation of security risk control measures

Conceptual construction in relation to disadvantages of the implementation of security risk control measures:

1. Use of illegally obtained information
2. Incorrect information may lead to arrest of innocent persons and civil claims
3. Selling of information to criminals
4. Leakage of information
5. Abuse of security information
6. Need experienced personnel to apply strategies
7. Physical security protection systems may be unaffordable
8. Incompetence
9. Language barriers

The responses in **Category 6** indicate that the implementation of security risk control measures is not managed according to a standardised framework.

Category 7: Problems experienced in the implementation of security risk control measures

Conceptual construction in relation to problems experienced in the implementation of security measures:

1. No policy framework for the implementation of security risk control measures
2. Feedback is given informally
3. No evaluation on the implementation of the security risk control measures
4. Shortage of personnel
5. No budget
6. Clients are not prepared to fund physical security protection systems
7. No training is provided for the implementation of security risk control measures
8. Lack of understanding

The responses in **Category 7** indicate that the problems are management related and refer to human, financial and physical support problems.

Category 8: Solutions to overcome the problems in the implementation of security risk control measures

Conceptual construction in relation to solutions to overcome problems in the implementation of security risk control measures:

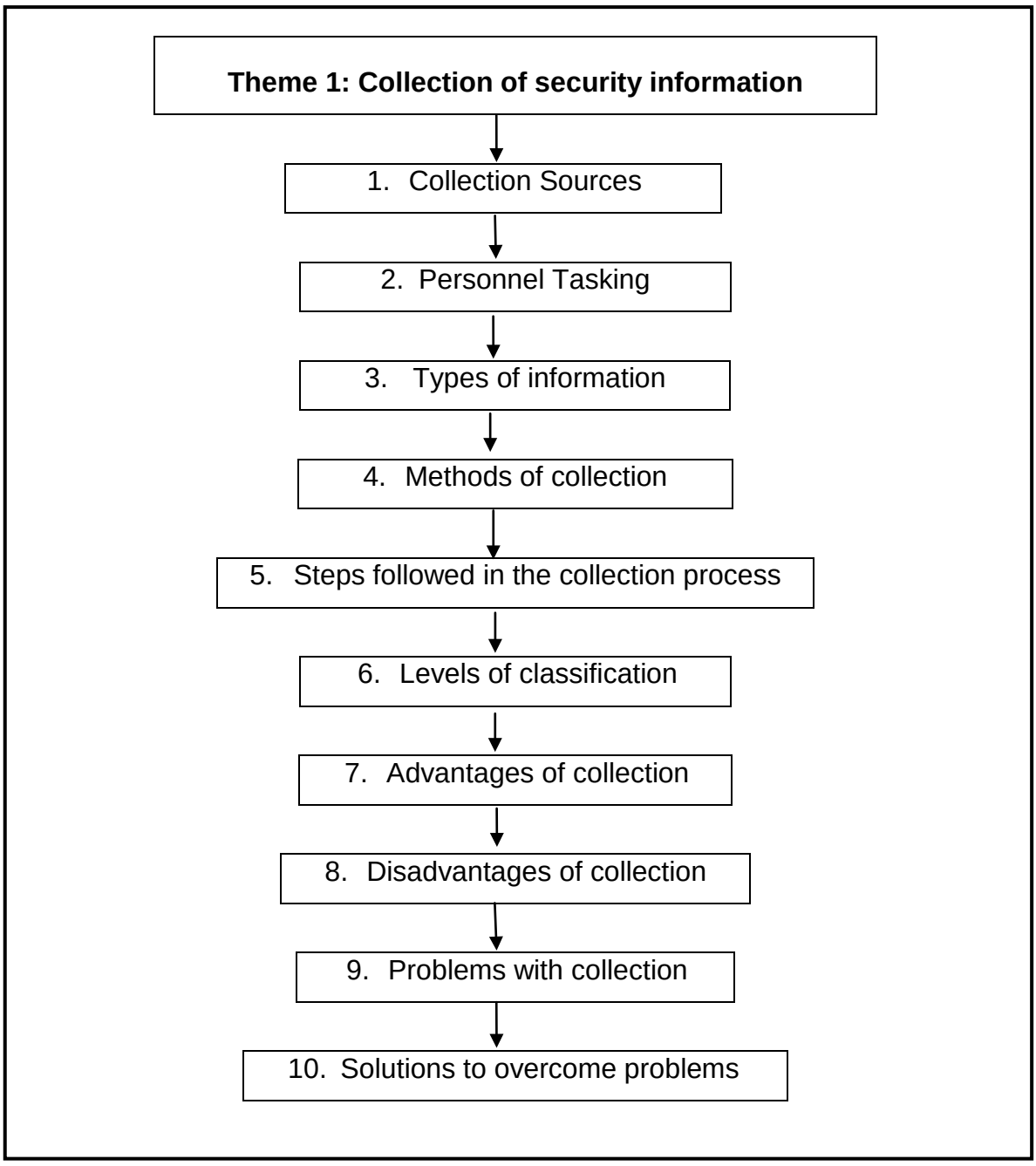
1. Employ the correct people for the job
2. Better communication between management and end-users
3. Have a separate unit for the implementation of the security risk control measures
4. Need to have a structured way of dealing with information control measures
5. Marketing the need for the implementation of specific security risk control measures

The responses in **Category 8** indicate to management related solutions which will require human and physical resource support.

3.2.1.4 Development of the grounded theory

The themes, categories, concepts and processes which have been discussed under Paragraph 3.2.1.1, 3.2.1.2 and 3.2.1.3 above, led to the unfolding of a storyline in relation to the collection, analysis and the implementation of security risk control measures. The researcher looked at what was most striking in each of the areas of this study and considered that to be the storyline. Once the researcher had committed himself to a storyline in each of the areas of study, he moved beyond description to conceptualisation of the storyline by analysing the story and giving the central phenomena a name and as a category related it to the other categories. The lists of categories were used to identify a category which was abstract enough to encompass all that had been described in the story. This helped identify the core category. The themes, categories and a storyline (assumptions) which led to the core category and the development of the grounded theory are schematically provided in Figures 3.2, 3.3 and 3.4 below, which was designed by the researcher.

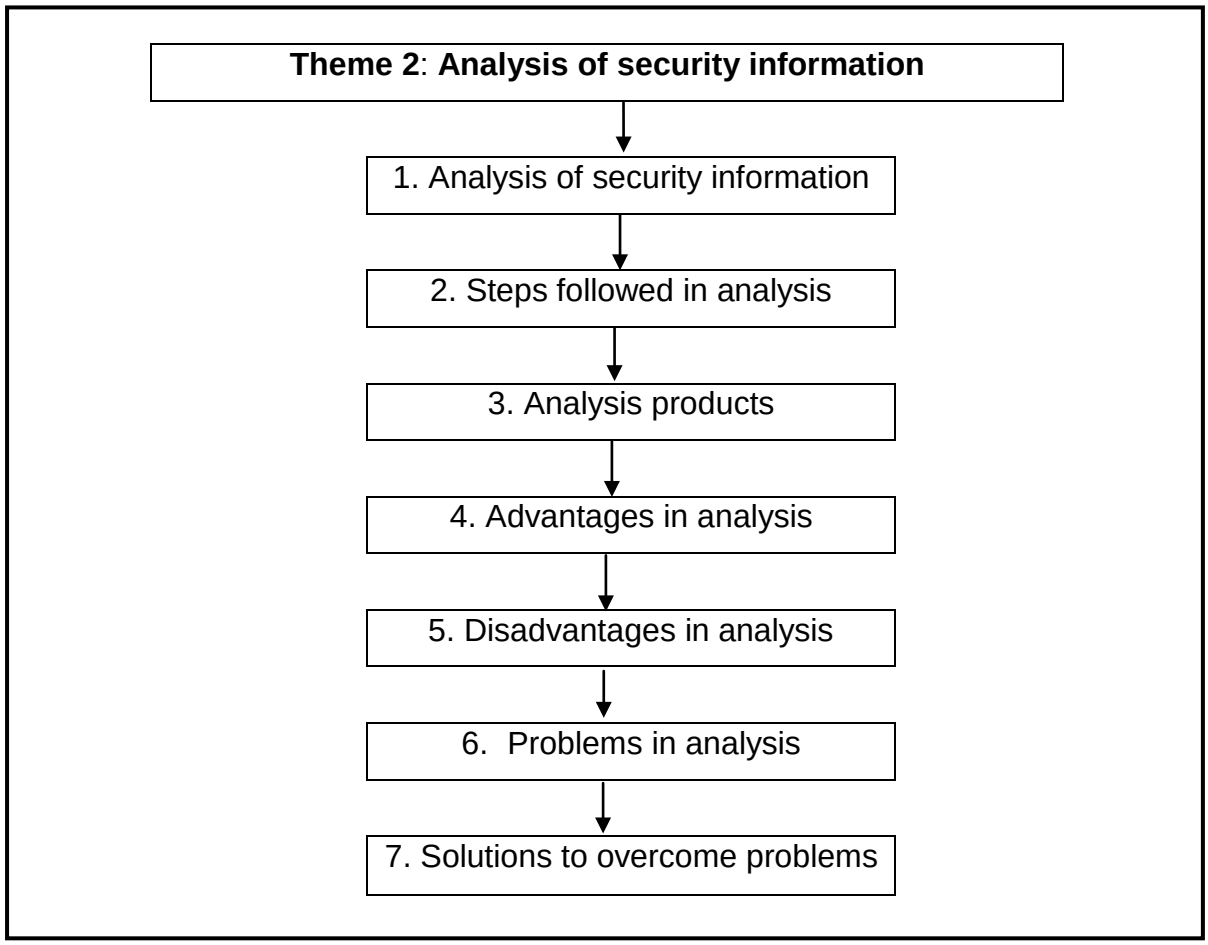
Figure 3.2: The underlying processes in relation to the collection of security information



Storyline 1: There seems to be no communication between the client and the collector of the security information. A security plan has not been mentioned as the guiding instrument on the type of security information to be collected. Security officials do not know the focus areas of the organisation and the needs of the client. As a result money, human resources and technology is wasted on collecting security

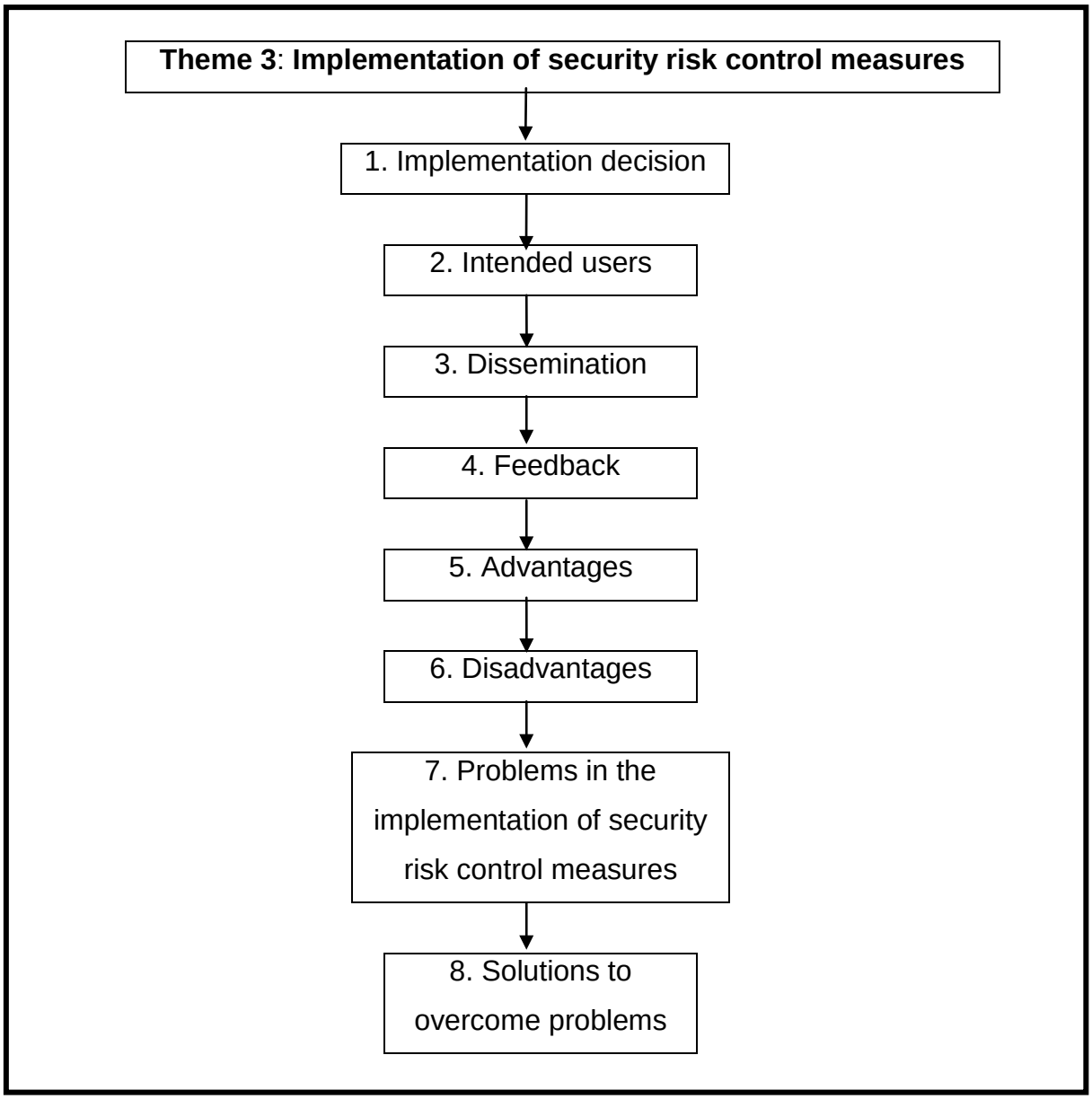
information which is not a need to the client. This wastage of resources is not good for an organisation whose reason for existence is profit making. It amounts to fruitless expenditure. The assumption is that the collection of security information is not strategically driven by a strategy or a plan.

Figure 3.3: The underlying processes in relation to the analysis of security information



Storyline 2: No indication that a threat assessment, vulnerability assessment and incident pattern analysis is being done. It would seem as though the focus is on looking at incident information which can be analysed by investigators and security supervisors. There seems to be no need for analysed information by the clients, as the analysis is not directed at addressing specific threats or vulnerabilities. No mention is made of automated system software used for analysis. The assumption (hypothesis) is that qualified analysts are not employed to do analysis on threats, vulnerabilities and incidents.

Figure 3.4: The underlying processes in relation to the implementation of security risk control measures



Storyline 3: The implementation of security risk control measures is not considered in conjunction with the organisation's security plan. Security information is collected randomly (without any structure, benchmarks or integration) without knowing the client's specific security needs. A criticality assessment to implement the analysed security risk control measures is only done after money, human resources and technology had been invested on the collection and analysis of the security information. Management only decides during the implementation phase not to implement the analysed security risk control measures due to the costs involved.

The implementation of the security risk control measures is then shelved. Much of the analysed security risk control measures are not qualitatively assessed by evaluating its deterrence, detection, delay and response capabilities (and impact after application). The assumption is that objectives such as the reduction of crime, increase in detection rates and the prevention of losses are not considered in the implementation of security risk control measures.

Selective coding is a process of selecting the core category. The process unfolded by systematically relating to other categories, validating those relationships and filling in categories that need further refinement and development. The selective coding process resulted in the following conclusion: the core category that emerged after coding was the security officials' "management of security information". According to Glaser (1992: 155) and Straus and Corbin (1990: 23), for the grounded theory to qualify as a theory, it must satisfy the following requirements:

1. It must be applicable to the phenomenon under study.
2. The theory must be understandable.
3. The theory must be applicable and relevant to the substantive themes under study.
4. The theory must be adaptable or controllable.

The coding process discussed under Paragraph 3.2.1 above, led to the development of a grounded theory in relation to security information management. The grounded theory is that security officials do not manage security information by using a standardised framework (De Vos, 2007: 345). The grounded theory for security information management is explained and described together with its important points in a schematic presentation (Figure 3.5).

3.3 SCHEMATIC PROPOSAL OF THE GROUNDED THEORY

The grounded theory for security information management is presented schematically in Figure 3.5, which was produced by the researcher.

Figure 3.5: Security information management: grounded theory

SECURITY INFORMATION MANAGEMENT

Phase1

COLLECTION OF SECURITY INFORMATION

Collection sources

- Internal/external sources

Personnel tasking

- Security managers/Supervisors
- Risk managers/Investigators

Types of information

- Incident information
- Information on physical protection systems

Methods of collection

- Technical methods
- Human methods

Collection process

- Receive voluntary information from third parties
- Information is recorded in pocket books
- Supervisor is informed verbally
- Supervisor enters the information in a register (occurrence book) in the control room
- Forward to intelligence unit
- Supervisor informs management of the information
- Store security information in electronic systems

Protection of information

- Unregulated information protection measures

Phase 2

ANALYSIS OF SECURITY INFORMATION

Analysis process

- Verify the information
- Interpret the information
- Decide on action
- Discuss with management
- Security officials who provided information are not involved in the analysis

Analysis products

- Actionable Information products

Phase 3

IMPLEMENTATION OF SECURITY RISK CONTROL MEASURES

Decision to implement security risk control measures

- Supervisors decide on the implementation of security risk control measures

Identify intended users

- Security personnel
- Personnel from the protected organisation
- SAPS

Dissemination

- Verbal and written communication

Feedback

- Verbal and written communication

3.3.1 Exposition of the grounded theory in security information management

The grounded theory around security management which was outlined in Figure 3.5 is explained hereunder:

Management of security information is divided into three phases, namely:

i) collection phase;
ii) analysis phase; and
iii) implementation phase.

The first phase cannot stand on its own, as it is influenced by the analysis and implementation phases. The collected information must be analysed and implemented as security risk control measures to complete the security information management chain.

Phase 1: Collection of security information

Collection of security information is the first phase of the security information management chain. Security information is collected on incidents and physical protection systems. Security information is collected from internal and external sources by security managers, supervisors, risk managers and investigators. Security service providers employ technical and human methods to collect the information. Voluntary information received from human sources is recorded in the security official's diary. The supervisor is informed of the information. Supervisor enters the information in a register (occurrence book) in the control room. If the company has an intelligence unit, it is forwarded to the intelligence unit for collation, analysis, interpretation and the obtaining of missing additional information (if deemed necessary). If the organisation is linked to an information management company such as SABRIC, PSI or CGRI, the information on the incident is sent to them for further management, i.e. adding to information received from other entities or organisations serving the same sector. The supervisor informs management of the information. The information is classified using different classification methods for the sake of protection. The classified information is stored in a database.

Phase 2: Analysis of security information

The analysis phase is the second phase of the security information management chain. This phase refers to the analysis of the collected information. The collected information is passed onto supervisors for a decision. The supervisor verifies and interprets the information, decides on the most appropriate action, discusses it with management when necessary and implements the relevant security measures. Security officials who provided the information are not involved in the analysis and decision making of the collected information. Only some of the large organisations have the requisite infrastructure with qualified analysts. Smaller security service

providers do not find it financially viable to have an infrastructure with analysis capabilities within their organisation/company. Those that do have analysis capabilities mainly produce actionable information products for implementation.

Phase 3: Implementation of security risk control measures

The third phase of the security information management chain is the implementation of security risk control measures. Here a decision is made by the supervisor on whether to apply security risk control measures or not. If a decision is made to apply specific security risk control measures, it is disseminated using verbal or written communication to the intended user/s. The intended users include the security personnel, personnel from the organisation being protected or the SAPS. Feedback is also requested from the end user. Feedback is usually given using verbal or written communication.

3.4 CONCLUSION

This process of building a grounded theory, unfolded by means of the analysis of the data obtained via the semi-structured and focus group interviews. The data was analysed using open coding, axial coding and selective coding processes. This helped determine the status quo of the collection and analysis of security information and the implementation of security risk control measures by security service providers in Gauteng. The grounded theory was generated. The grounded theory assisted the research to further understand the status quo and the existing problems in security information management. The researcher achieved reliability and validity by making certain there was no drifting of the definitions of the codes and the meaning of the codes during the process of coding. Data was constantly compared with the codes and by making notes about the codes and their definitions/meanings. Themes and categories with definitions and meanings were also checked with the participants, to obtain the participants contribution on their accuracy.

CHAPTER 4

SECURITY INFORMATION MANAGEMENT

4. 1 INTRODUCTION

It has been said that:

> …security is both a state of being and a means to that end. As a state of being, security suggests two quite distinct objective and subjective conditions. And as an objective condition, it takes a number of possible forms. Firstly, it is the condition of being without threat: the hypothetical state of absolute security. Secondly, it is defined by the naturalisation of threats: the state of being protected from. Thirdly, it is a form of avoidance or non exposure to danger ….. As a subjective condition, security again suggests both the positive condition of feeling safe and freedom from anxiety or apprehension defined negatively by reference to insecurity (Zedner, 2003: 155).

For the purpose of this study, security information is referred to as information related to any incident, threat or vulnerability which has the potential to exploit an asset or group of assets and thereby cause losses to an organisation (Blyth & Kovacich, 2006: 25). Security information is important to reduce crime, increase detection rates and prevent losses. For many years society has relied exclusively on the police to prevent and control crime. It is now the time for the security services to play a greater role in the prevention and control of crime than ever before (Fischer et al., 2008: 41). Due to limited literature on security information and the similarities between security information on threats and incidents of crime, literature on the collection, analysis and implementation of crime information will also be discussed.

This chapter provides a comprehensive literature study on the collection and analysis of security information and the implementation of security risk control measures.

4.2 SECURITY INFORMATION MANAGEMENT CULTURE

4.2.1 Security awareness culture

Despite the efforts by the police, community programs and private security, crime continues to be a major concern for most citizens in South Africa (Van Rooyen, 2008: 2). There is close relationship between the rise of private security and changes to mainstream policing. Community expectations about the ability of the police to control and regulate crime have dropped and fear of crime has risen. Awareness has grown that paying for private security services is acceptable and sensible for individuals and corporations (Smith & Natalier, 2005: 112-113).

According to Louw (2001: 4), the absence of an “information culture” in the SAPS gave rise to problems in policing. The events of the September 11, 2001, attacks on the World Trade Centre in New York and the Pentagon in Washington, D. C., have changed the face of security operations in South Africa and elsewhere in the world. A culture of security awareness became a common theme considered by almost every person in the world (Fischer et al., 2008: 1).

A culture of security is the logical conclusion to a well-driven security awareness programme. Once people become aware of incidents, threats and vulnerabilities affecting the assets of an organisation, it is in their nature to react to it. Well motivated people want to solve a problem if they feel concerned about it. A culture of security is not an objective in itself; it is a state of mind and ‘the way things are done around the organisation’ which supports achievement of broader organisational objectives. Establishing or even defining a security culture that will do this is not simple. Many attributes are involved to shape behaviours, attitudes and trust. Given the similarities between safety and security, we should consider the idea that a high performing security culture is also equally an informed culture (Talbot & Jakeman, 2008: 62).

Security cultures are highly dependent on the knowledge gained from rare incidents, mistakes and near misses. 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 to report near misses or minor events that might otherwise go unnoticed (Talbot & Jakeman, 2008: 66).

4.2.2 Security management culture

Because of their positions in organisations and companies, security managers need to play a primary role in creating a thriving environment for the awareness of security information. According to Fischer et al., (2008: 149), “being aware of all possibilities is the characteristic of a good security manager. The best manager can think like a thief and thus is able to consider policies to reduce the vulnerability of company property. Therefore, a manager must develop the ability to analyse threats and vulnerabilities.”

Managers are found in all areas of work and at different levels within an organisation ranging from supervisor to chief executive officer. They are responsible for running the organisation, developing strategies, setting targets and objectives, overseeing projects and co-ordinating activities. This is done to achieve performance targets and to ensure that everything runs smoothly. The size and scope of the responsibility may differ, depending on the size of the organisation, department, project, team or small business. There are certain common skills which managers need in order to manage security information effectively and efficiently. Managers need to:

- *plan*-decide how best to achieve the targets for a particular responsibility area;
- *organise*-decide on the most suitable ways of using resources (people, money, material and information) to maximise efficiency and profitability;
- *direct*-communicate effectively and guide others towards the organisational goals and objectives; and
- *control*-monitor and evaluate how the security plan is being carried out. This will involve setting timescales and target dates for goals and objectives and measuring progress at each stage. There may also be a need to adjust the plan to correct for delays and take advantage of new opportunities (Burt, 2004: 10-11)

4.3 COLLECTION OF SECURITY INFORMATION

The first step in security information management is collection. This study involves the collection of security information on incidents, threats and vulnerabilities. The collection of security information must follow specific legal procedures and processes. Information collection must involve all personnel and customers who come into contact with the organisation. It must cover the entire organisation. There should be proper management and control of the collected security information at all levels of the organisation. To put money into security information management is investing in the company's future (Fischer et al., 2008: 148-156).

Currently, very little notice is taken of threats and vulnerabilities on a day to day basis. If this information is immediately collected and acted upon, it will result in the eliminating, disguising or lessening of the vulnerabilities, so that threats do not materialise. The local environment may provide information about the threat for a specific organisation. Conditions outside the organisation and inside the organisation should be considered in this regard. Conditions outside the organisation such as the general attitude of the community, whether the surrounding area is urban or rural and the presence of well known extremist groups, can provide information on threats. Conditions inside the organisation, such as the workforce, labour issues, industrial relations policies, security awareness and human reliability programs, may also affect the potential threat (Smit, 1989: 4-5).

An environmental scanning of the local and national population can be useful in determining a potential threat to a specific organisation. Any discontented and disgruntled group of the population should be addressed. Special attention should be given to war veterans, technically skilled people, political extremists and employees with experiences in or access to similar organisations. There are several features of an organisation that may make it more or less attractive to an adversary if there is a perception that these features can be used to his/her advantage. Geographic and structural differences of the organisation, the attractiveness of specific assets and the adversaries' assessment of vulnerabilities are a few of these features (Garcia, 2008: 32).

Two types of information on crime is important, the first is information as knowledge, which is provided first hand by victims, complainants, witnesses and offenders which can be related directly to investigators and the courts. Information may also come from those who do not have first hand knowledge of a crime, such as those from informants or opinion from experts. The second type is information as data, most often in the form of objects, documents, images, recordings and scientific samples from which investigators and courts can infer facts about the case (Stelfox, 2009: 86).

Crime information must be timely, because the chances of apprehending an offender responsible for a series of cases depend on quick identification of the crime pattern (Goldsmith et al., 2000: 4).

Recorded crimes suffer from problems of under-reporting and are also highly variable in their accuracy and quality, particularly in the way addresses and locations are geographically referenced (Hirschfield & Bowers, 2001: 239). Even where crimes are reported and recorded by the police, the police record may contain a number of vague or inaccurate pieces of information. In some instances the inaccuracies may be as a result of the interpretation put on the information by the recording official (Ainsworth, 2001: 78-79). According to Gardner (2005: 352), the quality of the processed information depends largely on how well a police service can store and access data.

Reuland (1997: 9) mentions that most organisations probably have few options for obtaining external information, since they have little control over external data bases. According to Block et al. (1995: 3), the absence of a close working relationship with the community, incorporating an effective and mutual exchange of information, seems to be a problem in a community.

The following problems were discovered in the SAPS, pertaining to the collection of crime information at station level:

- the recording of exactly where crimes happened;

- the classification of certain crimes, e.g. aggravated versus common robbery, serious assault versus attempted murder; and
- updating the SAPS data sheet that provides information on the outcome of a case once it has been to court (i.e. whether a conviction was achieved, whether the case was withdrawn, etc.) (Louw, 2001: 4).

In many instances deductive or inductive arguments and rational reconstruction are not applied to collected information in the investigation of cases. Most detectives work in a routine and repetitive fashion, relying on knowledge information of complainants, victims, witnesses and suspected persons (Altbeker,1998: 28). According to Altbeker (1998: 30-36), the proper collection and analysis of crime information in the investigation of crime will increase detection rates.

Paulsen (2004: 234) states that the field of policing has had an uneasy relationship with technology, often being slow to adopt new technologies despite their potential benefits to policing. Police agencies in the USA rely on the electronic transfer of data, laptop computers transmitting data through radio frequencies or scan forms to ensure receipt of timely crime data (Goldsmith et al., 2000: 4). According to Reuland (1997: 12), although computers have had limitations in the past, an organisation needs to decide on the kind of technology that will be required for this purpose. The use of mainframe computers and micro-computers should be compared before making a choice. Mainframe computers are faster in their searching ability and can store far more data than their micro-computing counterparts. Mainframes are valuable, however, for storing and archiving data, as long as they can be easily assessed by microcomputers (smaller machines).

4.3.1 Kinds of security information

This study is directed at information on incidents, threats and vulnerabilities.

Smit (1989: 5) describes information on incidents, threats and vulnerabilities as follows:

- incidents (crime/policy violations);

- threats (crime, terrorism, foreign intelligence, commercial or industrial; competition and maliciousness or other malevolent acts); and
- vulnerabilities (outcome of the failures, non application, under-application, erroneous application or superficial application of security risk control measures).

According to Talbot & Jakeman (2008: 66), all incidents of crimes and policy violations that had taken place in the organisation should be subject to investigation by the police or the organisation where the incident took place. An incident register should be used to record all reported incidents. The management of security incidents should be addressed in some detail in a policy document on incident management and reporting. The particular focus should be on the operationalisation of the information. According to DeKock (2011), all crime incidents in the SAPS are recorded in registers and computer systems for analysis. This information is subsequently used to develop a Crime Pattern Analysis (CPA) document for use by police officials in their day to day operations. He is of the view that the record of all incidents may also be used to develop an Incident Pattern Analysis (IPA) document, similar to the CPA. The IPA may also be used by security officials in their day to day operations.

Information on vulnerabilities may be collected during vulnerability assessments, site survey/inspection or implicitly by observation and complaints received from clients or personnel. Information must be collected on any weakness or flaw in the physical layout of the organisation, procedures, management, administration, hardware or software that may be exploited to cause harm to the institution, business or activity (Simonsen, 1998: 202). This information may be used to develop a vulnerability assessment document (Garcia, 2006: 306).

Procedure on collecting information on threats begins with a strength, weakness, opportunity and threat (SWOT) analysis conducted by top management of the organisation. Management should prepare a security plan identifying the threats that have the potential to adversely affect the organisation. Security information on incidents and vulnerabilities should also be considered by management in the

preparation of the security plan. The identified threats should be grouped according to their source, motivation and method of operation. This should be used to develop a threat assessment. The recorded incidents and the vulnerability assessment should be used to enrich the threat assessment. The threat assessment should be used to identify the targets to be addressed. A collection plan should be developed from the security plan for the collection of security information on the identified threats. This plan should be developed and managed by the senior security manager (Talbot & Jakeman, 2008: 33).

4.3.2 Collection plan

The Security Manager must develop and manage a security information collection plan related to the threats. Security information on incidents and vulnerabilities must be taken into consideration in the preparation of the collection plan. The Security manager must identify the threats that can become security risks of specific assets. The focus areas of the collection plan should be directed at the assets that are essential for the organisation to perform its function. It should be grouped according to the threat and consequent risk posed (Talbot & Jakeman, 2008: 33).

According to Peterson (1994: 36), and Bozza (1978: 1), a systematic plan of action for the collection of information forms the basis of any security project. A collection plan shows what needs to be collected, how it is going to be collected and by what date. A collection plan may include a survey instrument, a chronological table and possible hypotheses which one intends to prove or disprove. A collection plan is usually approved by top management of the organisation being protected (Peterson, 1994: 36).

4.3.3 Collection sources, methods and techniques

4.3.3.1 Sources

Sources for security information include intelligence sources, crime analysis, studies, professional organisations and services, published literature, government directives and legislation (Garcia, 2008: 32).

According to Smit (1989: 8-10) vulnerability may give way to a security risk. Vulnerabilities can be typified as security weaknesses. Different types of vulnerabilities may present themselves where no or inadequate security risk control measures are in place. Examples of such vulnerabilities include unmaintained fences, rusted burglar bars, holes in fences, outdated alarm systems, poor supervision of personnel, insufficient security personnel on duty, vehicles not properly searched. Information on vulnerabilities also includes information on irregular and negligent acts. This information presents itself mostly as physical evidence. Security information may be collected on the following actions:

- failure to act (an omission)while in the employ of the company;
- legal duty was not carried out;
- breach of duty;
- foreseeable Injury to other employees; and
- actual harm or injury to other employees (Fischer et al., 2008: 131).

Information on the issue of crime may be described as “crime-specific elements that distinguish both one criminal incident from another and one group of offences, related in one or more ways, from a larger group of similar offences” (Reuland, 1997: 7). Pre-defined crime data elements that may be collected include for example the modus operandi such as points and methods of entry, the suspect’s action, use of force or threats. It will also include information on a weapon and suspect’s physical descriptors (Reuland, 1997: 11). According to Van Heerden (1986: 216), crime information entails solid or liquid material which could establish an associative relationship between a person, weapon or vehicle and the crime or the victim. Crime information may present itself as either testimonial evidence or forensic evidence (Gardner, 2005: 7). The collection of crime information is important, to assess the nature and distribution of crime, in order to efficiently allocate resources and personnel.

Workplace investigations are undertaken to establish whether an act, intention to act or omission may be labelled a crime or an irregularity. This creates an opportunity for management to get to know the activities taking place in an organisation. The

information collected during the course of an investigation should be stored in the database and analysed with other information (Newburn et al., 2008: 426-427).

Before collecting information in any investigation, the investigator should prepare himself by obtaining all the relevant information that can assist him in interviewing witnesses. Information such as organisational charts, electronic files, personnel listings for potential interviews, financial statements, operational statements, public documents, press releases and internet postings may be used for this purpose, depending on the type of investigation being conducted. If there were anonymous tips, complaints or letters, this would be the time to obtain them as well (Van Rooyen, 2008: 98).

Corporate investigators are sometimes faced with intricate investigations such as white collar crimes and protracted fraud investigations. They need to gather as much information as possible, from as many different sources as possible. In any investigation, information is the key to success and a start, to the gathering of information must be made right from the beginning of the investigation (Montgomery & Majeski, 2005: 510).

According to Fischer (2004: 1), investigating officers should have the ability to recognise, collect and use crime information in investigations. Crime information collected in the investigation of crime will assist the investigating officer to reconstruct the incident, ascertain the sequence of events, determine the mode of operation, uncover a motive, discover what property was stolen, find out all that the criminal may have done and recover physical evidence of the crime (Fischer, 2004: 48).

Reuland (1997: 10); Vellani and Nahoun (2001: 27); Ainsworth (2001: 63-65); Hirschfield and Bowers (2001: 11), identify and discuss the different internal sources of crime information used by police agencies internationally. Table 4.1 shows the manner in which some of the internal sources may be used to assist in investigation.

Table 4.1: Collection of crime information from internal sources

Internal sources	Uses
Offences/Crime incident reports	Provide information on the crime-specific elements of a particular offence and serve as the basis of crime analysis.
Field interview cards	Become the primary source of field intelligence about suspicious persons interviewed at specific locations and times and about the activities of known offenders.
Evidence reports	Determine availability of latent fingerprints.
Selected calls for service	Identify times during which alarms were triggered in areas.
Investigative supplements	Provide additional crime-specific elements that result from follow-up investigations and interviews.
Arrest reports	Describe known offenders and the details of how crime was committed.
Traffic citations	Provide information about vehicle movements in key areas
Teletypes from local agencies	Track crimes across jurisdictional boundaries
Confessions from arrestees	Confirm exact modus operandi of offenders.
Intelligence files	Provide information on drug abusers and organised crime groups.

Reuland (1997: 10).

External sources refer to databases under the control of other institutions and agencies. It is used to collect and store information that may be relevant to the decision makers of another institution or agency. External sources can provide valuable information on adult career criminals and known offenders (Reuland, 1997: 8-9). According to Block et al. (1995: 87), external data sources or data banks are often geographically based and information from parole and probation officers, mental health outpatient clinics, social services offices and similar agencies located in the most probable areas, can also prove to be of value. For example, a serial

rapist in New York City emerged as a suspect after the investigator checked parolee records for sex offenders.

Reuland (1997: 9) and Block et al. (1995: 87), identify and discuss the different external sources of crime information used by police agencies internationally. Table 4.2 shows the manner in which some of the external sources may be used to assist in investigation.

Table 4.2: Collection of crime information from external sources

External sources	Uses
School records	Identify and track problem children, identify potential serious habitual offenders
Bail information	Identify suspects committing crimes while on bail
Parole information	Provide information to officers about the release of known offenders into the community
Probation information	Provide information to officers about conditions of probation related to associates, places, alcohol use, etc.
Furloughed prisoners	Track appearance of old modus operandi over a series of weekends
Other agencies	Identify and track crimes and offenders across jurisdictional boundaries
Census data	Understand the demographics of a given area

Reuland (1997: 9).

According to Reuland (1997: 9), an inter-agency database was created in Jacksonville, United States of America, along with the juvenile courts, probation officers and social service agencies, to share offender-oriented information. In a short time, information about truancy, referral rates for absences, tardiness, behaviour problems, student conduct violations and academic history was made available for the purpose of creating a multi-agency supervision and intervention plan. A clear picture of disruptive incidents and trends emerged, along with additional knowledge of how youths interact with other students. From such an analysis, troubled youths could be identified more quickly and appropriate interventions

applied more broadly. Such efforts were not possible previously, because the participating agencies had believed for a long time that information could not or should not be shared. The result was the maintenance of separate and usually incomplete files. Currently, most jurisdictions allow inter-agency sharing of juvenile information.

The Chicago Police Department is supported by a Geographic information system (GIS) called a Geoarchive. Characteristics of the Geoarchive are address-based data, information on both law enforcement and the community and an analysis that is used at community level (Block et al., 1995: 222). The Geoarchive acts as an institutionalised memory for law enforcement, holding not only law enforcement information, but also community information that is not always readily available to the local law enforcement official. The community data comes from a variety of city, state and federal agencies. The law enforcement data and the community data can be used together for decision-making and problem-solving (Block et al., 1995: 223-226).

Open source information from interviews with employees, neighbours, competitors, fire and ambulance crews, union representatives, security officers, postal employees, regular delivery drivers/suppliers and community members may serve as vital collection points (Broder, 2000: 93).

4.3.3.2 Methods

Security service providers generally use a security survey instrument to conduct a security assessment of the organisation being protected. In addition to the information included on the security survey instrument, the security official is required to use observation and interviews to obtain pertinent information that may not have been required by the security survey instrument itself. Security surveys can take the form of a standardised checklist compiled at the discretion of management or a complex report. These assessments are carried out whenever the need arises (O'Block, 1981: 254). A security survey is a critical on-site examination and analysis of an industrial plant, business, home, public private institution carried out in the light of a prevailing criminal threat. The security survey will determine the present security status, identify security deficiencies or excesses, determine the level of protection

needed and make recommendations to improve overall security (Fennelley, 2004: 141).

Early in 1994, Computer Statistics (Compstat) crime reduction strategy was instituted by William Bratton, in New York City. It started by collecting information, analysing the information and implementing strategies to reduce crime. Electronic pin-mapping software and the mainframe computer network was used to manage the crime information. It is a process which can be adopted in areas other than policing. It has since been adopted and adapted to improve other local government agencies in the USA. In practice, the development and use of the Compstat as a data source is a prime example of information led policing. It uses information technology to analyse crime, collate individual crimes in different policing areas and develop crime patterns which can indicate linkages to show the work of individual offenders, criminal gangs or syndicates and allows resources to be targeted effectively to deal with crime and the criminals (Edwards, 2011: 300-301). Managing the growth and improvement of the Compstat process is challenging, especially with regard to technology and software changes. Computer hardware, operating systems and mapping software change at a very rapid pace. The department does not adopt every software revision and operating system upgrade. Eventually, some changes do take place. In some instances new hardware may not support older software and vendors may discontinue technical support for their older products. An ongoing assessment of changing technology and its impact has become a routine part of managing the Compstat process (Goldsmith et al., 2000: 12-13).

During workplace investigations information is collected using different information collection methods. This task may be given to a corporate investigator in an organisation. A corporate investigator's function is highly skilled and challenging. As a corporate investigator he/she should have the knowledge and skills in information collection and fact-finding methods. It is the responsibility of the corporate investigator to select the most appropriate information collection method/s and use them properly to achieve the investigative objective (Smit, 1989: 4). According to Ferraro & Spain (2006: 97), although each information collection method may be used alone, the best investigation results are usually achieved by combining them in

some logical fashion. Some of the methods that can be used in collecting security information include the following:

Physical surveillance

Physical surveillance takes place by either foot or vehicle, in order to follow a subject or subjects and this is called “mobile” or “tailing” or the investigator remains in a fixed position to observe a subject or subjects and this is called a “stakeout” or “static” surveillance (Ferraro & Spain, 2006: 120).

Electronic surveillance

Electronic surveillance, which is similar to that of physical surveillance except that it is carried out with electronic technology, for example CCTV cameras, etc. (Van Rooyen, 2001: 98)

Research and auditing

Research involves the examination of information from external sources for example public records. Auditing applies to those records and documents internal to the organisation – specifically the examination of documents and information that would not normally be available to someone outside the organization. These might include attendance records, productivity reports, personnel files, etc. (Ferraro & Spain, 2006: 128).

Forensic analysis

Forensic analysis includes all forms of information gathering and analysis that employs science or scientific method. Examples include bodily fluid analysis, chemical and substance analysis, fingerprint examination and comparison, accident, crime or incident reconstruction, computer forensics, various deception and detection methods (including polygraph) and forensics document examination (Ferraro & Spain, 2006: 140). Ribaux, Girod, Walsh, Margot, Mizrahi and Clivaz (2003: 58), mention that there is considerable potential to combine forensic data within geographical information.

Undercover investigations

Undercover investigations, although complicated and difficult at times, can be of great value to the protection and preservation of corporate assets. However, undercover investigations should only be chosen as a measure when no other alternatives are available and when the company can reasonably expect a significant return on the investment. Therefore, knowing when and how to employ undercover investigations with the assistance of the SAPS and the National Directorate of Public Prosecutions (NDPP) is critical for its success (Van Rooyen, 2008: 275-279).

Interviews and interrogation

Van Rooyen (2008: 318-319), states that investigators experience the "information seeking interview" and the "admission seeking interview". There are a few skills more important to the fact finder than the ability to obtain information through effective interviews and Interrogation. Although volumes have been written on the subject, one need to examine interviewing and interrogation as an investigative tool to gather information in workplace investigations. The terms interviewing and interrogations mean different things to different people. Often these terms are used interchangeably, confusing both the user and the public. Many practitioners define interviewing as non accusatory. This technique is used to gather information. Alternatively, the interrogation technique is seen as accusatory and its purpose is to gain the truth (Ferraro & Spain, 2006: 187).

4.3.3.3 Techniques (means)

MacHovec (2006: 8), states that security officers also do electronic sweeps to detect "bugged" rooms, vehicles or equipment to prevent theft of trade secrets (e.g. a competitor's agent working undercover as an employee within the rival company/business). They also protect executives from harassment, injury, kidnapping or terrorist attacks. As undercover employees or consultants they can prevent fraud, theft, property damage or criminal acts by suppliers, employees or outsiders. Industrial security protects offices, factories, warehouses or prized possessions against damage or theft. Cyber-crime investigators detect and prevent hackers from planting viruses or stealing credit card numbers or accessing a company's information and operational databases.

The techniques or means used to collect crime information for the investigation of crime typically include the overt crime information collection technique, which can be generally defined as personal interaction with people and the covert crime information collection method. This is commonly known as intelligence gathering. The overt information collection technique is used to collect crime information through open means (Stelfox, 2009: 95). Open means of crime information collection takes place by means of personal interaction with people and the perusal of public information sources. Many of the people who may provide open source information are complainants, witnesses to crimes, victims of crimes, suspects, journalists and representatives from agencies/institutions (Van Rooyen, 2008: 218). Open means also include the collection of security information from the television, radio, scientific journals, news bureau, current affairs, grey literature, databases, images, maps, libraries, literature, academic public reports, private companies and people (Lyman, 1988: 147). Scenes of crime may also be an open means for the collection of crime information as this is the location of observable information which is gathered before it can be processed as evidence (Marais & Van Rooyen, 1990: 19).

The covert crime information collection technique is used to collect crime information in a clandestine way or closed means. Closed means of collecting crime information refers to actions of people who are generally known as informants or agent provocateurs. These informants or agent provocateurs carry out clandestine operations to obtain crime information for the investigation of crime (Matthews, 1986: 189). According to Lyman (1988: 147), closed means include the use of physical surveillance, electronic surveillance, informants and undercover officers, for the purpose of reducing crime, increasing detection rates and prevention of losses.

According to Altbeker (1998: 34), in order to move against the leader of a criminal group or syndicate, it is necessary to have information and evidence. Information can be obtained through closed means, namely, electronic interception of communication, from informers and agents. If recordings of conversations or intercepted mail are to be used as evidence, permission must be obtained for these procedures and information supplied by an informer or agent can only be used in court if the person is prepared to testify. For that reason the police tend to use agents, because, as paid police officials, they are certain to testify. Informers, on the

other hand, who are associates of the subjects, usually refuse to testify or may be discredited when they do. Police officers can provide valuable advice on the application of covert information techniques (Stelfox, 2009: 123-124).

Despite the potential for the use of closed means, there are resource constraints when using these means, as they are costly, require high levels of commitment and skill and most importantly, require visionary and innovative managers. Confidential sources need to be employed in a more proactive, strategic and targeted way, so that the benefits may outweigh the risks (Ratcliffe, 2009: 134-135). For these reasons, closed means are mainly used to guide investigations into syndicate crime. The difficulty, however, is ensuring that the information gathered can eventually be used as evidence in court (Altbeker, 1998: 34).

4.3.4 Security information collection capacity

The National Strategic Intelligence Act, No 39 of 1994 was legislated to carry out the functions as stipulated in section 210 of the Constitution of the Republic of South Africa Act, No.108 of 1996. This national legislation empowers specific government agencies to maintain an intelligence collection capacity, for the sake of national security. SAPS have a crime intelligence gathering unit which gathers intelligence for the purpose of policing (De Kock, 2011). Private security industry is excluded from this legislation. The Private Security Industry Regulatory Act, No.56 of 2001 does not provide for the management of security information in the security industry in South Africa.

Security information management in the South African security industry is not given the same attention as risk management. Emphasis is placed on the identification of vulnerabilities, studying of risks and optimising risk management alternatives. Human resources and technology are seldom used to obtain information on incidents, threats and vulnerabilities. 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 threat definition as well as the target that need to be protected. The required information need to be defined by management and organised to make it usable. The information of

adversaries may include information on motivation, potential goals based on targets, tactics, numbers and capabilities. Sources of information should include intelligence, crime studies, professional organisations, published literature, policy and legislation and many more (Garcia, 2008: 32-34).

In the United States of America the collection of security information in the private security industry is authorised by management. The information is directed at safeguarding an organisation's assets against threats. Information is collected on incidents, threats and vulnerabilities that may exploit the assets of an organisation and result in losses (Fischer et al., 2008: 149). Many security service providers use investigators to collect security information. Investigators need to master the art of information collection. Information is everywhere; investigators need to know what to look for and whom to ask. It is therefore important to encourage workplace investigations in order to maintain such a collection capacity (Nemeth, 2010: 87). Security officers only collect security information when conducting investigation on incidents for the sake of disciplinary investigations or reporting to the police.

Information collected on a daily basis is very seldom analysed or enriched as intelligence for implementation. This is because many security service providers do not have an analysis capability. This information is handled by supervisors and given to the police where necessary. According to Jordaan (2003b: 59), timely and actionable security information must be enriched into intelligence or evidence by the intelligence unit/collection unit or the investigator, who may add value to the collected information (Jordaan, 2003b: 59).

Companies also use security information companies to collect information for them. Some security companies also have their own security information collection capacity. Common businesses and industries create central repositories of security information deemed important to all their common interest nationwide and make it available in various ways to their separate groups (Fischer et al., 2008: 38-39).

4.3.5 Sharing of security information

Information-sharing is the act of exchanging information between collectors, analysts and end users to help function more effectively and efficiently. In South Africa the need to share security information with the SAPS is a necessity to ensure a reduction in crime rates and an increase in detection rates. Simultaneously, users need to protect the information made available to them. The inability or unwillingness to share this information was recognised as a weakness by the Minister of Safety and Security. He called for partnership policing between the police and the private security to improve in the sharing of information. This call, which proved to be excellent in facilitating greater information sharing, is a start to shaping policy and governance around information sharing between the private security industry and the SAPS (refer to Paragraph 1.3.3). The abovementioned statement by the Minister of Safety and Security was endorsed during 2011, by the Minister of Police when he acknowledged that private security companies contributed in reducing crime for 2010/2011(refer to Paragraph 1.3.3).

Clark (2010: 54-55) states that: " Fusion Centres and War Rooms were originally started to share information in support of homeland security in the United States of America (USA). The short-fuse synthesis (often called fusion) differs from normal synthesis and analysis only in the emphasis that time is of the essence. Fusion is aimed at using all the data sources to develop a more complete picture of a complex event, usually with a short deadline. The analyst is there to fit in any new or additional incoming data as well as anything that is immediately accessible to them in a database or in memory." The security information management companies in South Africa use the fusion centre approach to handle current incident based information, to support ongoing operations and to allow additional collection to be done in a shorter period of time. The need for this type of information has domestically led to the creation of Fusion Centres to support their clients, beneficiaries, the SAPS and other stakeholders. These Fusion Centres integrate information coming from business, private security providers and SAPS (SABRIC, 2011).

SAPS also have Fusion Centres which have been created along the lines of a war room. The SAPS War Rooms handle diverse sources and types of information on threats. These war rooms exist provincially in SAPS. Some of the so called war rooms have done very little fusion work with the private sector (De Kock, 2011).

The Private Security Industry Regulation Act, No. 56 of 2001 of South Africa, provides for the promotion of a legitimate private security industry. It acts in terms of the principles contained in the Constitution and other applicable laws. It directs the industry to act in the public and national interest in rendering security services. Section 5 of the Act, read with section 6, provides for the governance of the Private Security Industry (PSI) by the Private Security Industry Regulatory Authority. The private security industry in South Africa has for many years played a supportive role in helping the SAPS to combat crime. As a fast-growing industry, the question that comes to mind: 'Is the private security industry doing enough to support SAPS in the sharing of information of an operational and strategic value?' If not, what are the challenges and what should be done to overcome these challenges? Security information on threats and vulnerabilities should be collected on a daily basis by security service providers. It should be shared as raw information, products, techniques, strategies and/or actionable information products on an informal or formal basis with the SAPS. It will assist them in the prevention and control of crime.

According to Minnaar and Ngoveni (2004: 57), to promote partnership policing it is felt that not only the raw information should be shared but that the collection, analysis and the dissemination of information should be managed on a formal and organised basis (specifically by means of an Information Protocol).

4.3.6 Ethics in the collection of security information

In the collection of security information the gatherer must respect the law and the fundamental principles of privacy (Nemeth, 2010: 87). Information must always be collected in accordance with the Constitution of the Republic of South Africa, Act, No. 108 of 1996 and any legislation that regulates the obtaining of such information. Whenever it becomes necessary to use an information collection method, the investigator should consult with the legal advisor of the corporate for legal advice.

In the South African context, information and facts should be collected in accordance with the following legislative requirements:

- National Strategic Intelligence Act, No. 39 of 1994
- Protection of Information Act, No. 84 of 1982
- Promotion of Access to Information Act, No. 2 of 2000
- Protected Disclosures Act, No. 26 of 2000 (the so-called Whistle-blowers Act)
- The Constitution, Act, No. 108 of 1996
- Interception and Monitoring Act, No. 127 of 1992
- Section 252A of the Criminal Procedure Act, No.51 of 1977

There have been a few visible problems with the misuse of information in South Africa. This led to strong public and media criticism (De Kock, 2011). In hindsight, it is apparent that most of these problems were the result of poor management of security information.

Du Preez (1996: 16-17), states that: “the continued possession of information, from the time it is first collected until it is presented in court as evidence, must be assured – as well as its control, coordination and cumulative use”. It is important to ensure the integrity of information collected. This will avoid legal restrictions that may prevent the introduction of such information as evidence at a trial or the development of a solid case for prosecution (Gardner, 2005: vii).

The collection of information for the investigation of crime must be conducted in a lawful way, so that the evidence being presented will indeed be admissible as evidence. The evidence must also be of such a nature that the unlawful act of the accused is demonstrated beyond any reasonable doubt. For this reason, systematic and planned action is an essential part of criminal investigation (Van Heerden, 1986: 187).

4.4 ANALYSIS OF SECURITY INFORMATION

There are four types of analysis which are often used by law enforcement in combating crime. They include crime analysis, intelligence analysis, operational analysis and investigative analysis. These types of analysis may also prove to be useful to security practitioners for reducing crime, increasing detection rates and preventing losses (Gottlieb et al., 1994: 11).

Traditionally much of the analysis was carried out mentally by seasoned managers who used to pass down techniques to colleagues by word of mouth. The advent of the modern computer has, however, allowed the police and other agencies to have more sophisticated systems to help understand crime patterns (Ainsworth, 2001: 82). Analysis can be done manually or through the use of computer systems, though many agencies prefer the automated approach. Reuland (1997: 12), is of the opinion that expensive computer applications are not the answer, as they are no substitute for analytical creativity. It is usually the analyst's skill, experience and creativity that determine what to look for and computers only expedite the process.

Manual processing of actionable crime information products can be traced back to the early 1900s, when August Vollmer introduced the English technique of systematic classification of known offender *Modus Operandi* (MO). Manual analysis entails the systematic manual analysis of daily reports of serious incidents. This is done to determine the location, time, special characteristics and similarities to other similar incidents. It can also help with various significant facts that may help to identify either a criminal or the existence of a pattern of criminal activity (Block et al., 1995: 221-222).

Block et al. (1995: xiii) state that the change from manual analysis to automated analysis is important, not only because it supplements the expertise of experienced officials, but also because the knowledge and techniques accumulated over the years do not retire with a official. They are there for others to build on. Ainsworth (2001: 82), states that crime mapping and geographical profiling (which is manually done on a map by using a selection of different-coloured pins, each of which represents a crime or incident that has taken place) are useful in showing crime

hotspots and allowing decision makers to see at a glance where crime is concentrated. Such information assists managers to allocate their resources more effectively and to focus their policing on those areas which appear to have the highest rates of crime.

One of the most important purposes of crime information analysis in the investigation of crime is to identify and generate crime information products needed to assist in the investigation of crime (Goldsmith et al., 2000: 4). An analyst is responsible for turning the raw security information into timely and actionable crime information products, which can be used by an investigator for the investigation of crime. The timely and actionable crime information product is enriched into court-directed evidence by the investigator, who adds value to the crime information product (Atkin, 2000: 3). During the analysis stage, staying objective and keeping a broad perspective is crucial to success (Clark, 2010: 290).

Clarke and Eck (2003: 1), are of the view that personnel appointed as analysts should be accustomed to provide the kind of analysis results needed to support the end user. This means that analysts should:

- know how to use modern computing facilities and how to access and manipulate comprehensive databases;
- know how to use software to map incidents, to identify hotspots and to relate these to demographic and other data;
- be able to routinely produce actionable crime information products such as charts showing weekly or monthly changes in crime at force and beat level, perhaps to support Compstat style operations;
- be accustomed to carry out small investigations into such topics as the relationship between the addresses of known offenders and local outbreaks of car theft and burglary;
- carry out some before-and-after evaluations of crackdowns, say, on residential burglaries or car thefts;
- have some basic knowledge of statistics and research methodology such as that provided by an undergraduate social science degree; and

- be able to recommend security risk control measures for consideration by management.

Analysts must think of themselves as experts, knowing what works in the investigation of crime, promoting problem-solving, learning about environmental criminology, developing research skills and communicating effectively (Clarke & Eck, 2003: 2). Individual analysts should be appointed to service a team of investigators specialising in specific investigations, so that there is continuous collection, analysis and recommendations on security risk control measures (Goldsmith et al., 2000: 4).

It is evident from Reuland (1997: 64), and Redpath (2004: 36), that an organisation working with security information should have its own Security Information Analysis Unit (SIAU) with appointed analysts functioning under the control of a Manager. A SIAU ought to be seen as a sub-component of security information management. Hirschfield and Bowers (2001: 23), mention that the use of automated systems also demonstrates that with a little effort and very little analysis know-how, it is possible for an analyst to produce actionable information products by following directions on the computer system.

Most departments have at least three choices. One option is to develop an in-house analysis system. Another option is to contract with an independent vendor who would custom-design a system for the organisation. The third option is a system transfer, here the agency obtains a portion of a computer software application that was developed for or by another agency. The extent of the transferred information can occur at one of three levels, namely, concept transfers, design transfers and operational transfers (Reuland, 1997: 13).

As microcomputers become the preferred analysis platform, system transfers from more advanced departments to less advanced ones will undoubtedly become more prevalent. The advantages of the transfer option include the specificity of these programs to security information and the low cost associated with working directly with another security service provider (Reuland, 1997: 13). According to Block et al. (1995: 160), because microcomputers have become more affordable and powerful, computer applications have become a practical tool in analysis.

Analysing the information needed by investigating officers can also pose problems, especially in terms of the investigating officers' needs, the level of training of the analyst and the technical support (in terms of the operating systems, hardware and software) (Block et al., 1995: 161). The final impact of the analysis lies in the monitoring and evaluation of the application of the security risk control measures. One of the most important responses developed to overcome obstacles has been the effort to create systems of information management, as well as methods of prioritising potential suspects so that investigations can proceed in the most effective and efficient manner possible (Block et al., 1995: 67).

Peterson (1994: 6) states that knowing analytical concepts and methods in security information management will equip investigators better. This is why the majority of the people who undergo analytical training are investigators. They are not interested in analytical career paths but want to utilise the proven techniques of analysis in the investigation of cases.

4.4.1 Evaluation/verification

All security information collected from different sources must be evaluated/verified before undergoing any form of analysis. This will avoid unnecessary costs, time and energy.

According to Talbot and Jakeman (2008: 142), "the ***Admiralty Scale*** is commonly used as a technique to quality control security information received from sources. The scale provides a means of rating the reliability and accuracy of collected information through a graduated alphanumeric scale, hence determining the usefulness of the information." The reliability of the information source is assessed on criteria such as the previous quality of information provided by the source, the situation, the location and likely access of the source at the time to the information collected. Each item of information received is assessed for accuracy before the collected information is analysed for application.

Table 4.3: Admiralty scale

Reliability of source		Accuracy of information	
A	Completely reliable	1	Confirmed by other sources
B	Usually reliable	2	Probably true and accurate
C	Fairly reliable	3	Possibly true and accurate
D	Not usually reliable	4	Doubtful
E	Unreliable	5	Improbable
F	Cannot be judged or assessed	6	Cannot be judged or assessed

(Talbot & Jakeman, 2008: 142).

Once evaluated and verified the security information may undergo analysis (Talbot & Jakeman, 2008: 142).

4.4.2 Collation

All evaluated/verified security information is collated by the analyst or a data capturer using an automated system with the relevant computer software. Collation is defined as the indexing, sorting and storage of raw information (Reuland, 1997: 11-13). Raw information in itself is seldom of much value. Only when similar information is collected and considered together can the analyst provide meaning to the information (Gottlieb et al., 1994: 27). Effective threat information collation requires communication with the client that originated the threat and the interpretation of the information requirements. A limitation of many existing police collation strategies is the dominance of only the internal source of information. Over-reliance on just the internal law enforcement information sources places considerable limitations on the quality of the information (Ratcliffe, 2009: 128). To improve the quality of the information, analysts will have to enhance the collation mechanisms with information from external organisations and this brings us back to information sharing. Information collation is therefore seen as a challenge to modern policing. This includes improving of information sharing, the question of whether liaison officers

can resolve information sharing problems and the role of information from confidential informants in strategic decision-making (Ratcliff, 2009: 129-130).

4.4.3 Incident Pattern Analysis

Incident Pattern Analysis (IPA) in the security industry will consist of incident patterns of both crime incidents and policy violation incidents. Since no literature could be found on incident pattern analysis of policy violations in the security environment, the researcher decided on using the crime pattern analysis process employed by police agencies. According to Gottlieb et al. (1994: 161), crime pattern analysis contains information relative to continuing occurrence of particular criminal activities. This crime pattern analysis acquaint officers with the types of crimes being committed; lists the days, times and locations of their occurrence; and provides officers with any known suspects, suspect vehicle, modus operandi and/or property loss information. Information concerning the preferred target of attack (victim and/or property) should also be included, as should results of past analyses or predictions as to when and where suspects may strike again. Alerts should be updated until suspects are arrested or the pattern comes to an end. These crime patterns are used by officers on patrol to create directed patrols or tactical action plans. Patrol officers are given as much information as possible to enable them to develop a strategy which effectively deals with a problem (Reuland, 1997: 80). This is accomplished by providing patrol officers with a narrative description of the incidents, a map depicting past and future locations of occurrence and any graphs that clarify the problem (Paulsen, 2004: 234).

The geographic identification of patterns of crime means that certain types of similar crimes occur frequently at particular spots. By applying the Geographic Identification System (GIS) a crime pattern analysis document can be retrieved from the GIS for application by end users (Horne, 2009: 73).

4.4.4 Threat Assessment

Once the security information on the threats has been identified, the key is to consider the specific threats in a given situation. Each individual organisation has

threats that are unique. Therefore individual managers must develop the ability to do Threat Assessments (TA). A thorough threat assessment, if comprehensive and accurate will lead to the implementation of effective security risk control measures (Fischer et al., 2008: 149).

Threat is usually assessed and described using a combination of intent and the capability of a threat actor, whether individual or organisational, to attack or adversely impact on an organisation or its assets (Talbot & Jakeman, 2008: 141). Threats may vary from one organisation to another. In addition one organisation may face several different threats compared to another. This will depend on the nature of the organisation and the operations being conducted by the organisation. Threats are usually directed at specific targets. A threat also includes anything that has the potential to prevent and hinder the achievement of objectives or disrupt the processes that support them (Garcia, 2008: 26). The first activity in any security information management process is to understand the threat. It has to be determined beyond all reasonable doubt if the threat exists and the risks posed by the threat to the organisation and its assets. If the threat poses a risk, the targets for attack must be determined, so that security risk control measures may be applied (Talbot & Jakeman, 2008: 141).

People, mechanical failures or management systems can create threats. People are not only capable of deliberate actions to release hazards or cause loss, but also have the capability of applying creative intellect to their miss-deeds (Fischer et al., 2008: 149). The ability to apply intelligence enables human beings to identify and evaluate any existing security barriers and to devise and test ways of bypassing them (Talbot & Jakeman, 2008: 141).

During the analysis of security information the threat is discussed with subject matter experts and intelligence officers. Analysts review past incidents related to the threat. Open source information is also collected of the threat. Such an approach almost invariably involves some element of subjective estimation. In such situations, one way of determining the likelihood of threat occurrence is to rely on the knowledge and experiences of subject matter experts and information/intelligence collection units. All attempts to fill in the information holes should be based on their considered

contributions. Once a threat assessment has been completed, typical processes related to the application of security risk control measures would commence (Talbot & Jakeman, 2008: 142).

“Two twin drivers which are used to determine threat are intent and likelihood. They are likely attributes of the threat actor which motivates him/her to function” (Talbot & Jakeman, 2008: 143). Understanding the difference between motivation (strategic objectives) and general or specific intent is a key challenge, but one which offers insights into early countermeasures.

To identify the security risks posed by the threats, there are three specific methods which may be used to do the threat analysis. Threat analysis is an organisational security risk analysis process. A threat analysis is conducted by security risk professionals who are informed by generic risk analysis information (Talbot & Jakeman, 2008: 32-34).

1. In the *first method* the analyst must determine if the source has the potential, motive and operational capability to carry out the threat (Table 4. 4).

Table 4.4: Source, motive and method of operation

Source	Motive	Method of operation
Criminal	Profit	Theft, robbery, assault, fraud, Disclosure
Terrorist	Political manipulation	Bombing, hijacking, kidnapping, Assassination
Foreign Intelligence Services	Strategic, military, political or economic advantage	Espionage, sabotage, subversion, Disclosure
Commercial or industrial competitors	Profit, competitive edge	Industrial or economic espionage
Malicious people	Revenge, fame, discredit	Disclosure, destruction and Vandalism

(Talbot & Jakeman, 2008: 33).

2. In the *second method* the analyst should focus on the assets (functions, resources and values) that are essential for the organisation to perform its role and group them according to the threat and consequent risk posed (Table 4. 5).

Table 4.5: Organisations assets, risks and threats

Organisations assets	Risks	Threats
Buildings, facilities	Destruction, damage, unavailability of the building or facility	Fire, explosion, hoaxes, power failures, contamination, unauthorised access
Information systems	Loss or compromise of security classified material, loss of confidentiality, availability or integrity of information	Unauthorised users, forensic disc examinations, careless handling of printout, careless transmission
Management's confidence in the business unit or program	Loss of management or public confidence in the business unit or program or its processes	Mishandling of sensitive data, inconsistent policy or service delivery, adverse media coverage.
Organisational reputation	Loss of organisational reputation	Poor service, mishandling of sensitive data, inconsistent policy or service delivery, adverse media coverage

(Talbot & Jakeman, 2008: 33).

3. In the *third method* the analyst should look at the organisational exposures or vulnerabilities and to then use them to review the suitability of existing security controls (Table 4. 6).

Table 4.6: Asset group and possible exposures or vulnerabilities identified

Asset Group	Possible exposures or vulnerabilities identified
People assets	Assassination Bombing Civil Crime disorder Disgruntled employees Discrimination/prejudice Attack, assault or harassment Sexual harassment Domestic violence Inadequate procedures/training/vetting Loyalty/coercion/collusion/corruption, Mismanagement Reluctance to adopt security policy Workplace violence Public perception Staff attraction Conferences/exhibitions Cultural or religious differences Financial stress or gain Impersonation as staff member
Information assets	Destruction or corruption Disruption of service Inadvertent disclosure Leakage Manipulation of data/information Staff loyalty Fire/arson Sabotage Fraud
Physical assets Information and communication technology	Break-in Hacking Fire

	Maintenance Vandalism Theft Commercial espionage-electronic surveillance/ listening device Inadequate emergency management procedures Failure of equipment, e.g. maintenance and reliability Inadequate threat details Procurement methodology Mail handling Funding

(Talbot & Jakeman, 2008: 34-35).

4.4.5 Vulnerability Assessment

Physical Protection Systems (PPS) includes all security products and technology. The primary functions of these PPS are detection, delay and response. Both quantitative and qualitative methods of Vulnerability Assessment (VA) may be conducted on PPS. It is very important to determine before the start of the assessment whether a quantitative or qualitative assessment method will be used. Quantitative assessments are recommended for facilities with huge asset losses. Qualitative assessment can be used if the asset values are much lower. When performing VA, the general purpose is to evaluate each component of the PPS to estimate their performance as installed at the organisation. Once this is done an estimate of the overall system performance is made. The key to a good VA is accurately estimating component performance (Garcia, 2006: 9).

When using a quantitative approach, this is done by starting with a tested performance value for a particular PPS component, such as a sensor and degrading its performance based on how the device is installed, maintained, tested and integrated into the overall PPS. For qualitative analysis, performance of each component is degraded based on the same conditions, but the performance of the device is assigned a level of effectiveness, such as high, medium or low rather than

a number. In addition, component performance must be evaluated taking into consideration the weather conditions, the existing condition of the organisation and all the threats affecting the organisation (Garcia, 2006: 9).

When vulnerability assessment is dealt with as part of the security management cycle, it should be a continuous process (Garcia, 2006: 10).

A vulnerability assessment is carried out by collecting information on the PPS. The specific PPS is checked if it could detect an intrusion, generate an alarm and then transmit that alarm to a location for assessment and response. The organisation is reviewed to determine if it conformed to all legal and administrative compliance requirements. A checklist is used to document the presence or absence of components and component parts. A deficiency report is prepared with notes if the component is out of compliance. The VA report summarises these findings and the organisation makes improvements according to its organisational policy (Garcia, 2006: 32).

4.4.6 Criticality Assessment

According to Talbot & Jakeman (2008: 154), criticality assessment is a vital step in the identification of risks. It assists in the prioritisation of threats and understanding of an organisations' vulnerability to those threats. It also assists with risk identification as well as analysis and the application of security risk control measures in order to focus on priority assets that are of utmost importance to an organisation. Criticality assessment determines the probability of loss due to an incident, threat or vulnerability and the impact the loss will have on the organisation.

4.4.6.1 Probability

Once security information on incidents, threats and vulnerabilities have been collected and analysed, it is essential to determine the probability of loss. When security managers are confronted with a series of problems, they must determine which problems need immediate attention. According to Le Roux (2004: 19-27) and Fischer et al., (2008: 157), probability is a mathematical statement concerning the

possibility of an event occurring. Unfortunately such mathematical precision must wait until various subjective security measures can be turned into numerical values.

The best we can do today is to make subjective decisions about probability. Such decisions should be based on data such as the physical aspects of the incidents, threats and vulnerabilities being studied. For example criminal acts, spatial relationships, location and composition of the structure. Procedural considerations must be studied together with the policies of the organisation. The history associated with the industry is of great importance, particularly the incident, threat or vulnerability being studied. The essential question is: How likely is it that a particular threat event will take place? Has the product been a target before? What is the current situation regarding the threat (Fischer et al., 2008: 157).

4.4.6.2 Impact

To separate the security information on incidents, threats and vulnerabilities into finer categories, security managers use the principle of criticality. The term has been defined as the impact of a loss in Rands (South African currency of money). The impact of the threat is an approximation based on the organisation's prior experiences and the experiences of similar companies in similar situations. Rands are the customary measure of impact. The security manager must take into consideration the costs of replacement, repair, lost productivity, forfeiture of business opportunity, clean-up, litigation, damage to reputation and undermining of customer goodwill. Even when the impact is upon human life, the yardstick is a Rand value (Fischer et al., 2008: 157). The impact is also determined by the following:

1. replacement cost (other indirect costs);
2. temporary replacement (hiring costs);
3. downtime (business is not as usual);
4. discounted cash (withdrawals from investment);
5. insurance rate changes (increase in premiums); and
6. loss of marketplace advantage (product cannot be delivered on time) (Fischer et al., 2008: 157-158).

Impact is an extremely important concept for security managers to understand. In general, company managers who usually think in terms of cost/benefit analysis will not be interested in spending money for security if the cost is greater than the potential loss of money. Impact, much like probability, is a subjective measure, but it can be placed on a continuum. Using the rankings generated for probability and impact and devising a matrix system for various security risks, it is possible to quantify security risks somewhat and to determine which risks merit immediate attention. Using the matrix, probability and impact alphanumerical values can be assigned to each security risk. If a choice has to be made, impact should take precedence over probability. If for example the security risk is Robbery, then the criticality assessment may be interpreted in terms of the Table 4. 7 as 1D (probability of occurrence is virtually certain and the impact will be serious) (Fischer et al., 2008: 157-159).

Table 4.7: The Probability/Impact matrix

Probability	Impact
1. Virtually certain	A. Fatal
2. Highly probable	B. Very serious
3. Moderately probable	C. Moderately serious
4. Probable	D. Serious
5. Improbable	E. Relatively unimportant
6. Probability unknown	F. Critically unknown

(Fischer et al., 2008: 159).

4.5 IMPLEMENTATION OF SECURITY RISK CONTROL MEASURES

The analysis of the collected security information will identify specific risks that will need security planning. These risks will require the implementation of specific security risk control measures. The security risk control measures may take the form of physical protection systems, strategies and actionable crime information products (Fischer, 2008: 173).

4.5.1 Determine objectives for security risk control measures

The first step in the process is to determine the objectives for security risk control measures. To formulate these objectives, the designer must understand the organisations operations and conditions, define the threat and identify the target (Garcia, 2008: 15).

4.5.1.1 Organisational description

A thorough description of the organisation and the processes within the organisation is required. This information can be obtained from different sources, including the organisational design blueprints, process descriptions, safety analysis reports and environmental impact statements. A tour of the organisation and interviews with the personnel are necessary. This will provide an understanding of the physical protection requirements for the organisation as well as an appreciation for the operational and safety constraints. Additional consideration will also include an understanding of liability and any legal regulatory requirements, which must be followed. Each organisation is unique, so this process should be followed each time a need is identified (Garcia, 2008: 3)

4.5.1.2 Threat definition

In defining the threat, specific information needs to be considered. If this information has not yet been collected, additional tasking needs to be given for the collection of this information. The additional information needs to answer three questions about the adversary:

1. What class of adversary should be considered?
2. What is the range of the adversary's tactics?
3. What are the adversaries' capabilities?

(Garcia, 2008: 4).

Adversaries can be separated into three classes: outsiders, insiders and outsiders working in collusion with insiders. For each class of adversary, the full range of tactics (deceit, force, stealth or any combination of these) should be considered.

Deceit is the attempted defeat of a security system by using false authorisation and identification; force is the overt, forcible attempt to overcome a security system; and stealth is any attempt to defeat the detection system and enter the facility covertly. For any given facility there may be several threats, such as a criminal outsider, a disgruntled employee, competitors or a combination of the above. The PPS must be designed to protect against all these threats. Choosing the most likely threat, designing the system to meet this threat and then testing to verify the system performance against the other threats will facilitate the process (Garcia, 2008: 4).

4.5.1.3 Target identification

Finally target identification should be performed for the organisation. Targets may include critical assets or information, people or critical areas and processes. A thorough review of the organisation and its assets should be conducted. Such questions as “What losses will be incurred in the event of sabotage of this equipment?” will help identify the assets or equipment that are most vulnerable or that create an unacceptable consequence (Garcia, 2008: 4).

4.5.2 Design security risk control measures

Given the information obtained in the facility characterisation, threat definition and target identification, the designer can determine the protection objectives of the PPS. Examples of protection objectives may be to detect and arrest the adversary, prevent the criminal conduct or irregularity of the adversary, create awareness to prevent losses (Garcia, 2008: 4).

4.5.2.1 Physical protection systems

The next step in the process, if designing a new PPS, is to determine how best to combine elements such as fences, barriers, sensors, procedures, communication devices and security personnel into a PPS that can achieve the protection objectives. The resulting PPS design should meet these objectives within the operational, safety, legal and economic constraints of the facility. The primary

functions of the PPS are detection of an adversary, delay of the adversary and response by security personnel (Garcia, 2008: 5).

4.5.2.2 Strategies

Some situations may require immediate action and prompt intervention. Some are cyclical, managerial and are amenable to technical solutions and problem solving methods. Others are chronic, endemic difficulties that require the application of strategies over time, to change conditions and move an organisation ahead. The security manager needs to know the differences amongst these, what knowledge is required and how to access it though personnel or other means. Additionally, the security manager must explore the adequacy of the concepts from the knowledge base and how and when to apply them (Opolot, 1999: 144). The challenge is for security managers to stay current on innovative design strategies to couple this knowledge with the latest information on issues of changes in cultural values, crime, technology, market conditions and political conditions (Opolot, 1999: 229). Some examples of strategies may include crime prevention through environmental designing, business watch, car guard watch, neighbourhood watch, awareness, sharing of information, electronic networking with other service providers and organisations. Many of these have served as best practices in the law enforcement environment.

4.5.2.3 Actionable crime information products

According to Peterson (1994: 29-59); Goldsmith et al., (2000: 6); Hirschfield and Bowers (2001: 4-6), crime information products commonly used by law enforcement are as follows:

- case docket analysis: this is the overall study of investigation dockets to provide recommendations for its successful completion;
- activity flow charts: these are used to explain the paper trail in complex investigations, such as money laundering, commercial fraud, etc.;
- tables: all data is placed in tabular format to ascertain any commonalities or patterns. In a series of armed robberies, for example, the factors may include:

time of day, location, type of establishment robbed, number of perpetrators, use of weapons, language spoken, manner of dress of perpetrators and the type of financial instruments taken;

- matrices: these are used in analysis to organise data in such a manner that it can be compared to similar data. The triangular matrix is commonly used as an association analysis matrix. For example, with names of crimes on one side and the names of places where the crimes occur on the top side, thus connecting at a triangular point, indicating a connection or commonality;
- collection plan: this is a preliminary step towards completing a strategic assessment, which shows what needs to be collected, how it is going to be collected and by what date;
- criminal profile: this is the product of criminal investigation analysis in which indicators of behaviour and activity are used to create models. A profile is created by gathering all possible information on a type of behaviour or occurrence and then analysing and comparing that behaviour to cases or incidents on hand;
- assessments: these are a product of the strategic analysis process. They are written reports which can include the results of surveys, independent research, information gathered from independent case dockets and data received from other law enforcement sources;
- analytical briefings: these are oral presentations of findings or products based on the data analysed;
- maps: these depict the location of offences, victims and, occasionally, offenders. They can provide information concerning the location of crime hotspots or high levels of reported crimes;
- crime analysis: traditional crime analysis includes both the breaking down of criminal incidents into their composite parts (factors) to determine patterns and similarities, which may lead to the apprehension of the perpetrator(s) and also the statistical analysis of crimes to forecast future crimes. Information on a series of crimes which have been committed is used to complete a crime analysis. This information may include victim data, suspect data, dates, times and location of crimes, physical evidence, weapons used and the fruits of the crimes;

- linkage analysis: correlates a suspect to one or more incidents. It can narrow search areas by identifying known criminals or other suspects who reside within a certain distance from incident locations. The objective of linkage analysis is the apprehension of suspects and case clearance;
- association analysis: depicts the relationships among people, groups, businesses or other entities in a way that provides the investigator with information on the nature of the group and the manner in which the group interacts;
- criminal investigative analysis: this entails the use of components of a crime and/or the physical and psychological attributes of a criminal, to ascertain the identity of the criminal. This technique has been used by the FBI in the area of homicide and sexually motivated crimes. Some analysts refer to it as profiling. In fact, a profile of a criminal is a product developed as a result of the criminal analysis process;
- statistical analysis: this is a review of numerical data to summarise it and to draw conclusions about its meaning;
- pie charts: these are used to give a graphic depiction of the parts of a whole; the pie equals the whole of something and the slices equal smaller parts. They are applied by law enforcement to show the occurrences of particular crimes in relation to the overall crime rate or the relative amounts/percentages of income from illegal sources. A bar chart is a graphic depiction of a certain activity in relation to or in comparison with another factor such as time, cost or another occurrence – both of which can generally be measured in numbers. It can be used in conjunction with a number of other analytical techniques;
- composite tables: all data is placed in tabular format to ascertain any commonalities or patterns. In a series of armed robberies, for example, factors may include: time of day, location, type of establishment robbed, number of perpetrators, use of weapons, language spoken, manner of dress of perpetrators and the type of financial instruments taken. The information known about each of the armed robberies committed could then be put in tabular form. The table would then be reviewed for possible patterns, commonalties and differences. Conclusions about the persons responsible for the robberies might then be drawn;

- automated mapping: automated pin-mapping, hotspot analysis and radial analysis are a few of the most extensively used. They can be used to identify the locations of high concentration of crimes, known as hotspots. An investigator may use intelligence and modus operandi data to identify that the same offender is likely to be responsible for a series of incidents;
- geographic flow mapping: this is a simple graphic depiction of a specific region, used to show some activity or occurrence related to criminal activity. Information gleaned from a map can relate to territories covered by a crime group or to sources and routes of goods or services being transported by crime groups;
- target profiling: this identifies locations that may have an unusually high likelihood of victimisation within an active pattern area. Within a large geographic area, offenders tend to target certain types of locations rather than others, especially for crimes influenced by the location of commercial or service-oriented activity, such as convenience stores or banks;
- offender movement pattern analysis: ties at least two or more points to one or more criminal incidents. One example is the theft location and recovery site of a stolen motor vehicle. Connecting the two locations – theft and recovery – may help identify the roads used by an offender after stealing an automobile. Similarly, relating an offender‘s last known residence to an arrest location, such as an open air drug market, can identify roads used by dealers to transport drugs; and
- forecasting: this is a process which predicts the future on the basis of past trends, current trends and/or future speculations. Within the field of analysis, both numeric and descriptive forecasting are done. Numeric forecasting is numerically used and generally rests on past and current numbers of occurrences. Descriptive forecasting takes both quantitative and descriptive trend data to predict the future. Forecasting is used both in crime analysis and strategic analysis.

The abovementioned actionable crime information products may be used to reduce crime, increase detection rates and prevent losses.

4.5.3 Dissemination of analysis products

Peterson (1994: 271), describes dissemination in the security information management process as the release of analysis products to a client, under certain conditions and protocols. It is usually based on the security classification of the information and the security clearance of the client. Jordaan (2003a: 59), refers to dissemination as vital, as it encompasses information that was collected, analysed and which must be packaged and delivered to the clients and stakeholders who can use it. The incident pattern analysis product from analysts can prompt an immediate response from the specialised anti-crime surveillance units. Taking a proactive approach is likely to reduce future incidents to be committed by the perpetrator. In a similar way, the officials may request analysts for listings of possible incidents where an arrestee may be involved. Analysts can also assist investigators with suspect and victim profiles (Reuland, 1997: 28-29). Dissemination can be carried out in several different ways, namely, by attending briefings and strategy sessions, presenting verbal reports, providing written reports, having face-to-face contact whenever the need arises and public information systems for both written and electronic media (Reuland, 1997: 35).

4.5.4 Feedback on analysis products

The last phase of the security information management is feedback. Analysts should not go blindly forward from day to day, without knowing which output products and formats (written reports, charts, graphs, overheads, computer-generated presentations and maps) work and which do not. Analysts spend a great deal of time preparing analysis products and must know how the end users plan to use the final product and how useful it was for them. Additionally, if the end users view the analysts' output as non-responsive to a request, they may not make additional requests. Either scenario wastes effort and compromises efficiency. To obtain feedback, analysts should routinely include a survey form with the prepared analysis report (Reuland, 1997: 36-37).

4.5.5 Monitoring and evaluation of security risk control measures

Monitoring and evaluation of the security risk control measures begins with the review of the PPS design and thorough understanding of the protection objectives the designed system must meet. This can be done simply by checking the required features of a PPS, such as intrusion detection, entry control, access delay, response communications and response force. 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).

4.6 CONCLUSION

A professional security service is fast gaining momentum in South Africa. Citizens are looking out for every new physical protection system backed up by the latest technology and/or piece of equipment that can safeguard property and give protection against criminal elements. Changes and developments in the security service environment demands new innovations and creativity to enhance traditional models. A literature study was conducted to enhance the traditional ways of managing security information. There was limited literature in South Africa on security information management. The researcher was compelled to focus on international literature for the theoretical framework. The Information Management and Crime Analysis Model used in law enforcement was found to be a success both internationally and nationally. The Model was studied and customised to the security service environment.

CHAPTER 5

CASE STUDIES ON SECURITY INFORMATION MANAGEMENT

5.1 INTRODUCTION

The aim of this chapter is to focus on security information management practices used by security service providers in the Gauteng province of South Africa and in Perth, Western Australia. Case studies on security information management were conducted in Gauteng, South Africa and in Perth, Western Australia.

The South African case studies revealed that security information on crime incidents are managed differently to incidents related to policy violations, threats and vulnerabilities. Crime incident information in South Africa is managed by SAPS. In major business entities such as banks, petroleum companies, retail, etc. crime incident information is also co-ordinated and managed by security information management companies. Threats are reported to the SAPS and handled internally by individual companies. Vulnerabilities and incidents related to policy violations are expected to be managed by individual security service providers.

The case study conducted in Perth, Western Australia (WA) was co-ordinated with the assistance of the School of Computer and Security Science in the Faculty of Computing, Health and Science, Edith Cowan University (ECU) in Joondalup. During May 2011, the researcher spent a three week research period at ECU in Perth, Western Australia conducting the case study. In Western Australia, security information on threats and vulnerabilities are managed differently to incident information. Threats are reported to the police and handled internally by individual companies. Threat information is also shared with network forums in Western Australia. Crime incident information is managed by the Western Australian Police (WAP). Information on vulnerabilities and incidents relating to policy violations are managed by individual security service providers.

5.2 CASE STUDY STRATEGY OF ENQUIRY

The case study strategy of enquiry can be best described as an intensive study of a single or collective type of cases with the aim of generalising across a larger set of cases of the same general type (Gerring, 2007: 65). The case study strategy provided for an intensive study of security service providers operating in Gauteng in South Africa and from Perth in Western Australia. The collective type of case study research helped the researcher to obtain a better understanding of a larger group of similar companies operating nationally and internationally. Evidence was collected by conducting semi-structured interviews using an interview guide (See Appendix1).

5.3 SECURITY INFORMATION MANAGEMENT IN SOUTH AFRICA

5.3.1 Case Study 1: Government departments, South African Police Service and the South African Private Security Industry

5.3.1.1 Background

Since the late seventies private security development in South Africa was supported by government. Government encouraged the development of the private security industry to fill the vacuum left by the police in the safeguarding of strategic installations. In 1980 the National Key Points Act, No. 102 of 1980, was passed. This granted greater powers to the private security guards who were tasked to guard and protect identified strategic installations. The Act granted full powers of arrest, search and seizure to security officers in pursuance of such task (Irish, 1999: 1).

Over the years the private security industry in South Africa has undergone tremendous change. Not only has it seen a growth in the numbers of personnel but also a proliferation and expansion of different sectors in terms of specialisation. In addition, it has also seen a number of changes to its regulatory legislation and controlling framework. All these factors have impacted on the focus, profitability and future expansion of the industry. With reference to the regulation there has over the years been a long process of legislative amendments and regulatory changes aimed at better controlling and monitoring the private security industry in South Africa,

specifically in terms of registration, compliance and training standards. Starting with the South African Security Officer's Act, No. 92 of 1987 and the introduction of the Private Security Industry Regulation Act, No. 56 of 2001, a strong regulatory framework for controlling and managing the South African Private Security Industry was established. The Private Security Industry Regulation Act, No. 56 of 2001, essentially set up the Private Security Industry Regulatory Authority (PSIRA) (replacing the Security Officers' Board), as well as obliging every security company inclusive of in-house security to register as a 'security service provider' and to have its personnel registered as well. The Act incorporated provisions for a new Code of Conduct and the Improper Conduct Regulations. Furthermore, it established an inspectorate with increased powers of inspection of all registered security service providers with powers of prosecution and reporting of charges of misconduct (Minnaar, 2007: 3-4).

Private security has grown steadily, since then identifying market opportunities in government departments and expanding its influence in the realm of community and neighbourhood policing and community safety networks in South Africa (Minnaar, 2010: 203). As of 22 October 2010, 7459 security companies were registered with PSIRA in the Republic of South Africa. These companies employed 387 273 security officers to work in the Republic of South Africa. As of 4 October 2011, PSIRA currently has 411109 registered security officers and 8828 security companies registered on the PSIRA database (Private Security Regulatory Authority (PSIRA), 2012).

Information is an extremely valuable tool for use by security officials, investigators and police officers for the reduction of crime, to improve detection rates and prevent losses. It is a key element in the sequence of events aimed at conceiving, implementing and evaluating measures to mitigate security risks (Ekblom, 1988: 1). It has proven to be an integral part of the skills package of specialists and experts, whose job it are to prevent and investigate crime and losses successfully. It helps them in reducing crime, making arrests, solving crimes and preventing losses. It is useful for security officials, police officers and investigators to know if a specific crime is on the increase, in which geographic part it is occurring, who is most likely to be committing it and where the offender(s) can be found (Lyman, 1988: 147).

Conducting analysis on security information makes it possible to devise security control measures appropriate to the local crime problem and its physical and social context. The implementation of these measures will require a great deal of commitment, coordination and perseverance. The form of evaluation of the preventative measures will depend on the broader context of a preventative initiative. Evaluation enables managers and practitioners to decide whether the initiative in question has had a sufficient impact on crime to be worth continuing, amending or extending (Ekblom, 1988: 4-7). The involvement of former intelligence and police personnel has had a marked impact on the security information management skills of private security companies in South Africa (Irish, 1999: 13). This has also helped build a good working relationship between the private security officials and the SAPS (Interview no. 3).

5.3.1.2 Government departments

Government departments in South Africa have in-house security structures established within departments. These security officials are also registered with PSIRA. They possess civilian powers in terms of the Criminal Procedure Act 51 of 1977. Some in-house security officers employed by specific government department are empowered by national legislation relevant to the specific government department to carry out their responsibilities. Depending on the business case of the government department, they work with security information on incidents, threats and vulnerabilities. Crime incident information is reported to the SAPS for investigation. Threat information is reported to SAPS. Government departments address vulnerabilities by applying security risk control measures to mitigate risks. Incidents related to policy violations are investigated by internal investigators from the human resources section. According to those interviewed for this study, the collection and analysis of security information and the implementation of security risk control measures are not regulated in their departments. No policy framework was made available by any one of the service providers interviewed. The internet search engines could not provide any such policy frameworks (Interview nos. 1 & 2).

Security information is mainly collected by conducting security assessments. Voluntary information is also received from third parties. ‘Hot-line’ information is

collected by providing toll-free telephone numbers to the public. Some of the methods used to collect security information include surveillance, research (external sources), internal audit (internal sources), forensics and interviews. In some instances undercover operations are implemented together with the SAPS. This activity is usually led by the SAPS. The collected information is entered manually in specific registers (occurrence book, case registers). Security officers in government departments mainly direct their efforts on information collection pertaining to vulnerabilities and incidents related to crime and policy violations. The collection of this type of security information helps them understand the threats facing the department. All criminal matters are referred to the police and incidents of policy violations are investigated by workplace investigators. Much of the information is not complete. In most instances information is received late and not on time. Information obtained through direct interviews is always valid and reliable (Interview nos.1 & 2).

In most cases the collected information is analysed by management and a decision is made on security risk control measures. Very seldom do departments use analysts to evaluate, collate and analyse the information. In some instances ordinary clerks are used as analysts to determine trends and patterns pertaining to crime. They use computer software to collate and analyse the information. The computer software produces crime pattern analysis products. Vulnerabilities are given attention according to the threat they pose. The likelihood and consequences of the threat is considered by management at their meetings. Under normal circumstances no formal analysis is done on threats and vulnerabilities. Management makes decisions based on the security information placed before them. If the situation warrants it, security risk control measures are implemented based on affordability. There was no indication of probability, impact and cost benefit analysis being done in this regard. In many instances there was a dire shortage of personnel, computers and the correct software to collate and analyse the information. If additional information is required, risk managers, security officers or investigators are used to collect this information. Information is classified and handled in terms of the Minimum Information Security Standards (MISS) document[7] (Interview nos. 1& 2).

[7] Minimum Information Security Standards (MISS) document was approved by the South African Cabinet in 1996, for implementation in all government departments in South Africa.

5.3.1.3 South African Police Service

Legislative frameworks are provided to regulate the collection of crime intelligence in the country. The South African Police Service has a General as its National Commissioner, Lieutenant-Generals as Provincial Commissioners, Major-Generals are Cluster Commanders and Brigadiers and lower ranks are positioned at police station level. SAPS personnel are provided with guidelines and directives on the management of crime information and intelligence. In terms of security information management SAPS manages information on crime incidents, crime intelligence and threats. They do not manage information on private security vulnerabilities (Reddy, 2010).

All crime incident information reported by victims and complainants are captured on an automated Crime Administration System (CAS) by SAPS Crime Information Officers (CIOs) at police station level. The information is validated by supervisors and entered into automated systems by data capturers. This information flow starts from the police station level and moves upwards through the automated system to the provincial office and on up to the national office. The information is protected through classification in terms of the MISS policy document. The information may be accessed by anyone who has valid access to the information. If the person is not allowed to access the information, access will be denied by the CAS (De Kock, 2011).

The Business Intelligence System (BIS) is used by the Crime Information Analysis Centre (CIAC) to analyse the crime information at police station level. Crime Information Officers (CIOs) at police station level are involved in field work to gather crime information through interviews and visiting scenes of crime. The collection of this additional crime information is primarily used for addressing the what, why, where, who and how aspects of crime. The new information is used to add value to the existing information on the BIS so as to generate actionable crime information products for operationalisation at police station level. Some of the actionable crime information products generated by the Crime Information Analysis Centres (CIAC) include crime statistical analysis, crime pattern analysis, geographic crime analysis, linkage analysis, case docket analysis and profiling. The integration of all the

information from these actionable crime information products helps generate a Crime Threat Assessment (CTA) document at police station level. At police station level, some of the relevant crime information is shared at Community Policing Forums (CPFs) (De Kock, 2011 & Interview No. 3).

This CTA of the police station is integrated at Cluster level with the CTAs of the cluster police stations. Hence, a Cluster CTA is generated. Linkage analysis is done on the information from the cluster stations. The linkage analysis product is provided to the Crime Intelligence Commanders at Cluster level. The information is enriched to produce crime intelligence. The crime intelligence is used to effectively, efficiently, proactively and reactively conduct intelligence led policing in the Cluster (De Kock, 2011).

At Provincial level the Cluster information is integrated into a CTA document for Intelligence led Operations. This intelligence is enriched by security service providers both from private security and government. The Provincial Office has a structured 'War Room' which is used to obtain information from these and other and stakeholders in the fight against crime. Crime Intelligence is not shared with other stakeholders, unless authorised by the Provincial Commissioner (De Kock, 2011).

The information provided by the Provincial CTA is considered at National Level to address organised crime using unconventional methods such as undercover operations and specific surveillance methods (De Kock, 2011).

At all levels different methods are used to collect information. Some of the methods include physical surveillance, electronic surveillance, forensics, interviews, research, audits and undercover. Crime Combating Forum (CCF) meetings are held daily at Station, Provincial and National levels with all stakeholders including private security and other government departments, so that the application of information and intelligence can be monitored and evaluated through crime statistics, arrests, recoveries of exhibits, etc. (De Kock, 2011; Reddy, 2010).

All threat information received from other stakeholders such as private security and government departments are integrated into the CTA at the different levels (De Kock, 2011).

5.3.1.4 South African private security service providers

Security service providers in Gauteng handle security information on a daily basis. They collect security information on threats, vulnerabilities and incidents. The security information on incidents comprises mainly of crime incidents and to a lesser extent information on policy violations. All of the security service providers involved in the case study collects security information. In most instances information is collected during security surveys and by investigators involved in workplace investigations. Some of the methods used to collect security information include surveillance, research (external sources), internal audit (internal sources), forensics, interviews and undercover. Undercover sources are used in consultation with the SAPS. The case study showed that more security information is collected from internal sources compared to external sources. Most of the internal source information consists mainly of reactive information on crime incidents and irregularities which have already taken place at the facility. This was followed by internal information collected on vulnerabilities using surveillance techniques and security assessments. Much of the external information consists of threats received through hotline reports (toll free) and informer networks. External information on threats mainly originates from other security service providers organisations, forums and security networks (Conradie, 2010; Interview nos. 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16 & 17).

The majority of the security service providers do not have specific security persons assigned for the collection of security information. Only a few larger companies have collection units, risk managers or investigators assigned for the collection of security information. This is mainly because of the cost involved in establishing such a capacity. In most cases the security information is recorded in occurrence books and archived. Security assessments are done during specific intervals. Many security service providers outsource security assessment functions to Risk Management Companies They are carried out to a lesser extent by in-house security managers

due to a lack of knowledge and skills in this regard (Conradie, 2010; Interview nos. 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16 & 17).

All day-to-day incident based information is directed to a supervisor and manually recorded in an occurrence book or other similar types of register books. In some instances they are entered into automated systems for acknowledgement by top management. This is seldom done. Criminal incidents are reported to the SAPS, who register a case docket for investigation. Criminal incidents relevant to specific business entities are also reported to specific information management companies. SAPS is also informed of all security information on threats, so that responsible intelligence structures in terms of the National Strategic Intelligence Act, No. 39 of 1994 may be activated. The security service provider also initiates strategies in consultation with the police. Security information pertaining to incidents on policy violations are handled by workplace investigators or the human resource section of the company (Conradie, 2010; Interview nos. 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16 &17).

The day-to-day security information received by management is discussed at management meetings and decisions made to manage the risk. They either inform the police, human resources section or investigators of the incident or threat. Information on vulnerabilities is handled according to the threat it poses. In many instances supervisors analyse the information for operationalisation. Only large security service providers have in-house general analysts or specialist analysts. In the majority of cases if additional information is required, security managers, risk managers or investigators are tasked to obtain additional information (Conradie, 2010; Interview nos. 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16 &17).

When security assessment reports are received from Risk Management Companies, management makes a decision on the implementation of security risk control measures. These decisions are based on the financial position of the companies and the assets being protected. In residential and business complexes, many clients are reluctant to pay an increased premium to implement specific security risk control measures as recommended by the security assessment reports. Consequently, much of the needed security risk control measures are not implemented or are

shelved for the new financial year for consideration (Conradie, 2010; Interview nos. 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16 & 17).

Many of the security service providers apply security information to identify crime trends and patterns and investigative leads. The application of the security information is evaluated by comparing criminal incidents to previous periods (Conradie, 2010; Interview nos. 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16 & 17).

In recent years specific security information management companies have proven to be successful within specific sectors. Case studies were conducted with three of these security information management companies (SABRIC, CGRI, PSI) to identify their practices (Conradie, 2010; Interview nos. 36, 37 & 38).

5.4 SUMMARY

The above case study presented a background to security information management in South Africa. Although security information is a valuable tool for use by security officials, no legislative direction is provided to the private security industry on how to manage security information. Government departments collect security information on incidents, threats and vulnerabilities. Managers in the government departments make decisions for the implementation of security risk control measures based on the incident information. Many of these departments and companies do not have an analysis capability to analyse incidents, threats and vulnerabilities. The SAPS manages crime information on threats and incidents of crime but not vulnerabilities. They have a collection capacity for crime intelligence and a formal analysis capability of crime analysts. Private security companies handle security information on incidents, threats and vulnerabilities as they are received. Decisions are made by management on the implementation of security risk control measures based on the collected information. Many of the private security service providers do not have an information collection capacity nor do they have a formal analysis capability. The views presented in this case study by the different stakeholders might be similar to a certain extent, because they all addressed the same research questions of the study.

5.5 SECURITY INFORMATION MANAGEMENT BY SOUTH AFRICAN ORGANISATIONS AND COMPANIES

5.5.1 Case Study 2: South African Banking Risk Information Centre (SABRIC)

5.5.1.1 Organisational structure

South African Banking Risk Information Centre (SABRIC) is a section 21 security risk information management company which was established in 2002. It manages and collates crime incident information collected by its clients, analyses the crime incident information and recommends strategies and/or provides actionable crime information products aimed at mitigating organised bank related crimes. SABRIC adopted a centralised approach to information management, crime analysis and the application of recommended strategies and/or actionable crime information products. It is managed by a Chief Executive Officer (CEO), who is supported by a Business Support Office, Commercial Crime Office and Violent Crime Office. Clients (mainly banks/financial services organisations) of this company mandated the CEO to do information management, crime analysis and recommend strategies and/or provide actionable crime information products to its clients, partners and stakeholders. The clients contribute financially, partners mutually benefit and the stakeholders have a stake in the company (Interview no. 36).

Purposive interviews were conducted with senior managers from the Violent Crime Office. The infrastructure of the Violent Crime Office consists of a Consequence management office and Information office. Both these offices operate in an integrated fashion to address the strategic objectives of the company. The strategic objectives of the company include:

- developing a credible and actionable crime information repository;
- providing leadership that delivers quality services/products and effective strategies to tackle bank related organised crime;
- coordinating a range of activities to reduce bank related crime;
- optimising inter-bank cooperation;

- optimising beneficial public private partnerships by interfacing with a range of external organisations, most notably, government departments, law enforcement agencies, regulators and industry associations, both domestically and internationally;
- creating awareness amongst bank customers and the general public of bank related crime and ways to prevent it; and
- contributing to the general safety and security of the banking environment (SABRIC, 2011).

SABRIC, specialises in information management and crime analysis, recommends strategies and/or provides actionable crime information products to its clients, partners and stakeholders. SABRIC also acts as a source of information to its clients, partners and stakeholders. Daily crime incident information is provided to SABRIC by its clients, partners and stakeholders using their own collection methods and collection means (source techniques). It has Standing Operating Procedures (SOP) for information management, crime analysis and the utilisation of crime information strategies/information products (Interview no. 36).

5.5.1.2 Crime information management

SABRIC's information management strategy is to develop a credible crime information repository with integrity to recommend strategies and/or provide actionable crime information products to clients/partners and stakeholders. The consequence management office also serves as an information source. Strategies stem from the information in the repository. It is therefore important that the information in the repository is credible to work on. The purpose is thus to develop a credible crime information repository. Collected incident information is not parked on the system and forgotten. Evaluation/verification of the quality of the information is very important, as it is the key to the repository. All information on crime incidents received from sources, is evaluated/verified by the consequence management office through follow up, before the information becomes actionable through analysis. Written information products delivered from this repository for example, update

reports on Automated Teller Machine (ATM) related crime is what is termed as an actionable crime information product (Interview no. 36).

Standing operating procedures agreed upon by clients, partners and stakeholders are used to ensure credibility and integrity to the crime information provided by clients, partners and stakeholders. Internal sources of information also include the CEO, business support office and the commercial crime office. A company relies primarily on its clients (banks, cash in transit companies, etc.) and partners (South African Police Service (SAPS), Metro Police, Business Against Crime (BAC), stakeholders (Consumer Goods Risk Initiative (CGRI), Petroleum Security Initiative (PSI) and Telkom, etc.) and the mass media who serve as external sources. It does, however use open source techniques to enrich its crime information. The Commercial crime office may source information from the violent crime office and vice versa. Consequence management and the information office operate interdependently. If there is an incident, it is given via by the information office to the consequence management office to obtain more detail or to enrich the available information (Interview no. 36).

There are two types of risks, one is the organised bank-related crime risk, which SABRIC deals with and the other types of security risks are dealt with by the banks themselves. SABRIC cannot manage these risks because of the following factors:

- every individual bank should be looking at what affects them most;
- banks security models differ;
- they have different service providers from a security point of view; and
- their priorities differ from one bank to another (Interview no. 36).

Banks should, however, also have their own analysis capabilities to attend to day-to-day security risks affecting them operationally. Presently, some of them are outsourced to private security contractors who deal predominantly with day-to-day incidents. SABRIC provides a picture of what is happening in the banking industry in general (Interview no. 36).

According to the interviewees, they face challenges rather than problems. Some of the challenges include impediments to the constant flow of information from the source to the consequence management office which is sometimes also not provided according to the criteria set down in the standing operating procedures, e.g. timeliness of the information. The vicious cycle of new staff and restructuring within the partner structure poses a challenge, because they need to be trained to be knowledgeable to meet their challenges. Where technology is concerned, not all their partners and stakeholders have access to computers and not everyone has computer knowledge. Partners do not have cell phones to send an (Short Message System) SMS, but can only receive an SMS, some do not have emails instead they use faxes. Some partners operate in outlying areas and cannot be reached due to poor communication infrastructure. Some of the clients cannot receive comprehensive reports because of restrictions on their systems. Many clients/partners/stakeholders do not have appropriate software programmes and compatibility complicates matters (Interview no. 36).

Provinces are visited and particular client representatives including partners are made aware of the company model. Most of the information management challenges are addressed internally and externally through workshops and awareness programmes (Interview no. 36).

5.5.1.3 Crime information analysis

SABRIC has its own analysis infrastructure with in-house analysts. It also outsources specialised analysis functions based on specific needs. The company's analysis strategy is to use all available information from its repository to formulate strategies/actionable crime information products to mitigate crime, using different computer software programs and human skills. Analysis is done by using computer and manual skills. The company recruits highly competent analysts to perform the analysis function. The company starts with initial analysis by collating the data. Information from clients, partners and stakeholders are used in the analysis process. Verification, detail and integrity of the information are very important elements for analysis. Verification of information is done by testing the information with different sources. If information is not in detail, the missing detail is obtained from the

sources. Sources ensure that the information is timely. Information is also enriched by the sources according to Standing Operational Procedures (SOP). The SOP serves as a memorandum of understanding, which outlines the procedures to be followed by clients, partners, stakeholders and the company. It determines the needs of the clients, partners or stakeholders. These Standing Operational Procedures are contractual by nature. Analysts employed by the company perform a dual function. One such function is to do crime information analysis and the other is to be business minded in the mining of information (Interview no. 36).

The security risk information pertaining to organised bank related crimes is collated, verified, enriched, interpreted and produced as strategies/actionable crime products by consequence management for use by clients, partners and stakeholders. Both the consequence management and information office are sources for one another. They work together. Consequence management serves as a collection unit for information management. If a missing link is identified in the collated information or any additional information is requested it is passed onto consequence management to do a follow up. The company cannot work with outdated information, it is therefore important that sources should provide information on time. It keeps abreast with developments and monitors new methods criminals use in committing crimes. This may also require entering into new partnerships to combat specific types of crimes, e.g. identity thefts, scams, phishing, etc. The consequence managers do linkage analysis for example using modus operandi and photos received from the bank, etc. They support and assist the investigators and the police to link suspects and crimes with similar modus operandi between cases and suspects (Interview no. 36).

The analysts work with modus operandi data, geographic concentrated patterns and statistical information of crime risk factors, data from victims (clients) and explanations of crime. Analysts identify crime patterns, research theoretical explanations and formulate strategies/products for use by the intended users. They also keep abreast with developments in the political, economic, social, technological and international environments to add value to the strategies/actionable products. There is an integrated process all the way. Information is integrated for tactical and strategic purposes. Analysts liaise and verify the repository information with the bank officials or SAPS. If something has to be amended on the database not anybody can

do it. A process needs to be followed. Clients, partners and stakeholders do not have access to the database. They have their own databases, which feed into their organisational/company database. They do not have open access to the information. No exchange of information takes place from one database to another due to the agreed upon integrity and credibility of the company database (Interview no. 36).

Challenges in analysis are verification (verify information with different sources); detail (not all information is reported in full detail); integrity (checking on data integrity); and criteria (standards to be followed to collect information). The Standard Operating Procedures are sometimes not followed by the providers of the daily crime incident information to SABRIC (Interview no. 36).

5.5.1.4 Implementation of strategies and actionable crime information products

The company has a policy relating to the implementation of crime information. It produces a host of actionable crime information products namely; assessments, briefings, linkage analysis, statistical analysis, association analysis, crime analysis and written reports. Strategies and products are disseminated through briefings, meetings, handouts, reports, e-mails, compact discs, etc. Informational needs of clients, partners and stakeholders are identified in the SOP guideline. Continuous assessment is done on the client's needs in the different environments. Managers hold meetings with clients, partners and stakeholders to determine needs of the intended users. Clients also request additional information regarding a product (ad hoc request) and this assists with informal feedback. Impact studies are done to determine if all the information received is used accordingly and whether predictions have been realised. Formal meetings, one on one interview, quarterly client surveys, an annual partner surveys are used to do follow-ups on disseminated strategies/actionable information products (Interview no. 36).

Not just any person can add information to the database or access the database. Staff members are limited to add or access specific types of information. Two levels of classification are used namely; confidential and restricted. Staff members do not have problems to access the database; they need to have security clearance.

Classified access to the database gives credibility to the data in the database (Interview no. 36).

The South African Police Service has acknowledged that SABRIC has a big role to play in supporting its operations. Some of the challenges in the application of services, strategies and products are the leakage of information and not getting timely feedback from the intended users. These challenges are addressed internally and externally through workshops and awareness programmes (Interview no. 36).

5.5.2 Case Study 3: Consumer Goods Risk Initiative (CGRI)

5.5.2.1 Organisational structure

In this case study interviews were conducted with senior managers of the Consumer Goods Risk Initiative (CGRI), a business unit of the Consumer Goods Council of South Africa (CGCSA). The CGRI specialises in information management, crime analysis and the formulation of strategies and/or actionable crime information products for application by the retail industry in South Africa. The CGRI obtains its funding from its members. Its purpose is to work together with members, partners and stakeholders, to mitigate crime in the retail industry. Retail companies enter into a Memorandum of Understanding (MOU) with the CGRI to ensure that daily incidents of crimes are reported to the company in support of its initiative aimed at reducing crime in the retail industry. It serves about 4 600 retail/wholesale outlets in the country. Each retail/wholesale outlet also appoints a dedicated “Champion” to drive the initiative in his or her company. The Information Management Company obtains its information from its members and acts as a source of information to its members, partners and stakeholders. Standard Operating Procedures exist for information management, crime analysis and the application of strategies and actionable crime information products. This security risk information management company is not involved in the implementation of strategies nor does it have any control over criminal activities. Its focus is to provide strategies and/or actionable crime information products to reduce crime and financial losses at its retail/wholesale outlets (Interview no. 37).

Each retail/wholesale outlet also has its own database to store varying levels of information that affect them. However, their information is generally insurance focussed and does not facilitate crime analysis, in order to produce preventative measures or enhance police investigations. The CGRI is not prescriptive in that it only makes recommendations. The first concern of the retail stores is the safety of customers and its personnel. The second concern is the reduction of losses. The CGRI does not do security risk analysis or security surveys at these outlets (Interview no. 37).

The CGRI has adopted a centralised approach to information management, crime analysis and the utilisation of strategies and or actionable crime information products. The Head: CGRI and Manager for Member Services and Projects manage the Security Risk Information within the CGRI (Interview no. 37).

Business Against Crime has played a mentoring role to CGRI. BAC's role in the business sector and its communication line with the leadership in the Criminal Justice System-Police,Justice and the Private Security Regulatory Authority (PSIRA) has enabled CGRI to fast track its relationship with these stakeholders, to the extent that BAC facilitates meetings between CGRI and these stakeholders. The CGRI participates regularly in South African Police Service meetings. It builds relationships with the police stations and clusters (Interview no. 37).

5.5.2.2 Crime information management

Members provide daily crime incident reports to CGRI for crime analysis and formulation of strategies and/or actionable crime information products. Information collection starts at the store. The CGRI relies on the store to provide the information on the crime incident. First information of crime is a telephone call from the participating stores. The Store follows up on the telephonic incident with a relevant incident report for the specific crime and sends it electronically to the data administrator of CGRI. The data administrator on the Incident Management System (IMS) electronically captures it. A reference number is allocated to the incident. Statistical information, geographic information and modus operandi is also provided

to the data administrator. No false incidents can be reported as the incidents are coordinated with the police by means of the police case numbers (Interview no. 37).

Many stores are not prepared to invest in and install Closed Circuit Television (CCTV) surveillance camera systems. They are of the perception that installing CCTV cameras will not prevent an armed robbery from happening. It will only assist the store in identifying the perpetrators. Stores are keener on having criminal acts prevented. If prevention is linked to the apprehension of criminals then stores are prepared to invest. On the other hand certain stores invest a lot of money on the installation of CCTV cameras. They believe that the identification of perpetrators will lead to arrests of perpetrators, which will in turn reduce crimes, which in some cases has proven to be true. Some stores have decided not to invest in CCTV cameras, because their losses do not justify spending that much of money on CCTV cameras. Risk managers from the participating stores check out CCTV camera tapes and pass their findings to CGRI who conduct content analysis on the CCTV image (Interview no. 37).

Personnel Identity cards are also issued to retail store personnel to help monitor people involved in criminal activity in stores. Personnel identity cards are taken away from such personnel when disciplinary action is taken against them. Previously the offending personnel were able to commit an offence in one retail/wholesale outlet and go to work for another outlet without being detected. Personnel cardholders come from merchandising companies, promotion companies and labour brokers, etc. Members vet their own staff. CGRI only provides identification cards to all vetted personnel. CGRI coordinates information, develops best practices and gives advice to stores when requested to assist. The company only handles crime information and formulates strategies and or actionable crime information products to combat crime (Interview no. 37).

Information management, crime analysis and the application of strategies and/or actionable crime information products is managed through CGRI‘s operating procedures. Members provide voluntary information. No toll free public information line is available. Information is not always obtained from external sources. The Company discusses its crime incident reports, strategies and/or actionable crime

information products with private security companies, SABRIC, PSI, SAICB other stakeholders and the Police. CGRI is reactive incident driven. It does not work with covert information. They also work with proactive information which is passed to the police to follow up. SAPS liaise with other government departments for any additional information required by CGRI. CGRI does not work for the SAPS (Interview no. 37).

CGRI continuously engages with shopping managers and security personnel at the retail/wholesale outlets regarding potential security risks. A BAC project called ‘Crim Project’ (Cash Management Project) is currently implemented to prevent pavement robberies of cash from the bank, to the centre. This project is managed by SABRIC. Special projects are also managed in a team approach, with participants from the different stores and the police. Primary concern for the stores is the safety and security of their customers and staff, secondary is the losses they incur. The Company contributes towards its projects, which is focussed on its crime threats (Interview no. 37).

5.5.2.3 Crime information analysis

Crime incident reports are received electronically through the Hi-base automated information system or through email from members. The information is then transferred onto an analyst notebook. The analyst notebook is used by an analyst to evaluate/verify the information and to collate the information. Information is then sent weekly to the risk manager of the relevant outlets for evaluation/verification of facts. Data integrity is monitored and verified by senior crime analysts. Analyst’s programmes were specifically written for the junior and senior analysts. Incomplete data is a big problem. The data administrator has to follow up on the incomplete information. Trained data analysts are in-house (home grown). No specialist analysts are used. Analysts work is only outsourced if a problem occurs with specific types of reports; which need a much more sophisticated analysis. The analyst justifies all information, by verifying the information with the client and the police. The specific software programme used by CGRI handles all crime information related to shoplifting, short deliveries of stock, hi-jacking, cash in transit heists, credit card and cheque fraud, burglaries and armed robberies (seven identified crimes). It is not

confined to syndicate crimes only. The information is verified with the champion of the company. Problems are experienced with the completeness of the incident reports and in obtaining case numbers and details of investigating officers from the police (Interview no. 37).

Although it is not a big problem, retail outlets sometimes do provide incorrect statistical information. One of the biggest problems is the verification and completion of the data. When the crime incident comes in, the relevant data capturer, will look at it try to verify the information or try to get the case number and enrich the information (Interview no. 37).

Information comes in and goes out under classification. The system is not an open system and therefore cannot be accessed by anyone. CGRI's strategy is to collate the data relating to crime incidents, conduct analysis of the information in order to provide accurate and meaningful strategies and/or actionable crime information products to their members so that they can implement the crime-combating strategies in their stores. It also looks at the various aspects of the crime and decides on what should be done. It identifies problem areas, trends, new modus operandi, etc.; and develops new strategies to counter the problems. Analysts also produce profiles of wanted suspects, red alerts and provide police with photos profiles and any other analytical products when required. CGRI also adds value to the information through criminological research for the purpose of prevention. Criminologists experience problems to get access to victims. Analysts also seek clarification, interpretation, draw inferences and provide advice to members. Analysis is done according to Standing Operating Procedures. No problems are experienced with analysis (Interview no. 37).

5.5.2.4 Implementation of strategies and actionable crime information products

When an incident of serious crime occurs at a specific retail/wholesale outlet, CGRI sends an SMS messages to the cell phones of other members in the area. This will alert the other members as to the modus operandi of the particular crime, so that they can harden their targets, in order to prevent it occurring at their outlets.

Hotspots (vulnerable areas) are also identified in partnership with the members, partners and stakeholders. The identified users prepare a hotspot report (vulnerability analysis report) for use. The hotspot report identifies vulnerable areas for attention by SAPS. The South African Police Service (SAPS) deploys personnel according to the hotspot report. Whenever this intervention happens, sharp decrease in crime is noticed at the identified hotspots (Interview no. 37).

CGRI attends weekly, monthly, quarterly and annual meetings where strategies and/or actionable crime information products are shared with members, partners and stakeholders. Hints are given for the prevention of criminal incidents. CGRI is not involved in the operationalisation of the strategies and/or actionable crime information products. It does not decide on strategies but only recommends the implementation of the strategies. The Company contributes to special projects as a team member at a store (Interview no. 37).

Security information obtained through security assessments by respective stores are sometimes used to assist in formulating strategies to improve security measures at the store in order to prevent criminal activities. SMS's are used to disseminate information as alerts. Strategies and products are classified by using 'confidential' and 'restricted' (Interview no. 37).

The manager responsible for strategies visits the store and meets with the risk managers on a monthly basis. At that meeting statistics, trends and the strategies are reviewed. Opportunities and threats are discussed. Best practices are discussed on how to protect the safes, strong rooms, cash office and how to improve alarm systems. In the case of burglaries, to overcome the problem of criminals taking away the outdoor alarm communication systems. This issue was discussed and investigated by CGRI. Strategies and/or actionable crime information products are identified and recommended to mitigate the relevant security risk in this regard (Interview no. 37).

Risk managers from the participating stores sit on the monthly Management Committee (MANCOM) meetings called by CGRI. Information regarding crimes affecting the retail/wholesale industry as a whole is shared with them. Police

organised crime units are given information on syndicated criminal incidents for example housebreakings and armed robberies. All ATM crimes are handled by SABRIC despite the ATM being situated inside the stores. SABRIC also monitors ATM crimes in terms of modus operandi, etc. SABRIC maintains ATM statistics. CGRI discusses retail crimes with participating store groups and the police (Interview no. 37).

Different meetings take place with the police and the retail industry. The store works on their own initiative with the information, since the stores are responsible for their own security. They have their own meetings with the local police (Interview no. 37). Meetings are attended with the police nationally, provincially and locally. Vulnerabilities are also rated so that police deployment can be enhanced in those areas. Crime prevention awareness is done at shopping centres to overcome incidents of criminality (Interview no. 37).

Security personnel will only have access to information as deemed necessary by the store management. SAPS only share statistics which are case related. They do not share information on suspects or proactive information (Interview no. 37).

Some of the big security companies (Group 4 Security Company, Protea Coin Security Company and Fidelity Security Company) are privy to security information from CGRI as crime is considered as a non-competitive issue by them. Security guards at the stores do not have access to information from CGRI. Information provided by security guards is managed by the store management. If necessary it is referred to CGRI. The company communicates directly with police of the specific cluster commander or station commissioner organised crime units or the special task force of the police when it encounters crime incidents in progress (Interview no. 37).

Seventy percent of the participating stores implement strategies and/or actionable crime information products to combat specific incidents. An impact study showed a 46% decrease in crime statistics during 2009. During 2005, the Retail Industry used to undergo an average loss of about R100 000 per incident through armed robberies. Since then, it has decreased to about R30 000 per incident. Losses per incident came down because of cash management strategies. CGRI makes

recommendations to stores on cash management strategies for example; to have as little cash as possible at their outlets, to use as many Cash-in-Transit pick-ups as possible, encourage the use of ‘dropsafe’ drops and to have small cash floats in tills (Interview no. 37).

Feedback is given to the members on all information of incidents received. All information, strategies and/or actionable crime information products are classified to overcome leakage of information (Interview no. 37).

5.5.3 Case Study 4: Petroleum Security Initiative (PSI)

5.5.3.1 Organisational structure

In this case study interviews were conducted with senior managers from the Petroleum Security Initiative (PSI). PSI has been in existence since 2004. PSI is responsible for information management and crime analysis for the South African petroleum industry for all participating oil companies. It manages and collates crime incident information collected by its clients, analyses the crime incident information and recommends strategies and/or provides actionable crime information products aimed at mitigating serious crime related to the petroleum industry. This initiative is driven in partnership with five (of the six) participating oil companies. The purpose for PSIs existence is the high level of crimes perpetrated in the petroleum industry and the absence of information management and crime analysis strategies, as well as actionable crime information products. Their strategy is to identify the crime drivers, develop strategies to mitigate the crimes and to implement preventative measures. Its vision is to reduce the crimes perpetrated against petroleum retailers to an acceptable level. Reference is made to serious and violent crimes including robberies at service stations, hijackings, fuel thefts, truck hijackings, bombings of ATMs, etc. Most of the information focuses on petroleum industry related retail crimes including Cash-in-Transit (CIT) incidents and ATM crimes perpetrated at petrol station forecourts. Each oil manufacturing plant or service station operates under individual oil companies. They operate within the policy of the specific oil company for example Engen, Sasol, etc. The specific oil company specifies policy on how the crime information is to be provided to the Petroleum Security Initiative (PSI).

The infrastructure for PSI includes a general manager, consequence manager, data capturer and an analyst. Formal training is not provided to their personnel, since many of the incumbents are former police officers who had been exposed to crime information collection and analysis. However, they do provide on the job training on specific issues such as information technology and software training for analytical skills (Interview no. 38).

There are standing operating procedures on the expected service delivery requirements. There is no interference with the work of the South African Police Service. Petroleum Security Initiative (PSI) is there to support the South African Police Service in their endeavours to combat and limit crime-site-specific to premises of petroleum retailers (petrol stations) (Interview no. 38).

5.5.3.2 Crime information management

The Petroleum Security Initiative (PSI) has a 24-hour security incident reporting line. As incidents happen, they are reported through this line. A data capturer who takes down the information of the incident completes an incident report. The incident report includes all relevant details, according to a prescribed reporting format. All the information is captured onto an automated system. There is also a toll-free number for the reporting of crimes in progress, e.g. an armed robbery in progress. If a specific site uses the toll free number, it can be seen on the system as to who is reporting and from which site the report is emanating. The police are immediately informed of the crime in progress. This number is not for public use.

Sometimes the reporting of incidents by petrol service stations is very sketchy. Some retailers do not report the incident due to competition among retailers. The feeling is that if they do report they will be penalised by their oil company for not adhering to policy or administrative procedures. If crime incidents are hidden and not reported to the PSI, particulars of the crime incident is eventually obtained from SAPS, media, SABRIC, CGRI or other members of the Public Private Partnership (PPP). The PSI is in the process of putting in place a help line to encourage retailers to report crime incidents without being exposed. This helpline is to enhance reporting of hidden crime incidents. There is no Memorandum of Understanding (MOU) with all

stakeholders to share information, due to some entities being disorganised and not equally effective (Interview no. 38).
The PSI uses a Computerised Occurrence Book (COB) with coordinates to all its service sites. It can be used to send simultaneous SMSs to different sites in a particular radius or in general as soon as it receives information on crime incidents. If all retailers report crime incidents, it will improve the crime situation (Interview no. 38).

Business Against Crime (BAC) arranges meetings with the leadership of the police and holds bi-monthly meetings with all stakeholders. A representative from BAC also functions from the crime support centre at the 10111 police emergency centre. This person is there to liaise directly with all participating industries including the PSI, other stakeholders and the police regarding crime incidents occurring at oil company sites and other places of interest to the other stakeholders. This person represents the BAC (crime support centre). The Petroleum Security Initiative (PSI) liaises with the police both nationally and provincially, SABRIC, CIT companies and oil companies on a continuous basis. The police work in partnership with the PSI sharing information of commonality (Interview no. 38). Continuous meetings with SAPS cluster commanders and/or station commissioners impacts positively on police action. Police enhance operations at hotspot areas identified by the meetings. The enhanced police action reduces crime incidents in that particular hotspot. Annual statistics maintained by PSI showed that whenever there were meetings with the policing clusters, crime levels dropped at the identified clusters (Interview no. 38).

New managers come and go from the various petrol service stations, some new managers are not aware of security procedures on the reporting of crime incidents. Managers have far too many responsibilities than to focus on security. Their prime focus is to run a business and not to manage crime. They are not adequately trained on security related issues. Retailers do not train personnel on how to react in the event of armed robberies or how to prevent armed robberies**.** PSI is currently developing a curriculum to assist in the training of site personnel (Interview no. 38).

One big disadvantage is that information could be leaked to perpetrators during the sharing of information (Interview no. 38).

5.5.3.3 Crime information analysis

The automated incident report is sent to the analyst for processing. Using the appropriate software the analyst ensures that the information is enriched by using information provided by other sources, such as the police, other oil companies, Consumer Goods Risk Initiative (CGRI), South African Banking Risk Information Centre (SABRIC), the Post Office and South African Insurance Crime Bureau (SAICB), etc. The automated system also does linkage analyses by providing links to other similar information on the system. The information on the system is further enriched by collecting further information to fill the gaps. Once the information is enriched, the analyst then converts it into a daily incident report. The information on the daily incident reports also reflects information of incidents provided by SABRIC on banking and Cash-in-Transit incidents, which affect threats confronting the oil companies. The collected information is further enhanced with information from criminological research, the media and other open sources, to add value to information on crime incidents. It is a comprehensive document, some days it is up to twenty pages (Interview no. 38).

The Consequence Manager is tasked to conduct further investigations at every site in Gauteng where a crime incident had occurred. He will identify the cause/s that led to the occurrence of the incident, determine what has been done and what has not been done. He will also collect additional information, which has not been collected previously, e.g. Description of other occupants in the suspect vehicle, colour of vehicles, CCTV images will be viewed for possible suspects. Information on previous incidents is also collected at the specific site. Information on the modus operandi is also obtained. If a specific security weakness for example, poor locking devices and door fittings, watchman found sleeping, involvement of security officials, etc. resulted in the criminal incident taking place, this is also addressed by the consequence manager with the retailer and security company employed at the petrol service station (Interview no. 38).

The analyst will add all the new information onto the incident report. Weekly, the analyst will use all the collected information and provide management with a hotspot report. It will also provide a hotspot forecast by PSI, on where future incidents may occur and identify clusters that are being hit frequently. Hotspot reports are sent to the same recipients as the incident reports. A third report called the Joint Operational Committee (JOCOM) report is compiled in conjunction with SAPS and other stakeholders. It is a report that deals with crime trends, activities and frequency of crime incidents in the policing clusters where these incidents are most common. This report also serves as a Crime Threat Assessment (CTA) (Interview no. 38).

The crime information analysis process includes collation of the raw information, interpretation, verification and adding value by further investigating the information. Petroleum Security Initiative (PSI) does not have a policy for analysis. All analysis is done using intelligence software, similar to that used by SABRIC, banks, mines, SAIB, casinos and tourism, etc. (Interview no. 38).

Information is classified at two levels, namely: ‘confidential’ and ‘restricted to specific companies’. The analyst is supportive and gives advice whenever needed (Interview no. 38).

5.5.3.4 Implementation of strategies and actionable crime information products

A daily incident report is sent out electronically. The SMS is used to disseminate this information to the sites (petrol service stations), to all the clients including the South African Police Service for application. There are about twenty identified users of the daily incident report. It also provided to SABRIC, CGRI, Post Office, South African Petroleum Retailers Association (SAPRA) and the different service providers from the different oil companies. South African Police Service Gauteng (Provincial Commissioner: Crime Management Centre) also receives the daily incident report, which is disseminated to other policing structures in the Province. It is also possible that SABRIC, PSI and the CIT contracted companies will all report on the same incident to the provincial policing structure for proactive and reactive steps. For example ATM attacks or CIT attacks happened. All incidents in the daily incident reports have already been reported to the SAPS and will be part of their daily crime

report. Weekly Hotspot reports are sent to the same recipients, as the daily incident reports. A third report is the JOCOM report. The JOCOM report is not as widely distributed as the other two reports, due to their inclusion of confidential information applicable to specific companies. As a result of competition amongst oil companies, values of losses are not put in the report to all the recipients (Interview no. 38).

An Industry specific report is also provided to specific oil companies whenever an incident occurs at their sites. This report is also sent to other oil companies and the SAPS. The consequence manager's report is also sent to the specific oil company and the site (petrol service station) where the incident occurred. It is also sent to SAPS (provincial crime management centre) (Interview no. 38).

A monthly analysis report of all incidents is also given to the oil companies only. This report is not for general consumption. PSI also participates in big projects run by BAC and the SAPS. The company also registers projects if there is a major problem at specific sites (petrol service stations). There are advantages for service stations who implement strategies and/or actionable crime information products provided by PSI. This results in reduction of crime incidents. In some instances if the retail side does not want to implement certain strategies and/or actionable crime information products they just ignore the tasking by not acting on it. Those that ignore implementation of strategies and/or actionable crime information products, usually experience a high number of incidents (Interview no. 38).

Whenever there are meetings with cluster commanders/station commissioners and operational interventions follow, incidents at oil company sites show a decrease. On one occasion, there were investigators at Honeydew SAPS looking for the same suspects as SAPS Florida. They did not realise that the perpetrators were being investigated by SAPS Florida. There was no linkage analysis. Intervention by security officers of a private security company led to the perpetrators being arrested and linked to cases from Honeydew and Florida (Interview no. 38).

Police provide feedback on progress being made with investigations being conducted at the different sites. Oil companies also provide feedback on the implementation of strategies. The biggest response comes from individual petrol

service stations that liaise directly with PSI. There is no structured way of getting feedback. Formal feedback is given by written reports, emails and informal discussions with specific persons. All successes are also reported and coordinated by the analyst (Interview no. 38).

5.6 SUMMARY

The three security information management companies are private initiatives. They do not collect security information, but coordinate incident information received from their clients. They collate the crime incident information received from their clients, analyse the crime incident information and recommend strategies and/or provides actionable crime information products aimed at mitigating serious crimes confronting their clients. They do not analyse security information on vulnerabilities, but do support their clients with threat assessments depending on the gravity of the threat. All three companies are intent on reducing crime, increasing detection rates and preventing losses. The views presented in this case study by the different companies might be similar, because they all addressed the same research questions of the study.

5.7 SECURITY INFORMATION MANAGEMENT IN AUSTRALIA

5.7.1 Case Study 5: Security information management in Western Australia, Western Australian Government Departments, Western Australian Police and the Western Australian Private Security Service Providers

5.7.1.1 Background

The use of private security in crime prevention and law enforcement in Australia has grown to a point where security personnel outnumber police by more than two-to-one. During 2006, there were 52 768 personnel employed full time in the Australian security industry, compared with 44 898 police members. A decade earlier the police had out-numbered security (Prenzler, Earle & Sarre, 2009: 1).

Any person who conducts a business or is employed in a security related field within Australia is required to be licensed. Each of the six states and two territories (New South Wales, Victoria, Queensland, South Australia, Western Australia, Tasmania and Northern Territory) of Australia have separate legislations that cover all security activities. Licensing management in each state/territory is varied and is carried out by Police, Attorney General's Department, Justice Department or the Department of Consumer Affairs. Security officers are not permitted to carry firearms, handcuffs or batons unless they have a legitimate requirement to do so and then only when working and have the appropriate sub-class accreditation to their licence (Australian Security Industry Association Ltd, 2011).

Presently data indicates that over 5000 security and investigative businesses are registered in Australia and over 110 000 licences have been issued mainly to individuals (Prenzler et al., 2009: 1).

In Australia, threats and risks are considered as different concepts. Threat is a hazard or a source of risk (criminals, terrorists, etc.), usually measured in terms of intent and capability. A threat also takes into consideration direct impact of natural disasters, e.g. power outages, infrastructure and indirect impacts such as fire, looting, civil unrest, etc. Risks are considered as the likelihood of an attack with the most credible impact(s) or consequence on assets. Security Risk Management therefore involves understanding the threat as part of the objective of determining and implementing counter measures to manage risks (Talbot & Jakeman, 2008: 36).

5.7.1.2 Security information management in Western Australia

Private security activities within Western Australia are governed by the Security and Related Activities (Control) Act 1996 and the Security and Security and Related Activities (Control) Regulations 1997. Whilst the term security guard is used by many companies, government bodies and individuals use the term security officer, "Bouncers" are called Crowd Controllers and Store Detectives are called Loss Prevention or Asset Protection Officers. The Western Australian Police Licensing Services (Security) regulates and manages the security Industry. The aim is to provide the community of Western Australia a professional security industry where

competency (training), integrity and accountability is maintained at a high standard (Australian Security Industry Association Ltd, 2011).

In Western Australia businesses supplying security products or services must hold the following licences:

- Security Agents Licence which authorises the supply of security officers, security consultants or security equipment services.
- Crowd Control Agent Licence which authorises the supply of crowd control services.
- Inquiry Agents Licence which authorises the supply of investigation services.

Individuals who perform security services need to hold the following non-agent licences:

- Security Officers Licence: to watch, guard and protect property.
- Security Consultant Licence: to investigate and advise on matters relating to the watching, guarding and protection of property; including security services and equipment sales.
- Security Installer Licence: to install security equipment (does not include installers of security equipment in vehicles, vessels or aircraft)
- Crowd Control Licence: to monitor or control the behaviour of persons, screen persons for entry or remove people from premises. Required for licensed premises, places of entertainment and public or private events or functions (Australian Security Industry Association Ltd, 2011).

Investigators licence means to legally investigate the conduct of individuals or a corporation or the character of individuals, perform surveillance work or investigate missing persons (Australian Security Industry Association Ltd, 2011).

Security information is usually obtained from threat, vulnerability and criticality assessments as well as historical information, management systems and programme activities. This security information is analysed using a risk register. The risk register informs on asset criticality against identified risks and provides a framework from which to allocate the needed physical security resources and

funding. The likelihood and consequence of the risk is determined by assessing and defining the risk using descriptive terms (qualitative), using calculated data (quantitative) or the combination of the both (Talbot & Jakeman, 2008: 178-179).
Security information on incidents is handled according to an Incident Management and Reporting Guideline. The operationalisation of the security information depends on reports and trends identified through analysis of incidents. The analysis of incidents consistent with other institutional standards is essential in order to maximise the value of the information (Talbot & Jakeman, 2008: 66).

5.7.1.3 Government departments

The Government departments provide policy; guidelines and collection plans for the collection of security information. The owners of the buildings where the government departments are housed have contracted security service providers. Their functions are mainly directed at access control and taking care of the physical protection systems. The Government departments have their own Security Heads. They manage security related activities and conduct workplace investigations on misconduct and other policy related incidents in respect of the government department. These officials are all licensed to perform the specific security related activities. It is the responsibility of all employees and clients to report any information on threats, incidents and vulnerabilities to the security official at the sites. The security officials enter the information into the computer system using a specific template. Software programmes are used to collate the information. Much of this information is handled by the security officials at the respective sites.

Security information on crime incidents are referred to the WAP. All misconduct and policy related violations are referred to the Regional offices. Different methods are used to collect security information. Open means is most commonly used to collect security information. Networking is also used to gather information. Security managers identify misconducts and vulnerabilities. Risk management profiles determine the types of threats the department is exposed to. The Australian Security Intelligence Organisation Business Liaisons Unit (ASIOBLU), collects security information on threats, analyses it and provides threat assessment reports to

government departments in Western Australia. Information is also collected from third parties (Interview nos. 18, 19 & 20).

Government departments share information among themselves. All information is recorded manually and then transferred to computer systems. Feedback is given according to the information received. A collection unit is tasked to collect any additional information, analyse the information and make recommendation. Actionable information products and threat assessment reports are received for application as security risk control measures. Feedback is then also given on the outcomes of the application of security information (Interview nos. 18, 19 & 20).

5.7.1.4 Western Australian Police

The Western Australian Police (WAP) has a Commissioner as head, Assistant Commissioners as deputies, Superintendents in charge of the uniform and detective police divisions, inspectors appointed as district officers, senior sergeants and sergeants are in charge of police stations and constables as operational workers. The Australian Crime Commission Corporate Plan 2004 is used as a guiding instrument for the WAP to manage security information on crime (Interview nos. 21 & 22).

The WAP use the concept ‘intelligence’ rather than ‘information’. This was started in the 1990s when intelligence led policing first appeared in Australia. It was driven by a number of police commissioners. The local adoption included a new accountability structures at a local level, a greater integration of intelligence and investigation and improve targeting of daily police efforts through intelligence dissemination. For the purpose of the WAP the researcher will use the concept intelligence rather than security information (Interview nos. 21 & 22).

The WAP use overt and covert means of collecting intelligence. Public hotline systems are also used to get intelligence from the public. Intelligence is also provided by third parties. The WAP use different methods to collect intelligence. Some of the methods include physical surveillance, electronic surveillance, interviews, research, auditing, undercover and forensics. Intelligence is obtained

from both internal and external sources. All intelligence is entered into the computer and viewed at the local level. The intelligence from the different police stations is viewed by the intelligence group at district level. The different policing units have access to the intelligence according to the classification criteria. Anybody may access any intelligence if they have a valid reason to access it. If the reason is not valid, access is denied. All intelligence is also viewed by the State Intelligence Division. They share this intelligence at the Federal Intelligence level, so that all the police states and territories can have access to them (Interview nos. 21 & 22).

Private security companies directly share intelligence with the WAP at the different intelligence levels. National key point companies share intelligence with the State Intelligence Division at the Critical Infrastructure Security Forum (CISF). These meetings take place four times a month. This sharing is based on scenarios. All intelligence received goes through value rating and security rating, so that the intelligence is sanitised and declassified for sharing (Interview nos. 21 & 22).

The WAP has a specific Incident Management System to manage all reported incidents. All incidents of crimes are reported by private security companies to the WAP for investigation. They sometimes assist the WAP with preliminary investigations, but hand over all criminal investigations to the WAP (Interview nos. 21 & 22).

The intelligence is analysed by qualified intelligence analysts at the local, district intelligence offices and at the State Intelligence Division and operationalised according to the priority of the Commissioner. The intelligence is used to generate actionable intelligence related products such as profiles, linkage charts, crime pattern analysis and threat assessments for operationalisation. If any further intelligence is needed to enrich the present intelligence, several cells are activated to collect this additional intelligence. A collection plan is designed for this purpose by the analysts. Operationalisation is done by the superintendents. They do the monitoring and evaluation of the application of the actionable intelligence products. Feedback is only given on its success, where necessary (Interview nos. 21 & 22).

5.7.1.5 Western Australian Private Security Service Providers

Security Risk Management (SRM) is a sub-set and an essential part of a broader risk management system. It is simply another management discipline fitting predominantly within the sphere of risk management. In Western Australia more emphasis is placed on investing in Occupational Health and Safety (OHS) of personnel rather than on security risk control measures. This is attributable to the low levels of violent crimes being experienced in Western Australia (WA). The collection, analysis and application of security information are therefore not regulated in the private security environment (Interview nos. 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33 & 34).

Security service providers in Western Australia have individual ways of collecting security information on threats, vulnerabilities and incidents. They also use different collection methods depending on the type of security information they need. Some of the more common methods include physical surveillance, electronic surveillance, interviews, research, audits and forensics. Security companies sometimes hold workshops with interest groups to collect security information. Depending on the nature of the operations, collection plans are specifically structured and used for this purpose. Individual interviews are held, security assessments and critical inspections are conducted and information is collected from third parties. Security service providers do not use collection units to collect security information (Interview nos. 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33 & 34).

In the casino industry, the collection of security information is everyone's responsibility. An information awareness culture is created by the distribution of pamphlets, holding awareness workshops and using a common code of conduct for all employees at the casino. Television screen (LCD) messages are also used to encourage the general public to provide information to specific control points. When Campus security guards receive security information they enter them into their notebooks, obtain statements, prepare a written report and enter the information into a computer system. They handle the information as a policy violation, criminal act or in terms of a contract management plan. Everyone on campus is encouraged to collect security information, as security is everyone's responsibility for example

students will inform security if they observe a breach of security or criminal act. Information is managed as a policy violation, criminal act or in terms of a contract management plan (Interview nos. 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33 & 34).

Security information is initially referred to the supervisors and then entered into an electronic database. Sometimes security information is received verbally and managed by the immediate supervisors. The threat information is generally referred to the WAP and addressed by the security service provider in consultation with the WAP. Incident Reporting Information Systems (IRIS) is used by campus security to manage security information on incidents. This is usually governed by the policy of the security service provider. The incident information on criminal conduct is generally given preliminary attention and referred to the WAP for investigation. The WAP has the legislative mandate to investigate crime in Western Australia. All incidents on policy violations are sometimes referred to the human resources section of the company for attention or investigated by workplace investigators. All vulnerabilities are handled in terms of a risk management process as determined by the company. It also provides a threat assessment for operationalisation. Security service providers do not follow a standardised procedure in handling vulnerabilities (Interview nos. 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33 & 34).

The security information is handled in a protected manner. The information can only be accessed if the individual has been permitted to access the required information. Otherwise access to the information is denied. All security information pertaining to threats and crime in general is discussed with different stakeholders at different forums. There are specific forums which serve the needs of specific security service providers. Some of these forums include: The Critical Infrastructure Security Forum (CISF), Australian Security Industry Association Liaison (ASIAL), Council of Australian Governments (CAG), Industry Security Committee and Trusted Information Sharing Networks (ISCTISN). Security information is shared at these forums on a need to know basis (Interview nos. 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33 & 34).

Many security service providers do not have appointed analysts. Computer software is used in the collation, analysis and generation of actionable information crime

products. One such common software used in Western Australia is the IRIS software which is used to collate, evaluate and analyse information for application. Security information is analysed only if it can be used. Otherwise the information is left in the computer to be used as historical information. Investigators or security supervisors are tasked to collect additional information where necessary. They prefer clean information than corrupted information. The casino industry analyses its CCTV and other information as soon as it is received and the notify police immediately of any criminal conduct. It also takes immediate action if the incident is in progress. Data integrity is a problem. Much of the information is not entered onto the system immediately. Sometimes information is not correctly entered into the computer system. Actionable information products and alerts are generated for use by security officials. Feedback on the application of the actionable information products is usually done verbally or in writing (Interview nos. 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33 & 34).

Many security service providers are of the view that they do need to analyse their information as no losses occur at their companies. All crime information is analysed by the WAP and operationalised (Interview nos. 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33 & 34).

5.8 SUMMARY

Security officials employed in a security related field in Australia are required to be licensed. The businesses as well as individual security officers need to be licenced. Threats and risks are considered as different concepts in Australia, Threat is considered as a source of a risk, usually measured in terms of intent and capability, while risks are considered as the likelihood and consequence of an attack. Security information is usually obtained from threat, vulnerability and criticality assessments as well as from historical information, management systems and programme activities. This security information is analysed using a risk register. The risk register informs on asset criticality against identified risks and provides a framework from which to allocate the needed physical security resources and funding. Government departments in Western Australia have a collection unit that is tasked to collect specific information, analyse the information and make recommendation. Actionable

information products and threat assessment reports are received for implementation as security risk control measures. The Western Australian Police use the concept ‘intelligence’ rather than ‘information’. Private security companies directly share intelligence with the WAP at the different policing levels. Qualified analysist are used to analyse intelligence in the WAP. Security service providers in Western Australia have individual ways of collecting security information on threats, vulnerabilities and incidents. Specific collection plans are developed for the collection of security information.

5.9 COMPARISON BETWEEN SOUTH AFRICA AND AUSTRALIA

As much as the researcher is not keen on making comparisons between a developed and a developing country, there are, however matters of relevance in the management of security information which may be important to compare. Table 5.1 draws comparisons on the management of security information between security practitioners in Gauteng in South Africa and Western Australia. Table 5.1 was drawn up by the researcher.

Table 5.1: Comparisons on the management of security information between Gauteng in South Africa and Western Australia.

SOUTH AFRICA (GAUTENG)	AUSTRALIA (WESTERN)
Security officers are registered by PSIRA	Security officers are registered and licenced by the Western Australian Police
Threats and Risks are considered as similar concepts	Threat and risks are considered as different concepts
Security Risk Management involves understanding the risk as part of the objective of determining and implementing counter measures to manage risks	Security Risk Management involves understanding the threat as part of the objective of determining and implementing counter measures to manage risks
The term security guard, store detectives and security risk managers are commonly used in the Security	The term security guard is used by many companies, government bodies and individuals use the term security officer,

industry	“Bouncers” are called Crowd Controllers and Store Detectives are called Loss Prevention or Asset Protection Officers
Risk assessment or Risk analysis (Probability, Frequency and Impact analysis)	Criticality assessments (Probability, Frequency and Impact analysis)
Security information is analysed by managers using a security officers incident report	Security information is analysed using a risk register
Security information on incidents is handled by the supervisor according to discretion	Security information on incidents is handled according to an Incident Management and Reporting Guideline
Government departments do not provide policy; guidelines and collection plans for the collection of security information	Government departments provide policy; guidelines and collection plans for the collection of security information
Government departments do not share information among themselves nor do they use forums	Government departments share information among themselves and at forums
Collection units are not tasked to collect security information, analyse the information and make recommendation	A collection unit is tasked to collect security information, analyse the information and make recommendation
Concept crime information and intelligence is used by the SAPS	Concept intelligence rather than information is used by the WAP
Private security companies do not directly share information or intelligence with the SAPS at the different policing levels	Private security companies directly share intelligence with the WAP at the different policing levels
SRM is a model used by the Security Industry to manage risks	SRM is simply another management discipline fitting predominantly within the sphere of risk management
In South Africa more emphasis is placed on investing in security risk control measures	In Western Australia more emphasis is placed on investing in Occupational Health and Safety (OHS) of personnel

	rather than on security risk control measures
Security officials are not tasked to collect security information on threats, vulnerabilities and incidents	Security officials are tasked to collect security information on threats, vulnerabilities and incidents.
Private security information management companies coordinate and analyse security information on incidents of crime (SABRIC, PSI, CGRI)	Private security information management companies do not co-ordinate and analyse security information on incidents of crime

5.10 PRESENT DAY STANDARDS EMANATING FROM THE CASE STUDIES

The SAPS and the WAP have a structured way of managing crime incident information and intelligence. They use collection units and investigators to collect information and intelligence. Collection plans are specifically structured for each project, so that only the required information and intelligence is collected. The information flows from the bottom upwards to the highest decision maker in the organisation. Only persons who have the level of security clearance have the authority to access the information (De Kock, 2011 & Interview nos. 21 & 22).

All crime incident information/intelligence that enters the system is analysed by structured analysis units. The crime incident information/intelligence is shared with interested networks such as private security companies, intelligence structures and other information networks. The WAP sanitises the information and declassifies the level before information/intelligence is shared. Only the relevant portions of the information/intelligence are shared. Decisions are made by management to operationally and strategically apply the information. In addition to actionable crime information products, they also generate a CTA with all the information/intelligence they receive. All Threat information received by the police is also included in the CTA (Interviews nos. 21 & 22).

In Western Australia, security managers in government departments have a structured, regulated way in which they manage the flow of security information on incidents of misconduct. Internal directives are issued to ensure that security information on crime incidents, threats and vulnerabilities are managed at the different sites. The collected security information is then channelled to their Regional Office. The Western Australian government department use the complaints management unit to collect information on incidents of policy violations. All incidents related to misconduct are investigated by the ethical standards unit at their Regional Office. Their Director General discusses the information on policy violation with the Director Generals of other Government Departments at the Federal level (Interview nos. 18, 19 & 20).

Awareness is created by security service providers in Western Australia to encourage the collection of security information on incidents, threats and vulnerabilities. Security service providers at the casino in Western Australia use different awareness strategies such as code of conduct cards for staff, pamphlets and LCD screens for the general public to report any security information relevant to incidents, threats or vulnerabilities to a security officer at a control point. In this way the information is immediately acted upon by a response team (Interview nos. 33 & 34).

In South Africa on the other hand the crime incident information management companies have a well-structured, regulated way to manage crime incident information. The process is controlled by Standing Operating Procedures which were agreed upon by the clients and the service provider. The analysis and recommendation of strategies to clients and stakeholders is coordinated, monitored and evaluated. The sharing of crime incident information by crime information management companies in South Africa helps enrich the existing repository and avoids duplication of strategies to address the same problem, for example ATM bombings at a petrol station retail outlet. This incident will be attended by SABRIC, PSI and CGRI, all of whom have an interest in the crime incident. Networking assists in coming up with one formidable strategy for recommendation to the client and the police (Interview nos. 36, 37 & 38).

Although the crime incident information management companies discover vulnerabilities during the course of their investigation, they only provide recommendations to the site managers on how to address the vulnerabilities. They do not manage security information on vulnerabilities for their clients. They consider this to be the responsibility of the contracted security company or in-house security service provider (Interview no. 35).

5.11 CONCLUSION

This collective type of case study research was not done to draw comparisons between South Africa and Australia. It would be meaningless to draw comparisons between societies with vastly different cultures and levels of crime, especially violent crime. This case study design was used to primarily identify present day standards both in South Africa and Australia in order to enhance the management of security information. The researcher's intention was to include only those attributes relevant to the collection and analysis of security information and the implementation of security risk control measures. In-depth interviews for the case studies were conducted with senior managers from the police, government departments (with in-house security service infrastructure) and private security service providers both in South Africa and Western Australia. One of the advantages of the in-depth interviews was that it helped to record more fully the responses of the participants supported by their outward manifestations. The use of the case study design proved to be a natural advantage in this study, as it helped identify strengths and weaknesses relative to a larger class of similar units. The procedures followed in conducting the case study interviews were consistent. The same interview guide was used for all the case studies. The researcher also tried to get interviewees from similar environments in both Perth, Western Australia and South Africa. Due to differences in both the countries it was not possible to achieve total success in this regard. The case study interviews were successful in the identification of present day standards.

CHAPTER 6

DATA ANALYSIS OF QUESTIONNAIRES

6.1 INTRODUCTION

The non-experimental design was used for the quantitative data collection (Fouché, et al., 2011: 155-156). The data was collected by conducting a self-administered questionnaire survey. Different sectors of the security industry from Gauteng participated in the study. A total of 114 respondents participated in the survey out of an intended target of 150, giving a response rate of 76%. The data was analysed by an independent statistician. The data analysis procedures had to be identified within this design. Data was analysed using the descriptive and inferential numeric analysis process (Creswell, 2009: 218). Basically, data analysis entailed the breaking down of the data into constituent parts to obtain answers to the research questions in Paragraph 1.4 and to test the grounded theory. The data will be presented using tables and frequencies. Ranking will be used to prioritise aspects. When two or more observations are equal, the average rank is used. For example, if two observations are tied for the second-highest rank, they would get a rank of 2.5 (the average of 2 and 3) and also if there are three ranks tied at 4 they would get a rank of 5 (the average of 4, 5 and 6).

The analysis and interpretation of the data was necessary in order to answer the research questions. It was therefore necessary to describe and analyse the data and then interpret the results of the analysis.

This chapter examines and discusses the data analysis and interpretation of the data from the structured interviews carried out with security officials employed by the security industry in Gauteng.

6.2 ANALYSIS AND INTERPRETATION OF QUESTIONNAIRES

Two types of data were collected using the questionnaire survey method. They included categorical data and numerical data. The categorical data denoted

variables while the numerical data gave measurements or counts. The univariate analysis process was used, because of the fact that single variables were being analysed mainly with a view to describing that variable (Kruger et al., 2007: 217-245).

For the purposes of this study, the researcher decided to collate the responses from the questionnaire survey (See Appendix 14) into tables. The frequency distribution was used to summarise and display the data into tables (Kruger et al., 2007: 217-245). This involved developing qualitative themes and categories. The themes and categories were given numeric codes, then counting the number of times they occur in the text data. This quantification of qualitative data enabled the researcher to compare quantitative results with the qualitative data. The data was conceptualised into three main themes relevant to the categories. The frequency table which resorts under the specific theme is interpreted and explained. It is randomly supported by literature study to confirm the accuracy of the findings (Creswell, 2009:218).

6.3 CHARACTERISTICS OF THE STUDY GROUP

The sampling of this study group was discussed in Paragraph 2.2.4. The security officials gave their consent to participate in this study. The demographic characteristics of the study group are merely being presented to describe the study group.

6.3.1 Demographic characteristics

6.3.1.1 Security service sector with which you are involved at present (See Appendix 14 question 8)

Table 6.1: Security service sector (N = 110)

Security service sector	Frequency	Cases %	Rank
Protection services (military air force, intelligence service, correctional services other government department	27	24.5%	1
In-house security (university, complex, etc.)	24	21.8%	2
Retail sectors (shops, casinos, shopping centres and hotels)	21	19.1%	3
Public service entities (Telkom, post office hospitals, other parastatals)	15	13.6%	4.5
Mining sector	15	13.6%	4.5
Private security contract companies	11	10.0%	6
Financial and insurance institutions	9	8.2%	7
City and metropolitan councils	2	1.8%	8.5
Industrial sector	2	1.8%	8.5
Transport service (road, marine, aviation)	1	0.9%	10

Twelve companies from different security service sectors participated in the study.

6.3.1.2 Gender (See Appendix 14 question 1)

Table 6.2: Gender (N = 109)

Gender	Frequency	Cases %	Rank
Male	87	76.3%	1
Female	22	19.3%	2

A total of 109 of the respondents managed to indicate their gender status, that is, in this particular question 109 responses were valid. Nearly 80% of the security

personnel officers were males; the remaining security personnel, almost 20% were females. The ratio of males to females may be attributed to the fact that the field of security service is mainly dominated by males. At present females are trying to move into this field.

6.3.1.3 Ethnicity (See Appendix 14 question 3)

Table 6.3: Ethnicity (N = 111)

Ethnicity	Frequency	Cases %	Rank
Indian	4	3.5%	4
Black	72	63.2%	1
Coloured	7	6.1%	3
White	28	24.6%	2

In terms of ethnicity a total of 111 responses were valid. About 65% of the respondents to the survey were Blacks followed by almost 25% Whites. The two categories Indian and Coloured only comprised 10 % of the respondents.

6.3.1.4 Age (See Appendix 14 question 2)

Table 6.4: Age (N = 112)

Age	Frequency	Cases %	Rank
36 – 40 years	32	28.6%	1
31 – 36 years	29	25.9%	2
41 – 45 years	24	21.4%	3
26 – 30 years	9	8.0%	4.5
46 – 50 years	9	8.0%	4.5
51 years and above	5	4.5%	6
21 – 25 years	4	3.6%	7

For the question on age a total of 112 responses were valid. The respondents were all above 20 years of age. The largest percentage of respondents (48%) was in the range 30-46 years old with at least 90% of them aged over 30 years of age. The

service security personnel are mature and thus will be able to give reliable information.

6.3.1.5 Educational qualifications (See Appendix 14 question 4)

Table 6.5: Educational qualifications (N = 112)

Educational qualification	Frequency	Cases %	Rank
Standard 10/Grade 12	38	33.9%	1
Diploma (3 years)	32	28.6%	2
Certificate	17	15.2%	3
Postgraduate degree	12	10.7%	4
Degree	10	8.9%	5
Diploma (1 year)	9	8.0%	6
Standard 9/Grade 11	4	3.6%	7
Standard 8/Grade 10 and below	3	2.7%	8.5
Advanced diploma	3	2.7%	8.5
Diploma (2 years)	1	0.9%	10

A total of 112 responses were valid for educational qualification. Some respondents managed to give more than one qualification as this was a multiple response question. Almost 33.9% of the responses were standard 10 or Grade 12 whilst only 19.6% possessed a degree or postgraduate degree.

6.3.1.6 Security service working experience (See Appendix 14 question 5)

Table 6.6: Working experience (N = 109)

Working Experience	Frequency	Cases %	Rank
10 years and above	50	45.9%	1
5 – <10 years	30	27.5%	2
3 – <4 years	9	8.3%	3.5
4-<5 years	9	8.3%	3.5
Below 1 year	5	4.6%	5
1 – <2 years	4	3.7%	6
2-<3 years	2	1.8%	7

Nearly 46% (45.9%) of the total pool of respondents had a working experience of more than 10 years. The majority of the respondents (73.4%) had more than 5 years working experience and this group was in a good position to comment about security information.

6.3.1.7 Security service position occupied at present (See Appendix 14 question 6)

Table 6.7: Security service position (N = 110)

Current position	Frequency	Cases %	Rank
Manager	46	41.8%	1
Security officer	16	14.5%	2
Supervisor	14	12.7%	3
Administration official	11	10.0%	4
Investigator	8	7.3%	5
Patrol officer	4	3.6%	6
Security guard	3	2.7%	7.5
Educator	3	2.7%	7.5
Law enforcement official	2	1.8%	9
Control room operator	1	0.9%	11
Information analyst	1	0.9%	11
Legal advisor	1	0.9%	11

In terms of security service position there were 110 valid responses. The largest percentage of respondents (41.8%) were managers, nearly fifteen (14.5%) percent were security officials. Fourteen of the respondents (12.7%) were supervisors and eleven of the respondents (10%) were administration officials.

6.3.1.8 Security service work with which you are involved at present (See Appendix 14 question 7)

Table 6.8: Security service work (N = 112)

Security service work	Frequency	Cases %	Rank
Managing, controlling or supervising the rendering of any security-related service	49	43.8%	1
Protecting or safeguarding a person or property	47	42.0%	2
Giving advice on the protection or safeguarding of person or property, on any type of security service, or on the use of security equipment	34	30.4%	3
Performing the functions of an investigator	30	26.8%	4
Providing a reactive or responsive service in connection with the safeguarding of a person or property	20	17.9%	5
Control room operator	19	17.0%	6
Providing a service aimed at ensuring order and safety on the premises used for sporting, recreational, entertainment or similar purposes	18	16.1%	7
Providing security training or instruction to a security service provider	16	14.3%	8
Making a person or the service of a person available, whether directly or indirectly for the rendering of any specialised security service	13	11.6%	9
Monitoring signals of transmissions from electronic security equipment	7	6.3%	10
Installing, service or repairing security equipment	6	5.4%	11
Manufacturing, importing, distributing, or advertising monitoring devices contemplate in section1 of the interception and Monitoring Prohibition Act 127 of 1992	2	1.8%	12.5
Performing the function of a locksmith	2	1.8%	12.5
Collection, analysis and utilisation of security information	1	0.9%	14.5
Professional advisor to the security company/organisation	1	0.9%	14.5

The respondents were asked to indicate the type of security service work they are involved in. This was a multiple response question where a respondent gave more than one response. This means some of the security service personnel are involved in more than one area. Only 1% of the security officials were involved in the

collection and analysis of security information and the application of security risk control measures. One can conclude that most security service officials were involved in managing, safeguarding, giving of advice on the protection or safeguarding of person or property and investigating.

6.3.1.9 Security service training which you have undergone (See Appendix 14 question 9)

Table 6.9: Security service training (N = 112)

Security service training	Frequency	Cases %	Rank
Risk management (risk analysis, security survey, risk assessment)	57	50.9%	1
Fire-arm handling	54	48.2%	2
Security supervisor (Grade A)	53	47.3%	3
Security first-line supervision (Grade B)	40	35.7%	4
Occupational health and safety training	39	34.8%	5.5
Access control officer (Grade D)	39	34.8%	5.5
Asset and reaction officer (Grade C)	38	33.9%	7
Patrol security office (Grade E)	37	33.0%	8
Security threat assessment	34	30.4%	9
Fire risk assessment training	28	25.0%	10
Emergency preparedness training	25	22.3%	11
Intelligence training	22	19.6%	12
Specialised investigation training	21	18.8%	13
Collection of security information	20	17.9%	14
Specialised security training	19	17.0%	15
Analysis of security information	17	15.2%	16
Implementation of security risk control measures	16	14.3%	17
South Africa police service training	2	1.8%	18.5
National prosecuting authority	2	1.8%	18.5
Advance military law practitioner	1	0.9%	20

In terms of security service training, there were 112 valid responses. This was a multiple response question. It was found that most of the security service personnel had attended more than one training course, thus, this was a multiple response question. The most frequent courses attended were risk management (risk analysis, security survey, risk assessment), firearm handling and security supervisor (grade A). Eighteen percent attended courses in the collection of security information, 15% attended courses in the analysis of security information and 14% attended courses in the implementation of security risk control measures.

Training in the collection, analysis and implementation of security information is not included in the compulsory Grade A, B, C, D and E training curriculum for security officers (Minnaar 2007: 52-65). Security service providers do not prioritise the training for the collection, analysis and application of security information.

6.4 CONCEPTUALISATION AND CATEGORISATION OF DATA: A THEMATIC EXPOSITION

6.4.1 Theme 1: Collection of security information

6.4.1.1 Who in your organisation/company is tasked by the analysts to obtain additional information to enrich the collected information? (See Appendix 14 question 55)

Table 6.10: Personnel responsible for collecting security information (N = 110)

Personnel	Frequency	Cases %	Rank
Security managers	58	52.7%	1
Investigators	45	40.9%	2
Supervisors	32	29.1%	3.5
Risk Managers	32	29.1%	3.5
Self	30	27.3%	5
Information/Intelligence unit	21	19.1%	6
Crime risk officers	13	11.8%	7
Collection units	11	10.0%	8

Table 6.10 indicates that security managers are prioritised as number 1, investigators as number 2 and supervisors/risk mangers as number 3 for collecting security information. Security service providers had not mentioned the use of security guards for the collection of security information. Security service providers had not prioritised collection units or intelligence/information units over senior security officials for the collection of security information. This implies that many security service providers do not have these units.

6.4.1.2 Have you previously collected security information? (See Appendix 14 question 21)

Table 6.11: Security information collection (N = 107)

Security information collection	Frequency	Cases %	Rank
Yes	81	71.1%	1
No	26	22.8%	2

When asked whether respondents had previously collected security information, there were 107 valid responses. Seventy-one percent acknowledged that they had previously collected security information. Only 23% had not collected security information.

6.4.1.3 Do you need permission from your supervisor/manager to collect security information on behalf of your organisation/company? (See Appendix 14 question 18)

Table 6.12: Permission to collect security information (N = 113)

Permission	Frequency	Cases %	Rank
Yes	63	55.3%	1
No	50	43.9%	2

Fifty-five percent of the 113 valid responses indicated that they need permission from the supervisor/manager to collect security information on behalf of their organisation or company.

6.4.1.4 Does your organisation/company have the necessary resources to collect security information? (See Appendix 14 question 32)

Table 6.13: Resources (N = 110)

Resources	Frequency	Cases %	Rank
Yes	98	86.0%	1
No	12	10.5%	2

When asked whether respondents had the necessary resources to collect security information, there were 110 valid responses. Eighty-six percent of the 110 security service personnel who responded to the question indicated that their company has the necessary resources to collect security information. Only 10.5% indicated they do not have the necessary resources.

6.4.1.5 Please indicate if you have previously received security information in any of the following situations? (See Appendix 14 question 25)

Table 6.14: Receipt of security information (N = 108)

Situations	Frequency	Cases%	Rank
Information about a crime/incident from a victim/complainant	72	66.7%	1
Information while investigating a crime/incident	66	61.1%	2
Voluntary information from a third party	65	60.2%	3
Information from informants	59	54.6%	4
Information through interaction with personnel	58	53.7%	5
Information through interaction with clients	57	52.8%	6
Information through interaction with the general public	54	50.0%	7
Information while at a crime/incident scene from observers	51	47.2%	8
Information while investigating a suspicious activity report	45	41.7%	9
Forums (explosives, illegal mining forum, illegal special metal forum)	22	20.4%	10
Analysis results from an analyst	1	0.9%	11.5
Security information from the mass media	1	0.9%	11.5

A total of 108 valid responses, mentioned that they received security information under different situations. This was a multiple response question. The three most common sources from which security information was collected include information about a crime/incident from a victim/complainant, security information while investigating a crime incident and voluntary security information received from a third party. About 66.7% of security information about a crime/incident was received from a victim/complainant. About 61.1% of security information was received while investigating a crime/incident. About 60.2% of security information was voluntary information received from a third party. According to Table 6.14 no specific effort was made by the security officials to collect security information on specific matters within a specific context to address a specific threat.

According to Talbot and Jakes, (2008:142) the reliability of the information source and the credibility of the information should be assessed on criteria such as the previous quality of the information supplied by the source, the situation, the location and the likely access of the source at the time the information was collected. The accuracy of the information is assessed as an actual measurement in relation to each item of information received.

6.4.1.6 Please indicate the type of security information you personally collected during the past month (See Appendix 14 question 28)

Table 6.15: Type of security information collected (N = 99)

Type of information	Frequency	Cases %	Rank
Company policy breaches/violations, etc	58	58.6%	1
Physical security breaches	55	55.6%	2
Crime threats	53	53.5%	3
Electronic security breaches	35	35.4%	4

A total of 99 valid responses mentioned the type of security information they personally collected as indicated in Table 6.15. Table 6.15 shows that most security information collected related to company policy breaches/violations and physical security breaches. It is clear that crime threats were not prioritised by the respondents as compared to policy violations. There is no indication of the collection

of security information on vulnerabilities and incident. It would seem that the security service providers do not support the SAPS in the prevention of crime and investigation of criminal cases. There is no indication of collecting such information in Table 6.15. This implies that security service providers do not encourage the sharing of information with the SAPS.

6.4.1.7 Have you previously collected security information by making use of a 'collection plan'? (See Appendix 14 question 23)

Table 6.16: Collection plans (N = 108)

Collection plans	Frequency	Cases %	Rank
Yes	33	28.9%	2
No	75	65.8%	1

The "collection plan" seemed not to be a popular method of collecting security information. Only 28.9% of the 108 valid responses indicated that they had used it before. Thus, a large majority of the respondents, about 66 % had not used it before.

6.4.1.8 If you answered "Yes" to question 23, what kind of collection plan did you use? (See Appendix 14 question 24)

Table 6.17: Kinds of collection plans (N = 27)

Collection Plan	Frequency	Cases %	Rank
SWOT analysis	17	63.0%	1
Investigation plan	12	44.4%	2
Intelligence collection plan	9	33.3%	3
Occurrence book (OB)	2	7.4%	4.5
Statement	2	7.4%	4.5
Random collection of information	1	3.7%	6.5
Meetings with staff members from different sections	1	3.7%	6.5

On the different kinds of collection plans used, there were only 27 valid responses. Those who used collection plans mentioned the kinds of collection plans in Table 6.17. This was a multiple response question. The most common collection plans

were referred to as strength, weakness and opportunity (SWOT) analysis documents, investigation plans and intelligence collection plans. SWOT analysis was indicated by 63%, investigation plans by 44.4% and intelligence collection plans by 33.3%.Table 6.17 shows that the security service in Gauteng does not use a prescribed collection plan nor does it design one for individual situations. Further, it is implied that out of 114 respondents only 27 respondents participated in this question. This indicates that the majority of the security officials do not use collection plans nor do they know of such an instrument. This supports the finding in Table 6.16 that 65.8% of the respondents do not use collection plans

SWOT analysis documents may be used to put in place a threat assessment, which can result in the development of collection plan to collect security information.
SWOT analysis documents cannot by itself be used as a collection plan. An investigation plan will help guide an investigation until its conclusion, but cannot serve as a collection plan. With exception to the intelligence collection plan, all other responses provided in Table 6.17 cannot serve as collection plans.

6.4.1.9 Do you understand the steps to be followed when collecting security information? (See Appendix 14 question 19)

Table 6.18: Understanding of the steps used in the collection of security information (N = 103)

Understanding of the steps used in the collection of security information	Frequency	Cases %	Rank
Yes	76	66.7%	1
No	27	23.7%	2

Nearly 67% of the 103 respondents indicated that they understood the steps to be followed when collecting security information.

6.4.1.10 In the space provided, outline all the steps to be followed when collecting security information (See Appendix 14 question 20)

Table 6.19: Steps to follow in the collection of security information (N = 110)

Steps to follow in the collection of security information	Frequency	Cases%	Rank
Gather all the information	62	76.5%	1
Analysis of the collected information	34	42.0%	2
Identify the risk at hand	31	38.3%	3
Get a mandate from the company/top management	21	25.9%	4
Make notes/reports/complete specific forms	14	17.3%	5
Ensure high-level confidentiality	11	13.6%	6
Utilisation of analysis results	10	12.3%	7
Capture data and store in database for future reference	7	8.6%	8
Complete a detailed analysis report and forward it to immediate senior	6	7.4%	9
Establish a steering committee to implement policies and to exercise control	3	3.7%	10

According to Table 6.19 there were 110 responses for the steps to be followed in the collection of security information. This was a multiple response question where respondents indicated more than one step. The respondents identified the steps they are most likely to follow. Based on the different responses given by the participants on the steps to be followed, it can be concluded that there is no standard operating procedure to guide security personnel. When it comes to security it is important for security personnel to understand the steps to be followed in the collection of security information.

The steps which were given by most of the respondents were to gather all the information, analyse the collected security information and then identify the risk. These steps are commonly used in security risk management (risk analysis). The steps used for the collection of security management differ from those used for risk

management. According to Garcia (2006: 2), Security Risk Management is a set of actions an enterprise takes to address identified security risks and includes avoidance, reduction, spreading, transfer, elimination and acceptance options.

In security information management, the three documents which are crucial are: Crime Pattern Analysis (CPA) (Gottlieb et al., 1994: 161), Threat Assessment (TA) document (Garcia, 2008: 26) and a Vulnerability Assessment (VA) document (Garcia, 2006: 1). These documents define threats and vulnerabilities which need to be addressed. According to Garcia (2008: 26), a Threat Assessment document defines the threat and directs the collection of security information on the potential threat. A Vulnerability Assessment document defines the weak points for a defined threat at a facility. These weak points direct the collection of security information (Garcia, 2006: 1). A CPA document acquaints officers with the types of crimes being committed. It lists the days, times and locations of their occurrence; and provides officers of any known suspects, suspect vehicles, modus operandi and or property loss information.

Essentially, the first step in the collection of security information will involve the Threat Assessment, Vulnerability Assessment and the Crime Pattern Analysis documents approved by management. A specific mandate or security policy is required from an organisation's top management before collection of security information takes place (Rogers, 2008: 152). The context for the collection of security information is then defined (Talbot & Jakeman, 2008: 177). These three documents are used to develop a collection plan for the collection of security information. This step involves the identification of objectives for the collection of security information. The second step will be to establish the context, the area in which you want to direct your resources and energy to collect security information. You may want to focus on the external context, internal context and security risk management context, on the process/program structure, evaluation criteria, security agendas of stakeholders or on the security business case, specific assets, etc. The third step involves the gathering of security information on threats and vulnerabilities leading to security risk control measures. Incident based information is generated on its own. No collection plan is used for incident based information. Incident based information is used to enrich the Threat Assessment document. Security risk

identification normally flows from the context and is informed by the threat, vulnerability and criticality assessments as well as incident related information, management systems and program activities (Talbot & Jakeman, 2008: 177).

6.4.1.11 Please indicate if you have previously used any of the following method/s to gather security information (See Appendix 14 question 26)

Table 6.20: Methods used to collect security information (N = 108)

Methods used to collect security information	Frequency	Cases%	Rank
Physical surveillance (observation tailing, etc.)	71	65.7%	1
Electronic surveillance (camera, biometrics, hi-tech, etc	70	64.8%	2
Interviews (briefing debriefing, etc.)	64	59.3%	3
Internal audit (internal sources for example risk analysis security survey, etc.	49	45.4%	4
Research (external sources for example South Africa police Home affairs, etc.)	40	37.0%	5
Interrogations	37	34.3%	6
Undercover	33	30.6%	7
Forensics	15	13.9%	8
Hacking into computer databases for information	5	4.6%	9
Mass media	2	1.9%	10

In terms of the methods used in collecting security information there were 108 valid responses. The popularity of the methods used are indicated in Table 6.20. The most common methods are physical surveillance (65.7%) and electronic surveillance (64.8%), interviews (59.3%) and internal audit (security assessments) (45.4%). Very little use is made of open sources such as the mass media (1.9%) to collect security information. External sources (Research) and forensics are also neglected. According to Rogers (2008: 152), security risk managers gather security information through interviews, observation and the examination of internal and external source documents. They also use security survey checklists to gather security information on vulnerabilities.

Ferraro and Spain (2006: 13), state that there are six methods commonly used to collect information. These methods include physical surveillance, electronic surveillance, internal auditing, research, forensics, undercover, interviews and interrogations. These methods may be combined in some fashion or mixed and matched for use.

6.4.1.12 Please indicate the item that best describes how you handled the collected security information (See Appendix 14 question 29)

Table 6.21: Handling of security information (N = 105)

Handling of security information	Frequency	Cases %	Rank
Informed immediate manager/supervisor	65	61.9%	1
Recorded information in the control room OB	40	38.1%	2
Recorded information in an incident register	34	32.4%	3
Recording information in personnel pocket book	31	29.5%	4
Informed the investigating unit	30	28.6%	5
Utilised information to perform task	29	27.6%	6
Informed the unit that handles all collected information	23	21.9%	7.5
Entered the information into an electronic database (computer)	23	21.9%	7.5
Forwarded the information to law enforcement	21	20.0%	9
Informed the supervisor on the duty parade	14	13.3%	10.5
Forwarded the information to human resources management for disciplinary investigation	14	13.3%	10.5
Informed the analysis unit	13	12.4%	12
Did nothing with the information	1	1.0%	13

In terms of items that best describe how the collected security information is handled, a total of 105 responded to the question. About 75% of the respondents handed the collected information to their immediate manager/supervisor or the

supervisor on parade as indicated in Table 6.21. More than 70% either recorded the information in the control room occurrence book or in the information register. Twenty-two percent entered the information into a computer system. Twenty-two percent handed the information to the collection unit, whist 12.4 % handed the information over to the analysis unit. About 13% handed the collected information over to human resource management for disciplinary investigation. Only 1 % did nothing with the information. It is clear that there is no standard operating procedure on how the collected security information need to be handled. A standard operating procedure in this regard is important for the protection of security information and to prevent leakage of information (SABRIC, 2011).

6.4.1.13 Are there security measures in place in your organisation/company for the protection of information (data)? (See Appendix 14 question 30)

Table 6.22: Protection of security information (N = 110)

Protection of security information	Frequency	Cases %	Rank
Yes	104	91.2%	1
No	6	5.3%	2

A clear majority, almost 91.2% out of the 110 valid responses mentioned that there are security measures in place for the protection of information in their company. Only 5.3% indicated that there were no security measures for the protection of security information in their company.

6.4.1.14 If you answered "Yes" to question 30 please indicate which of the following information (data) protection measures are being used by your organisation/company (See Appendix 14 question 31)

Table 6.23: Security information protection methods (N = 105)

Security information protection methods	Frequency	Cases %	Rank
Organisation/company policy on the classification of information for example confidential, secret, restricted	73	69.5%	1
Information Protection Act	46	43.8%	2
Minimum information Security Standard (MISS) approved by Cabinet	37	35.2%	3
Security clearance to access classified information	36	34.3%	4
Access is allowed on a need-to-know basis	31	29.5%	5
Access to information database is not allowed to employees below management	30	28.6%	6
Access to information act	24	22.9%	7

One hundred and five respondents identified information protection methods as indicated in Table 6. 23.The three common measures mentioned by the respondents include; organisation/company policy on the classification of information for example confidential, secret, restricted; Information Protection Act and the Minimum Information Security Standard (MISS) approved by Cabinet. No regulatory standard has been implemented by PSIRA for the protection of security information by all security service providers (Private Security Industry in South Africa, 2012). Each security service provider applies his/her own method of protecting security information.

The ISO 7498/2 is considered one of the best reference frameworks for introducing information security. The five stages that ISO identifies are identification and authentication, authorisation, confidentiality, integrity and non repudiation (Kritzinger, 2006: 10).

6.4.1.15 Does your organisation/company store the collected security information in a database? (See Appendix 14 question 33)

Table 6.24: Storage of security information (N = 109)

Storage of security information	Frequency	Cases %	Rank
Yes	96	84.2%	1
No	13	11.4%	2

In terms of whether the company stores collected security information in a database, there were 109 valid responses and 84.2% indicated that their company stores security information. Only 11.4% indicated that their companies do not store security information.

6.4.1.16 If you answered "Yes" to question 33, in which database is the collected security information stored? (See Appendix 14 question 34)

Table 6.25: Security information storage database (N = 98)

Storage Database	Frequency	Cases %	Rank
Both electronically and manually	66	67.3%	1
Electronic database (computer system)	48	49.0%	2
Manual database (handwritten in a regular, document, etc.)	23	23.5%	3

Of the respondents who said that their company stores the security information in a database, 98 of them mentioned the data system in Table 6.25. About 67, 3% indicated that their company's store security information in both electronic and manual storage systems. Forty-nine percent indicated that their companies store security information in electronic databases (computer). It is of concern that there are still 23.5% of security service providers who are still using the manual system.

According to Block et al. (1995: 15), there are often too many pieces of information to store manually. It becomes impossible for the human mind to assimilate them, sort them and use them for strategic and tactical decision-making. This has precipitated a

technological revolution, such as electronic databases for the storage of information doing computer mapping and generating actionable crime information products. It has also been found that the electronic system supplements the expertise of experienced officers and it avoids that the knowledge and techniques accumulated over the years do not retire with a veteran official. It must be available for others to build on.

6.4.1.17 If the collected security information is stored in a database (computer or manual), who is responsible for entering the data onto the database? (See Appendix 14 question 35)

Table 6.26: Personnel responsible for storing security information (N = 105)

Personnel	Frequency	Cases %	Rank
Security managers	57	54.3%	1
Self	31	29.5%	2.5
Investigation officer	31	29.5%	2.5
Supervisors	21	20.0%	4
Data administrator	19	18.1%	5
Data typist	16	15.2%	6.5
Data analyst	16	15.2%	6.5
Admin. Official	10	9.5%	8
Clerk	5	4.8%	9

A total of 105 respondents mentioned the personnel involved in storing the information as indicated in Table 6.26. Table 6.26 shows that security managers (54.3%) are mostly involved in storing the information. Only a small proportion (4.8%) use clerks for storing information. Security personnel should be empowered to store their own security information onto the system. It is clear from the responses that only 29.5% of the respondents store their own information onto the data system.

6.4.1.18 Have you previously experienced any problems in the collection of security information? (See Appendix 14 question 39)

Table 6.27: Problems experienced in the collection of security information (N = 110)

Problems	Frequency	Cases %	Rank
Yes	44	38.6%	2
No	66	57.9%	1

Close to 39% of the 110 respondents mentioned that sometimes they experience problems when collecting security information whilst 57.9% did not experience any problems.

6.4.1.19 If you answered "Yes" to question 39, please indicate the nature and extent of the problems (shortcomings) experienced in the collection of security information (See Appendix 14 question 40)

Table 6.28: Nature and extent of problems (N = 41)

Nature and extent of problems	Frequency	Cases %	Rank
People scared to give out information due to fear of victimisation	23	56.1%	1
Incomplete/inaccurate/unreliable information	9	22.0%	2
Security personnel not trusted	8	19.5%	3
Insufficient knowledge on the collection of security information	4	9.8%	4.5
Lack of resources	4	9.8%	4.5
No sharing of information takes place	2	4.9%	6
Lack of role players to share information	1	2.4%	7

Those respondents who identified problems in Table 6.27 mentioned the nature and extent of the problems as indicated in Table 6.28. Fear and victimisation (56.1%) was seen to be the biggest inhibiting factor in the collection of security information. This indicates that personnel are reluctant to assist in workplace investigations involving their fellow employees because of fear of victimisation. Although companies encourage whistle-blowing, by providing for procedures in terms of which employees may disclose information anonymously regarding unlawful or irregular conduct by their employers or fellow employees, employees still fear victimisation and intimidation. Twenty-two percent indicated incomplete/inaccurate/unreliable information as a problem. About 20% indicated that security personnel are not trusted. About 9.8% indicated lack of resources, about 9.8% insufficient knowledge on collection and 4.9% reluctance in sharing information. This indicates that management is not doing enough to enhance an information awareness culture.

6.4.1.20 What solutions do you suggest for solving the problems (shortcomings) you encountered as indicated in question 40? (See Appendix 14 question 41)

Table 6.29: Solutions to overcome problems of collection of security information (N = 38)

Solutions	Frequency	% of cases	Rank
Security personnel to be developed on the collection of security information	13	34.2%	1
Should be policies for the protection of witnesses against victimization	12	31.6%	2
Security information to be protected through classification	10	26.3%	3
Trust the security personnel	7	18.4%	4
To have sufficient resources for the collection of security information	4	10.5%	5
Encourage sharing of information	1	2.6%	6

About 34.2% of the respondents indicated that security personnel need to be developed in the collection of security information while 31.6% indicated there should be policies for the protection of witnesses against victimisation. About 18.4% indicated that security personnel should be trusted and 10.5% indicated that there should be sufficient resources for the collection of security information. It is clear that there is a dire need for training in the collection of security information.

Interpretation: In general security information is not collected according to the threats and vulnerabilities confronting an organisation. Most of the information is randomly collected by security managers, investigators and supervisors. This type of collection is done mainly by using technical and human methods. No standardised framework is in place to guide security personnel on the collection of security information. There is no mention made of an organisational security strategy, security plan, Threat Assessment document, Vulnerability Assessment document or a collection plan on the steps followed to collect security information in Table 6.19. It is indicative that security information is arbitrarily collected with no objectives and outcomes to guide the process.

The handling of the collected security information should be streamlined to be less cumbersome, so that information may be immediately operationalised. More emphasis is placed on collecting security information on incidents than on threats and vulnerabilities. This is confirmed by the fact that 67% of the information is collected from victims and complainants involved in incidents. Security personnel are more accustomed to the model used for Security Risk Management. There is this confusion of mixing the processes used for security risk management with that of security information management.

Only 50% of the respondents use automated systems to store information. This is an indication that about 50% use other means than computers for the storage of security information. The protection of information should be based on trust rather than creating mistrust between management and grassroots security personnel. This is based on the assumption that grassroots security personnel come into daily contact with personnel and clients and serve as the eyes and ears of management. Sharing of information between management and grassroots personnel will go a long

way in intensifying the collection of security information. Fear and victimisation is seen as the biggest intimidating factor in the collection of security information. Personnel are reluctant to provide security. Many workplace investigations are not successfully concluded because of personnel being reluctant to make statements implicating colleagues. In view of existing problems in the collection of security information; it can be assumed that management in the security business is not creating a culture of information awareness. Issues such as training, policies, trust, classification of information, sharing of information and resources were identified as solutions to improve the collection of security information.

6.4.2 Theme 2: Analysis of security information

6.4.2.1 Have you previously analysed security information? (See Appendix 14 question 53)

Table 6.30: Analysis of security information (N = 111)

Previously analysed security information	Frequency	Cases %	Rank
Yes	88	77.2%	1
No	23	20.2%	2

Almost 77% of the 111 valid responses indicated that they had analysed security information before. Only 20.2% of the respondents indicated that they did not analyse security information before. The 77% of the respondents who indicated to have previously analysed security information are making reference to decisions made on the security information rather than analysis per se.They did not follow any analysis steps or processes in making decisions on the collected security information. Most of these decisions' were made on incident based information. Many of the security service providers do not have analysis capabilities in their companies. Security officers are not trained; neither do they possess the necessary qualifications as analysts to carry out any analysis function on security information.

6.4.2.2 If you answered "Yes" to question 53, please indicate which of the following stages of the analysis process you have previously been involved with (See Appendix 14 question 54)

Table 6.31: Stages of involvement in the analysis process (N = 87)

Stages of involvement in the analysis process	Frequency	Cases %	Rank
Identifying counter-measures that will prevent or mitigate security risks	62	71.3%	1
Identifying security risks to the assets	60	69.0%	2
Identifying assets (people material, legalities) deserving protection	59	67.8%	3
Estimating the probability that security risks will materialize	44	50.6%	4
Estimating the impact of security risks occurrences	41	47.1%	5.5
Assessment of manageability of security risks	41	47.1%	5.5
Estimating the frequency of event occurrences	39	44.8%	7

Only 87 respondents of the 88 who previously analysed security information as indicated in Table 6.30 mentioned the stages they were involved in as mentioned in Table 6.31. About 71% of the total respondents were involved in the identification of countermeasures that prevented or mitigated security risks occurrences. Sixty-nine percent were involved in the identification of security risks to the assets. About 68% were involved in the identification of assets (people material, legalities) deserving protection. About 50% were involved in estimating the probability of security risks occurrences, 47.1% on estimating the impact of security risk occurrences and 44.8% estimating the frequency of event occurrences. About 47% of the respondents were involved in the assessment of the management of security risks. This confirms that the respondents used the security information to make decisions for security risk management rather than following a security information analysis process in security information management.

The different stages of the analysis process indicated in Table 6.31 refer mainly to the Security Risk Management Process and not the Security Information Analysis Process in security information management. Both the processes have different approaches (refer to Figure 7.2 and Paragraph 1.2.6.). Security risk management allows the risk to be handled in a logical manner, using long held management principles. Security risk management includes four basic steps namely; identification of risks or specific vulnerabilities, analysis and study of risks, optimising risk management alternatives and the implementation of security programs (Fischer et al,. 2008: 148).

According to Talbot and Jakeman (2008:177), all security information including threats and vulnerabilities need to be evaluated/verified as the first step. This step will determine the likelihood and consequences of the information materialising. Collation is seen as the second step and analysis is seen as the third step. Once the security information is evaluated/verified, it is collated and analysed. The collation and analysis steps help identify security risk control measures. Incident based information is handled differently since the threat has already materialised. All the analysed information contributes to the threat assessment document, vulnerability assessment document and a crime pattern analysis document of all the incidents that have occurred.

6.4.2.3 Indicate the 'analysis result' provided to you (See Appendix 14 question 67)

Table 6.32: Types of analysis results provided by analysts (N = 108)

Analysis Results	Frequency	Cases %	Rank
Security assessments	56	51.9%	1
Crime analysis reports	49	45.4%	2
Security awareness products	48	44.4%	3
Alerts	42	38.9%	4
Profiles	40	37.0%	5
Security risk mitigating strategies	36	33.3%	6
Statistical analysis reports	31	28.7%	7
Target analysis reports	20	18.5%	8

In terms of the types of analysis results provided by the analysts, there were 108 valid responses. This was a multiple response question where respondents gave more than one response. Table 6.32 indicates that 51.9% of the respondents received security assessments. Over 90% of the respondents receive reports (crime, statistical and target related). About 33.3% receive strategies, while over 100% of actionable information products are generated. Table 6.32 shows that security service providers generate more actionable information products, reports and security assessments than strategies to reduce crime, increase detection rates and prevent losses.

According to Horne (2009: 78), the use of analysis results cannot be underestimated. Therefore, there is a need to employ competent and professional analysts to provide high quality analysis products. Some of the analysis results such as actionable crime information products commonly used in law enforcement include, linkage analysis, flowcharting, financial analysis, association analysis, spatial analysis, geographic crime pattern analysis, crime mapping, the Geographic Information System (GIS), profiling, timeline analysis and document analysis.

6.4.2.4 Have you previously experienced any problems in the analysis of security information? (See Appendix 14 question 56)

Table 6.33: Problems experienced in the analysis of security information (N = 109)

Problems experienced in analysis	Frequency	Cases %	Rank
Yes	35	30.7%	2
No	74	64.9%	1

About 31% of the respondents have previously experienced problems in the analysis of security information, while 64.9% did not experience any problems in the analysis of security information.

6.4.2.5 If you answered "Yes" to question 56, please indicate the nature and extent of the problems (shortcomings) you encountered when analysing security information (See Appendix 14 question 57)

Table 6.34: Nature and extent of problems encountered in analysis (N = 30)

Nature and extent of Problem encountered in analysis	Frequency	Cases %	Rank
Insufficient, unreliable and inaccurate information received for analysis	22	73.4%	1
Need for qualified analysts	10	33.3%	2
Information should be classified according categories in relation to crime	2	6.7%	3
Sometimes managers take long time to implement the results of the analysis	1	3.3%	5
Problems with IT equipment used for analysis	1	3.3%	5
Information overload	1	3.3%	5

Only 30 of the 109 responses indicated in Table 6.33 identified some of the problems experienced by them. This is indicated in Table 6.34. The problems relevant to data integrity (73.4%) shortage of qualified analysts (33.3%) and information overload (3.3%) shows that there is a need for intervention by management and standing operating procedures for the analysis of security information.

6.4.2.6 What solutions do you suggest for solving the problems (shortcomings) you encountered as indicated in question 57? (See Appendix 14 question 58)

Table 6.35: Solutions to overcome problems of analysis in security information management (N = 29)

Solutions to overcome problems of analysis	Frequency	Cases %	Rank
Training of security officers on the analysis of information	12	41.4%	1
Managers must have a good relationship with subordinates	6	20.7%	2
To provide more resources for analysis	4	13.8%	3
The sources and information must be tested before information is placed on record	3	10.3%	5
Collect as much information as possible to support the analyst	3	10.3%	5
Methods used for identification/classification should be improved	3	10.3%	5
Analysts to stay in touch with world class technology	2	6.9%	8
Policies and procedures must be implemented for the analysis of information	2	6.9%	8
Investigator must have knowledge of the specific action/conduct	2	6.9%	8
Experienced personnel should be used to do analysis	1	3.4%	11
Act according to the information received	1	3.4%	11
Outsourcing of the analysis function	1	3.4%	11

A total of 29 valid responses provided solutions to overcome the problems. This was a multiple response question were people gave more than one response. About 41.4% of the responses relate to the training of security officers in the analysis of security information. Other solutions include improvement of relationship between management and subordinates (20.7%), need for resources to do analysis 13.8%,

need for policies and procedures (6.9%), need for experienced analysts (3.4%). Table 6.35 shows that there is a need for intervention by management.

Interpretation: The quality of security information received for analysis will determine the results of the analysis which may take the form of a recommendation for strategy, security protection systems or actionable information products to address a specific threat. About 73.4% of the security information received by security officers for decision making is insufficient, unreliable and inaccurate information. In many instances this information is used for decision making by security management without any form of enrichment. These decision makers are mainly security officers or security supervisors with no analysis training or qualifications. Security information only goes through an analysis process if the security service provider has an analysis capability. Due to the cost of such an infrastructure, very few security companies have an analysis capability. Hence, very little security information goes through the analysis process. The indication that about 77% of the security personnel have previously analysed information is an indication that this percentage of security information was used by management for decision making, which has been interpreted by respondents as being analysed by the security company. This is further supported by the result that 71.3% of the security personnel have been involved in the identification of counter measures to mitigate security risks. This means that in the majority of cases security information was used for decision making on security risk management without actually following the steps in the analysis process for security information management. Security companies and the organisations being protected will need to establish analysis capabilities managed by trained and qualified security information analysts. It is important that qualified analysts should be employed to conduct security information analysis. According to Ratcliffe (2009: 94), the analyst should be an expert on security related matters. He/she must be able to apply environmental criminology, understand incidents of crime/violation of security related policies, vulnerabilities and threats. Security analysts must be able to perform in-depth analysis, identify solutions, communicate effectively and be able to evaluate the outcomes and solve problems.

The organisational strategic direction, the security plan, Threat assessment, Vulnerability Assessment and the needs of the clients ought to be considered for the purpose of analysis. It is clear from the types of results of analysis provided by analysts that this is not the case. It appears as though security service providers generate more actionable information products, reports and security assessments than strategies to reduce crime, increase detection rates and prevent losses. This function of analysis needs more innovation and cognitive thinking. There is also an information overload problem which indicates that any information is collected at random and given for analysis. It would seem that the trend is to analyse all information that is received to prepare counter measures even though there is no threat present. This to the knowledge of the researcher is a waste of money, human resources and technology on the analysis of security information which is a not a key information need of management. The key information need should be part of the security plan or specifically requested by management (Muller, 2002c: 5-6). The fact that there is a need for qualified analysts, computer equipment and analytical software it is sufficient to assume that security service providers find it difficult to reduce crime, increase detection rates and prevent losses. Issues such as training, evaluation of information, policies, technology, resources, relationships, classification and outsourcing were identified as solutions to improve the analysis of security information.

6.4.3 Theme 3: Implementation of security risk control measures

6.4.3.1 Indicate in what manner (way) the "analysis result" was disseminated to you (See Appendix 14 question 68)

Table 6.36: Dissemination of analysis results (N = 110)

Manner of disseminating analysis results	Frequency	Cases %	Rank
Reports	77	70.0%	1
Briefing	65	59.1%	2
Meetings	62	56.4%	3
Handouts	19	17.3%	4
E-mail	4	3.6%	5

Of 110 respondents who responded, 70% indicated that the dissemination was done by reports. The main modes of dissemination are reports, briefings and meetings as indicated in Table 6.36. According to Reuland (1997: 35), dissemination may be carried out in several different ways, namely, by attending briefings and strategy sessions, presenting verbal reports, providing written reports, having face-to-face contact with detectives whenever the need arises and public information systems – both written and electronic media.

6.4.3.2 Have you previously encountered any problems in the dissemination of the "analysis result" to you? (See Appendix 14 question 69)

Table 6.37: Problems experienced in the analysis of security information (N = 112)

Problems experienced	Frequency	Cases %	Rank
Yes	28	24.6%	2
No	84	73.7%	1

About 24.6% out of 112 valid responses have experienced problems in the dissemination of security information, while 73.7% did not experience any problems in the dissemination of security information.

6.4.3.3 If you answered "Yes" to question 69, please indicate the nature and extent of the problems (shortcomings) experienced in the dissemination of the "analysis result" to you
(See Appendix 14 question 70)

Table 6.38: Nature and extent of problems experienced in the dissemination of analysis results (N = 25)

Nature and extent of problems experienced	Frequency	Cases%	Rank
Management undermines and generalises the analysis results before it is disseminated	20	80.0%	1
No ongoing communication between analyst and user of analysis results	4	16.0%	2
Dissemination of analysis results not being done by analysts	2	8.0%	3.5
Analysis results takes too long	2	8.0%	3.5
No computer access given to receive analysis results	1	4.0%	6
Analysis results not protected by classification	1	4.0%	6
No policy for the dissemination of analysis results	1	4.0%	6

According to Table 6.38, the biggest setback is that management undermines the analysis results prior to dissemination. Many security service providers do not have policy for the dissemination of analysis results to end users.

6.4.3.4 What solutions do you suggest for solving the problems (shortcomings) indicated in question 70? (See Appendix 14 question 71)

Table 6.39: Suggested solutions for dissemination problems (N = 22)

Solution for dissemination problems	Frequency	Cases %	Rank
Regular communication should take place between analyst and user	9	40.9%	1
User should be allowed to request additional analysis on the result	5	22.7%	2.5
Dissemination should also take place formally by means of report	5	22.7%	2.5
Management should not undermine analysis results	3	13.6%	4
Train personnel in the dissemination of analysis results	2	9.1%	5.5
Management to trust security personnel and not generalise analysis results	2	9.1%	5.5
Analysis results should be classified	1	4.5%	8
Computer access should be given to all security personnel	1	4.5%	8
Management should not interfere with analysis function	1	4.5%	8

In terms of solutions, 22 responses provided solutions in Table 6.39. According to Table 6.39 over 40 % of the responses indicate better communication between the analyst and the end users. About 18% of the responses are of the view that management should not undermine analysis results or interfere with analysis function. On considering the solutions to overcome the problems in the dissemination of analysis results one can conclude that the respondents would like full cooperation from management.

6.4.3.5 Have you in the past provided feedback to the analysts on the implementation of the "analysis result" information provided (disseminated) to you? (See Appendix 14 question 72)

Table 6.40: Feedback on the implementation of the analysis results (N = 108)

Feedback	Frequency	Cases %	Rank
Yes	64	56.1%	1
No	44	38.6%	2

Fifty-six percent of the 108 responses indicated that they provide feedback to management on the implementation of the security risk control measures, whilst 38.6% do not provide feedback.

6.4.3.6 If you answered "Yes" to question 72, please indicate the type of feedback you provided to the analysts (See Appendix 14 question 73)

Table 6.41: Type of feedback provided to analysts (N = 78)

Type of feedback provided to analysts	Frequency	Cases %	Rank
Formal feedback	26	26.2%	2
Informal feedback	19	29.7%	3
Both (Formal and Informal)	33	51.6%	1

The types of the feedback were mentioned by 78 respondents as indicated in Table 6.41. Both formal and informal types are used in giving feedback to analysts.

6.4.3.7 Have you previously experienced any problems (shortcomings) in the implementation of the "analysis result" that was provided to you? (See Appendix 14 question 74)

Table 6.42: Problems experienced in the implementation of security risk control measures (N = 108)

Problems	Frequency	Cases %	Rank
Yes	20	17.5%	2
No	88	77.2%	1

Only 17.5% of the 108 respondents indicated that they experienced problems in the implementation of security risk control measures. About 77.2% did not experience problems in the implementation of security risk control measures.

6.4.3.8 If you answered "Yes" to question 74, please indicate the nature and extent of the problems (shortcomings) experienced in the implementation of the "analysis result" (See Appendix 14 question 75)

Table 6.43: Nature and extent of the problems experienced in the implementation of security risk control measures (N = 17)

Nature and extent of problems experienced	Frequency	Cases %	Rank
Analysis result not relevant to the security risk prevalent at the time	6	35.3%	1
Not experienced to utilise analysis results	4	23.5%	2
Data integrity of the Analysis results	3	17.6%	3.5
Clients are unwilling to pay for additional resources to implement analysis results	3	17.6%	3.5
Lack of resources to utilise analysis results	2	11.8%	5.5
No communication between the analyst and the user	2	11.8%	5.5

Respondents who answered this question indicated their problems in Table 6.43. About 35.3% of the respondents indicated that the analysis results are not relevant to the security risk prevalent at the time. About 11.8% indicates that there is a shortage of resources to implement security risk control measures. About 11.8% indicate that there is no communication between the analyst and the end user. The responses in Table 6.43 show that analysis is not being conducted according to the needs of the client.

6.4.3.9 What solutions do you suggest for solving the problems (shortcomings) indicated in question 75? (See Appendix 14 question 76)

Table 6.44: Solutions to overcome problems in the implementation of security risk control measures (N = 16)

Solutions to overcome problems	Frequency	Cases %	Rank
Training security personnel to utilise analysis results	5	31.3%	1
Data integrity of analysis results should not be compromised	4	25.0%	2
Regular communication should exist between analyst and user	3	18.8%	3
Formulate policies to guide the utilisation of analysis results	2	12.5%	4.5
Make available resources for utilisation	2	12.5%	4.5
Analysis results should not be generalised	1	6.3%	8
Implementation of analysis results should be cost effective	1	6.3%	8
Managers should not undermine the analysis results	1	6.3%	8
Experienced security personnel to be used in the utilisation of analysis results	1	6.3%	8
Project management approach to be followed in the utilisation of the analysis results	1	6.3%	8

A total of 16 respondents gave the solutions they think will solve the problems. This was a multiple response question were people gave more than one response. Looking at the solutions one can conclude that the respondents would like see security personnel trained to implement analysis results and the formulation of policies to guide the application of security risk control measures.

Interpretation: No policy framework exists for the implementation of security risk control measures. All analysts' findings and recommendations are generalised by

management to down play the seriousness of the threat or vulnerability. Different methods are used for dissemination and feedback. This may seriously compromise the protection of the information and result in leakage of information. The implementation of security risk control measures is not needs driven. It does not take into consideration the reduction of crime, increasing the detection rates and preventing losses. The fact that communication is not encouraged between the analysts and the end user indicates that the implementation of the security risk control measure is not monitored and evaluated. Issues such as training, policies, communication, data integrity, resources, experience and a project management approach were identified as solutions to improve the implementation of security risk control measures.

6.5 CONCLUSION

The themes, categories, concepts and processes were numerically analysed according to frequency, percentage and ranking. They were interpreted in terms of the research questions. The status quo of security information management was determined and problems were identified in the collection and analysis of security information and the implementation of security risk control measures. The findings of this data and analysis of the questionnaires will be discussed in Paragraph 8.1 and compared with the theory as identified in Chapter 3. The interpretations which are based on the responses provided by the respondents make the interpretation reliable and valid.

CHAPTER 7

SECURITY INFORMATION MANAGEMENT MODEL: THE CONCEPT

7.1 INTRODUCTION

Security information collection first emerged in the mid-1950s. From then onwards the extent, complexity and detail of security information collection, analysis, interpretation and utilisation changed dramatically and developed in many different ways (Fischer et al., 2008: 39). Chapters 4 and 5 discussed these changes and developments that have taken place both nationally and internationally. This study originated due to these changes and developments taking place in the field of security information management. All stakeholders in an organisation need to be informed of these changes and developments, in order to ensure that they are aware of the importance and impact of security information in their overall work environment.

Security information management will derive the most significant benefits from security management related issues that is integrated into an organisations existing functional processes. Security information management should be seen as part of the existing functional processes of an organisation.

This chapter will discuss the security management related issues that is significant to security information management and the security information management model based on the grounded theory, as referred to in Chapter 3. The model will also encapsulate the analysis and interpretations made in Chapter 6. The proposed model will form one of the building blocks towards the further professionalisation of the security services industry.

7.2 SECURITY MANAGEMENT RELATED ISSUES

Specific security management related issues needs to be understood within its own context. An understanding of the security management related issues will avoid confusion and misunderstanding of the security organisations existing functional

processes. A discussion of the different management related issues will help understand the operational competency areas of a security environment.

7.2.1 Risk Management

Risk management was not formally used until the early 1950s. It is accepted that the modern concept of risk management originated in the United States. Technical developments in the United States confronted the insurance industry with a multiplicity of insurable risks so that insurance was purchased on an ‘all risk’ instead of a ‘specified peril’ basis. The consequence of fluctuating premiums directed the attention of top management to the cost of insurance. This gave rise to the development of risk management actions aimed at containing the cost of insurance. Risk managers were also made responsible for finding innovative ways and procedures to reduce losses which resulted in the integration of risk control and risk-financing activities. Risk management developed in South Africa in the 1970s (Valsamakis et al., 1996: 3 & 6). Since its inception Risk Management has been very popular in South Africa. It was the only risk assessment activity which was widely used to contain the costs of insurance. However, during the 1970s, 1980s and early 1990s very little emphasis was placed on the importance of security information management to reduce crime, increase detection and prevent losses.

7.2.2 Security information management

According to Kritzinger (2006: 74), security information management is a growing issue in all spheres be it industry or government and affects management positions at different authority levels, from the end user to the board level. All employees of an organisation should understand the importance of security information management and how they, as employees, are responsible for their actions in the workplace. It is important that security information is managed according to strategy, policy and standing operating procedures. Many security service providers in South Africa have information security policies to ensure ongoing information security. Information security policies are there to ensure the identification, authentication, authorisation, confidentiality, integrity and non-repudiation of information (Kritzinger, 2006: 6 & 74).

7.2.3 Security information management culture

A security information management culture is about ensuring that all employees in an organisation are made aware of their role in and responsibility for the collection and analysis of security information. In an ever-changing environment, organisations must try to create and sustain a healthy security information management culture. A security information management culture focuses on encouraging the proper planning and management of all security information issues in the organisation, especially since organisations are dependent on the data, raw information, information systems and networks. Security information management must become part of the day-to-day operations of employees. Instilling a strong security culture in a company/organisation can help to ward off threats, incidents and irregularities. If they want their organisations to survive, they have to change their culture and keep up with current security information management developments. Cultivating a security information management culture among stakeholders will ensure the safety of all assets of the organisation (Kritzinger, 2006: 78). Security awareness programmes will be essential to ensure that security objectives are met. Such a programme may be developed by an organisation that employs in-house security or one that that employs security officers.

7.2.4 Corporate governance

Corporate governance is responsibility enforced by law in countries such as South Africa and England (King, 1994: 5). Corporate governance must be taken seriously due to the fact that the accountability for corporate governance ultimately rests with a company/organisation's board and executive management levels. If the corporate governance system fails in an organisation, it will be bound to lose its competitive edge and will not be able to ensure its survival. In South Africa all companies seeking public listings need to show corporate governance of the management of risks in their companies (Shaw: 2002: 1).

There is no section in the King Report 1, 2 and 3 that covers the management of security information or information security per se (Kritzinger, 2006: 49).The board and executive management levels in organisations are still accountable for security

information management in their organisations. Security information governance involves the leadership, organisational structure, processes and technologies used for the collection and analysis of security information and the application of security risk control measures. The managers at the level of board and executive management can be taken to court if the integrity, availability or confidentiality of information is compromised in any way. It is also essential that corporate governance include information security as a vital part of governing an organisation and that the board and executive management levels should also encourage effective and responsible use of information among all stakeholders in the organisation (Kritzinger, 2006: 74-75).

7.2.5 Security information management policy/plans/strategies

Before any organisation can start to manage their security information, they should have security information management policies, plans and strategies in place as a guideline to what must be managed and how this must be managed. Top management is responsible for the formulation of these policies, plans and strategies. These security information policies/plans/strategies should relate to the collection and analysis of security information and the application of security risk control measures. Middle management has to ensure that information is collected analysed and implemented according to standard operating procedures as outlined in policy/plans and strategies (Smit & Cronje, 2002: 12).

7.3 SECURITY INFORMATION MANAGEMENT MODEL

The security information management model prepared by the researcher is schematically presented in three phases in Figures 7.1, 7.2 and 7.3.

Figure 7.1: Collection of security information (Phase 1)

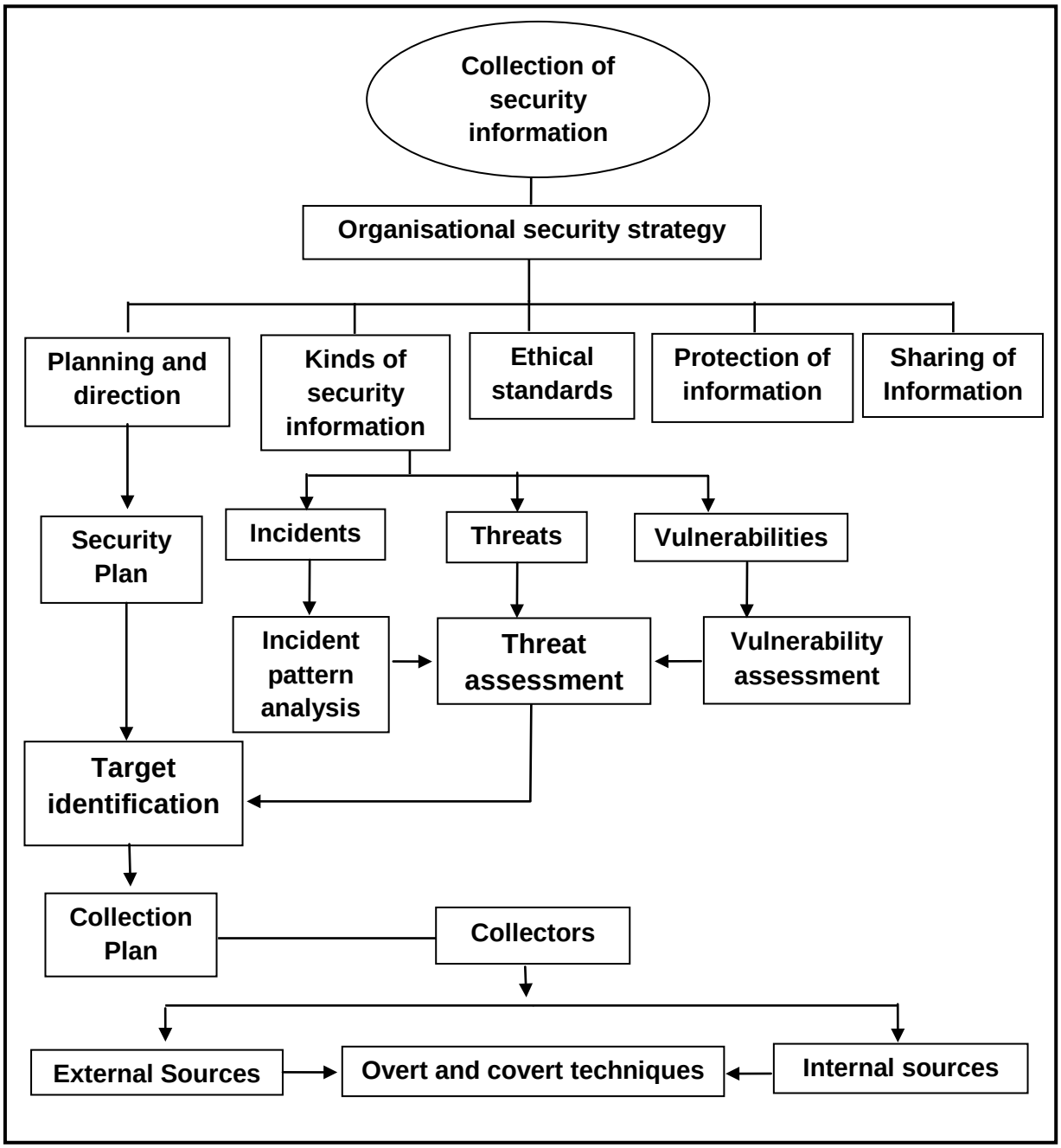


Figure 7.2: Analysis of security information (Phase 2)

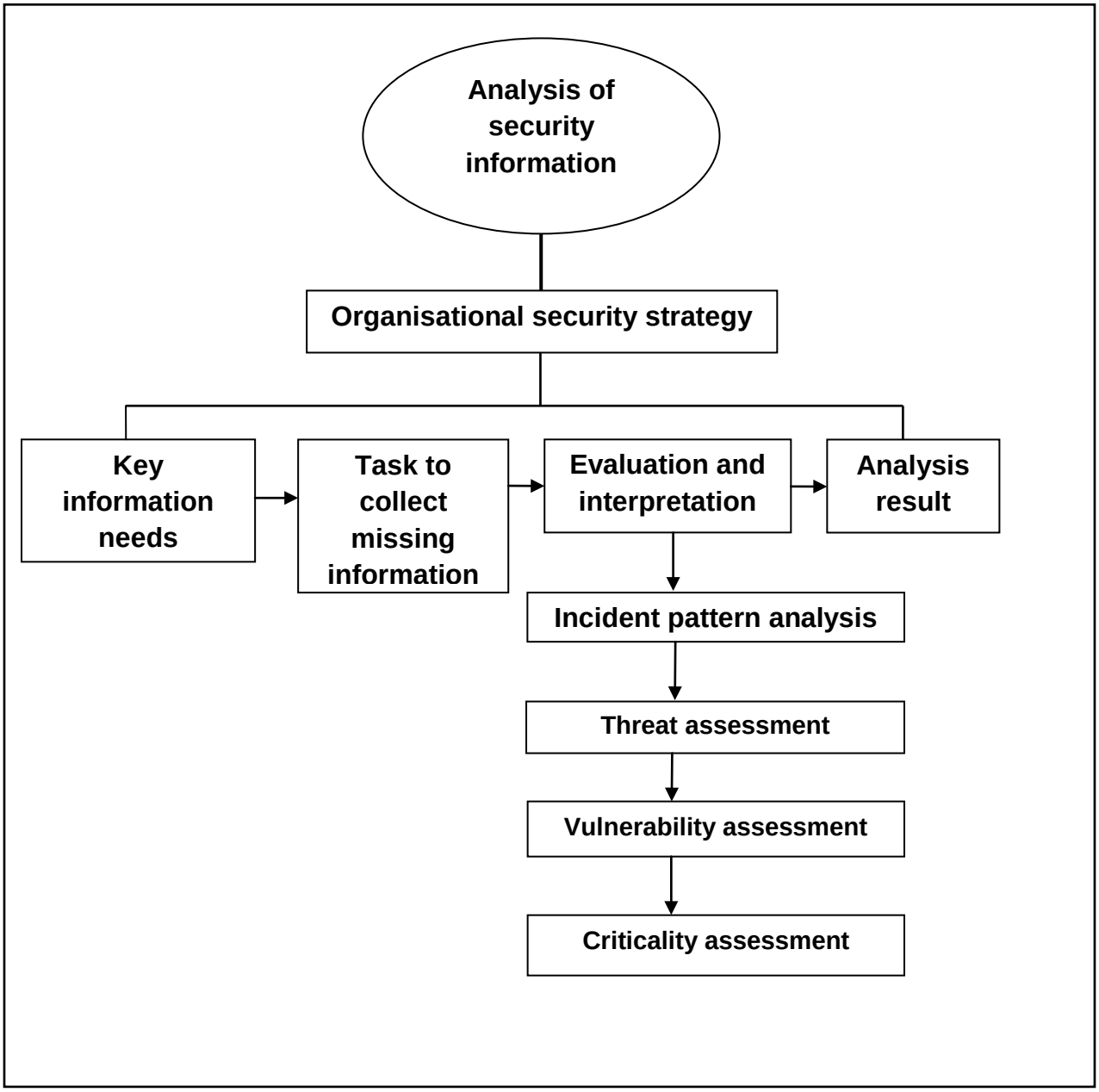
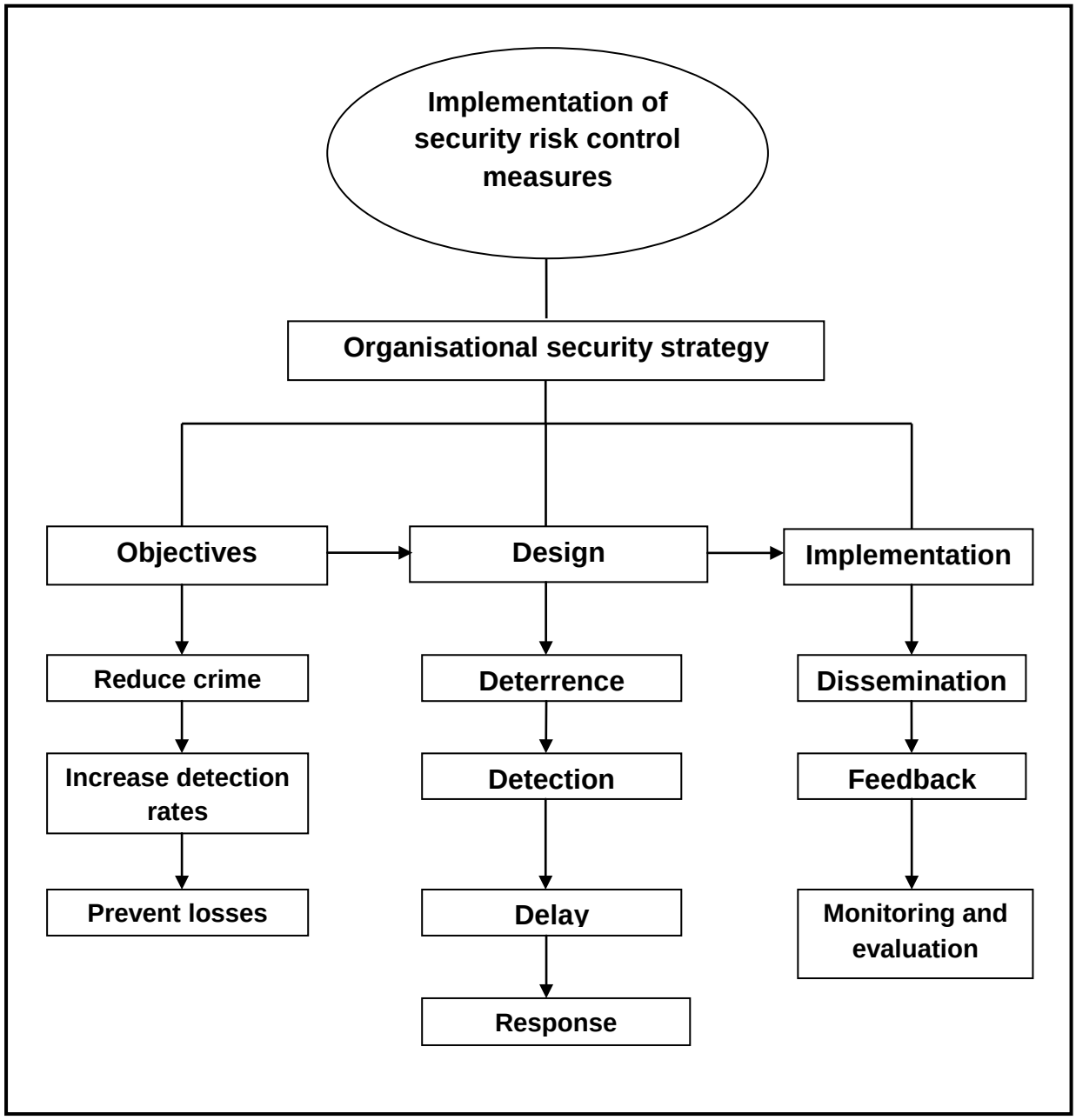


Figure 7.3: Implementation of security risk control measures (Phase 3)



7.4 EXPLANATION OF THE SECURITY INFORMATION MANAGEMENT MODEL

The substantive grounded theory on security information management which is reflected in Figure 3.4 and the findings of the self-administered questionnaire survey in Chapter 6 was used to develop the model in Paragraph 7.3 above. This model was discussed with specific security experts in South Africa. They were strongly in

favour of such a model to enhance security information management in Gauteng, South Africa. The model is explained as follows:

Security information management is spread out in three phases, namely the collection of security information phase; analysis of security information phase; and the implementation of security risk control measures phase. The collection and the analysis of the security information is handled by the Security Information Management Centre (SIMC) and referred to top management as an analysis report (result/outcome). The analysis report is handled by top management and referred to the operational manager or the human resources manager for the application of security risk control measures.

7.4.1 Phase 1: Collection of security information

7.4.1.1 Planning and/or direction

A Strategic Plan is developed by the Board of Directors and Executive Level Management. The Strategic Plan inter alia identifies the security threats affecting the organisation and its assets, as well as the organisational security strategy to address the threats. The threats are identified through the process of a SWOT analysis conducted by the Board of Directors and Executive Level Management. A security survey is initiated by the organisation to identify vulnerabilities relevant to the identified threats. An incident register is used to identify incidents related to the threats. The incident register will consist of reported incidents experienced by the organisation (Jacobs, Sheperd, & Johnson, 1998: 122-123). Planning is about collecting the right information that is needed to support top management's decision. It is about understanding the most important parts of the organisation, whether they are clients, government, technology, suppliers or competitors. The senior manager responsible for all security related matters in the organisation should develop a security plan to address the security threats using the organisational security strategy as a directive. The organisational security strategy should indicate projected costs and time frames to address specific threats affecting the organisation and its assets. These threats will be prioritised in the organisational security strategy according to importance, taking into account the cost of losses if the specific threat

has to occur. The security plan which should consist of the threats affecting the organisation, information on vulnerabilities and incident related information relevant to the threat should be used to address the prioritised threats in terms of the allocated budget. In essence, the security plan will consist of a Threat Assessment document, A Vulnerability Assessment document and an Incident Pattern Analysis document. These assessment documents should be prepared by a qualified security analyst and used as part of the security plan. The assessment documents should serve as tools to manage security risks, conduct performance management as well as impact studies on the physical protection systems. A target centred approach should be used to prioritise the threats for the collection of security information, analysis and implementation of security risk control measures (Clark, 2010: 13).

7.4.1.2 Target-centred approach

Target identification should be performed by the organisation. Targets may include critical assets or information, people, or critical areas and processes (Garcia 2008: 4) All stakeholders in an organisation, which includes senior management, collectors, analysts and operational management who are going to be involved in the implementation of the security risk control measures should be part of the target-centred approach. Here the goal is to construct a shared picture of the target, from which all stakeholders can determine what is expected of them to address the threat. They should be able determine the resources they would need to do their jobs and what they can contribute from their own resources or knowledge so as to create a more accurate target picture (Clark, 2010: 13).

Once a shared target had been identified, it is time to prepare a collection plan to focus on the threats and vulnerabilities affecting the shared target. The senior security officer should develop and manage this collection plan in accordance with project management principles. The collection plan should be developed in consultation with the security analyst. The security analyst should be able to provide guidance on the kinds of information to be collected and the key information needs to prepare specific analysis products in terms of the organisational security strategy.

7.4.1.3 Kinds of security information

Security information on threats, incidents and vulnerabilities should be lawfully collected in a structured manner within the ambit of an organisational policy framework. Standard operating procedures in line with the organisational policy framework should be developed to guide the collection of the different kinds of security information. The kinds of security information and the key information needs should be identified by the security analyst (Smit, 1989: 5; Simonsen, 1998: 202; Talbot & Jakeman, 2008: 66). All personnel from the organisation which is being protected, all security personnel, all stakeholders and clients of the organisation should be mandated to collect security information. Stakeholders and clients should be encouraged to provide security information which they intend to voluntarily share with the organisation. Such security information may be regarding their own experiences, observation or on the activities of adversaries from the inside or outside of the organisation. Stakeholders and clients may be assisted by the mass media as to the types of security information required by the organisation. This may appear in pamphlets, posters, newspapers or on television screens as alerts, notices etc.

A collection unit should be established within the Security Information Management Centre to collect security information and to service the analysts in the collection of missing information. The Security Information Management Centre should manage all the collected information and provide rapid response to security information that requires immediate action. All the collected security information should be managed by the SIMC who should have the information evaluated/verified and entered into a computerised database. All security information is collated by the analyst or a data capturer using an automated system with the relevant computer software. This includes indexing, sorting, and storage of raw information. A data base should be created for storage. Only when similar information is collected and considered together can the analyst provide meaning to the information (refer to paragraph 4.4) (Gottlieb et al., 1994: 27).

The SIMC manager may task the collection unit to obtain missing information to ensure data integrity of the collected security information. All threat information should be collated onto the Threat Assessment field, while vulnerabilities should be

collated into the Vulnerability Assessment field. The computerised system may be designed to also provide for an Incident Register to record all information on incidents. A computerised database will allow for the use of software to collate and analyse data into actionable information products. (Talbot & Jakeman, 2008: 33).

7.4.1.4 Collection process

The collection of security information is authorised by management either through job descriptions, service level agreements or a code of conduct. It is the act of gathering information on incidents, threats and vulnerabilities that may exploit the assets of an organisation and result in losses (Fischer et al., 2008: 149). Security information collection may also be outsourced to private security risk assessment companies (Fischer et al., 2008: 38). The best sources of information are people and technology. All collected security information ought to be validated, as misinformation can result in bad decision making. Hopefully, all employees in an organisation will be alerted to their responsibility of constantly reporting security information. The persons that should be approached first, from a tasking point of view, should be security personnel and those who work in the strategic areas and those that are well networked and attuned to the security information of the organisation (Muller, 2002c: 6).

There should be a code of conduct signed by all personnel in the service of the organisation which is being protected and by all security personnel. In the collection of security information the collector must respect the law and the fundamental principles of privacy (Nemeth, 2010: 87). Organisations and companies need their own set of ethical standards that should include issues such as preserving and protecting the organisation/company's credibility, value and public profile and what people may or may not do. Management should be clear about the fact that no unethical and certainly no illegal collection of information will be tolerated. When outsourcing certain aspects of security information collection, management should make sure that the contracted company knows the ethical guidelines in place in the contracting company or organisation. Transgressions by such contracted personnel will not exempt a company from liability, accountability and possible sanctions (Muller, 2002c: 20).

The protection of security information is the prerogative of each organisation and should not be undermined in any way. The security protection measures applied by government departments are coordinated by a policy framework called the MISS. Private organisations on the other hand may structure their own standing operating procedures in line with their policy framework for the protection of security information. Security managers refer to the term ‘sensitive’ when referring to information that has value and is protected. Organisations assign classifications to their ‘sensitive’ information. The names assigned to the classification levels may vary from organisation to organisation and include secret, restricted, confidential, private and personal. Sometimes top secret and highly confidential is used, depending on the type of information being classified (Fay, 2002: 289).

Personnel should be trained on how to collect security information and know what information they should collect (Muller & Whitehead, 2002: 5). Internal and external sources may be used to collect security information (Reuland, 1997: 9-10). Ferraro and Spain (2006: 97) identify methods such as physical surveillance, electronic surveillance, interviews, undercover operations, forensics, research and internal audit that can be used in collecting threat, vulnerability and incident information. The techniques that may be used to collect security information may typically include the overt information collection technique-which can be generally defined as personal interaction with people, and the covert information collection method, which is commonly defined as intelligence gathering (Lyman, 1988: 147; Matthews, 1986: 189).

7.4.1.5 Sharing of security information

The growth of information-sharing partnerships and networks and the recent development of ‘Fusion Centres’ in the United States promises a real-time information sharing and access for the future. Some security agencies uphold a ‘need-to-know’ culture of information protection rather than promoting a ‘need to share’ culture of integration (Ratcliff, 2009: 4-5). Without a proper security information management culture and attitudes that favours information sharing it is difficult to collect information in an organisation. Sharing of information goes hand in

hand with the concept of having access to information databases under the control of other stakeholders and organisations. This includes working together with the SAPS and other law enforcement agencies both nationally and internationally (Muller and Whitehead, 2002: 6). There should be a plan for the sharing of information. Funding should be available for training, infrastructure, the development of standards, and the building of trust between law enforcement and the security service providers. The United States government identified not only the technological barriers to information sharing, but, more importantly also the organisational and cultural barriers (Ratcliff, 2009: 32)**.**

Informal information sharing networks are used when formal systems prove to be too tedious. This is not encouraged due to the leakage of information (Ratcliff, 2009: 124)**.** There are no punishments or sanctions for not sharing information (Ratcliff, 2009: 5)**.** According to Clark (2010: 2), sharing requires openness. But any organisation that requires secrecy to perform its duties will struggle with and often reject openness.

7.4.2 Phase 2: Analysis of security information

7.4.2.1 Organisational Security Strategy

The security analysis function includes evaluation and interpretation of security information. It should be directed by the organisational security strategy and the key security information needs that result from changes and action in the organisational environment. An event or development in the organisation could give rise to key information needs. The routine monitoring and evaluation of an effective analysis capability regularly uncovers information that has the potential of impacting positively or negatively on strategy (Muller, 2002b: 6). The collected information should be properly organised to ensure that the right information is collected and gaps are determined. Organising the information means putting together relevant facts, developing appropriate titles and headings and then indexing the document for retrieval purposes. Factors such as chronology and geography can be used and information can also be ordered according to appropriate themes. This is important for later retrieval and checking (Muller, 2002b: 9).

An analysis function should be centralised because security information works on the principle of bringing together all relevant bits and pieces of data and information and adding meaning to it (Muller, 2002b: 2).The analysis capability should be situated at the SIMC. The development of an effective analysis capability; really, is the true justification for establishing SIMC. If correctly focussed information is not analysed and interpreted to ascertain the true impact of an event on the organisation's strategy, there would be little purpose in conducting security information management. According to Ratcliff (2009: 153-154), understanding the organisation which is being protected can go a long way in easily accepting and influencing analysis results. Three central points that analysts should recognise:

- decision-makers internal environment exerts considerable pressure;
- decision-makers demand strategies and actionable information products over descriptive reports; and that
- growth from knowledge to strategy or actionable information products is dependent on the nature of the decision-maker.

The standardised framework for the analysis of security information should provide for standing operating procedures. This should be approached in a multidisciplinary fashion. It should provide clarity on the following:

- what each person's input should be?
- deadlines;
- type of information required;
- most probable sources of information;
- time frame;
- cost estimate;
- planning for pitfalls e.g. unavailability of information; and
- framework for final report themes, titles, format (Muller, 2002b: 7).

Security information analysis is not a substitute for the analysis activities in areas such as sales, customer relations, the legal department, human resources, finance, market research, purchasing, or research and development. It would ideally add

value by the sharing and integrating of the information, and incorporating external information (Muller, 2002b: 2).

7.4.2.2 Key information needs

The collected security information should be accessed from the computer by the analyst to confirm the key information needs to provide an analysis result in line with the organisational security strategy. Analysis of security information entails evaluation and interpretation of the exact nature of the problem and the characteristics of the incidents, threats and vulnerabilities. Important factors to consider include where the incidents are occurring, at what times, who is involved, how and why the problem is occurring, and what solutions have been tried in the past. By determining the underlying causes of the problem through the collection of detailed information, more effective tactical strategies can be developed to address the threats (Block et al., 1995:3).

7.4.2.3 Task to collect missing information

Once the analyst has determined the key information needs and what information is missing or unavailable and where to find it, new tasking should be given to the collection unit or the responsible person for additional information. This new information will be used to enrich the information on hand, so that an accurate, complete analysis result may be produced (Muller, 2002b: 8).

7.4.2.4 Evaluation and interpretation of the collected security information

The evaluation phase is the true analysis phase and has three aspects i.e. assessing the information, integrating and interpreting the information. The reliability of the information source is assessed on specific criteria such as the previous quality of information supplied by the source, the situation, the location, and likely access of the source at the time to the information collected. The accuracy of the information provided is assessed as an actual relative measurement in relation to each item of information received (Talbot & Jakeman, 2008:142). Although the reliability of the source needs to be assessed, the credibility of the information is also important and

should not be neglected. The more primary information is used, the higher the importance of testing because of the subjective nature of human sources and the danger of mistaking misinformation and disinformation for fact. The information as well as where it was sourced, should also be tested for credibility and usability (refer to paragraph 4.4) (Muller, 2002 b: 8-10).

According to Gottlieb et al. (1994: 161), the interpretation of information is the true analysis function. It requires highly skilled and experienced security information analysts. These skills should include a variety of crime analysis tools, threat analysis tools, vulnerability analysis tools and criticality assessment tools. Incident pattern analysis will consist of incident patterns of both crime incidents and policy violation incidents. Since no literature could be found on incident pattern analysis of policy violations in the security environment, the researcher decided on using the crime pattern analysis process employed by policing agencies. Crime pattern analysis contains information relative to continuing occurrence of particular criminal activities. They acquaint officers with the types of crimes being committed; list the days, times and locations of their occurrence; and provide officers with any known suspects, suspect vehicle, modus operandi, and or property loss information.

Threats become more serious when vulnerabilities exist that can be exploited. There will always be potential threats in any protected environment. The threat should be assessed to ascertain the intent, capabilities and motive as this would impact on the security risk control measures that would be devised and implemented. Therefore, being able to counter an actor's threat means knowing the actors capabilities. For example;

- how effective is their intelligence capability?
- what measures would they employ?
- do they adhere to strict guidelines in terms of gathering information?
- do they have a history of using non-conventional methods, e.g. bugging? and
- how determined are they or how desperate are they?

In identifying possible threat actors one must not forget vendors, suppliers, customers, distributors, consultants and other indirect employees or associates. Do you really know them and their interests? What is it that they really know about the

protected company's operations, plans, strategies, capabilities and weaknesses? How do they handle information of importance against the protected company (refer to Paragraph 4.4.3) (Muller, 2002a: 9).

All organisations/companies have areas of vulnerability and the bigger the vulnerability the more severe the threat. It is therefore important to assess the vulnerabilities. Potential vulnerabilities often include the following:

- a lack of defensive awareness amongst employees;
- unmaintained physical security protection systems;
- deliberate harmful actions by a disgruntled employee; or
- communication via telephones, facsimiles and even e-mail and the internet.

Information and other service vendors, consultants and service providers can also pose a threat. Weak links are usually people and the way they communicate with others. People's talkative habit may sometimes make them spill the beans. This step requires knowing the rivals' capabilities and expected actions. How would it go about "attacking" your vulnerabilities? Requirements for such an assessment are typically a record of dubious, often inexplicable incidents, e.g. stolen computers, break-ins, hacking incidents. Recognising vulnerabilities also means that companies are aware of potential loopholes and can in time take alternative measures to protect interests. It is about taking preventive measures to limit a potential threat (refer to Paragraph 4.4.4) (Muller, 2002a: 9-10).

In Criticality Assessment the essential question is: How likely is it that a particular threat event will take place or the probability of a threat event occurring. Has the product been a target before? What is the current situation regarding the threat. Was it previously attacked, if so how frequently? The security manager must take into consideration the costs of replacement, repair, lost productivity, forfeiture of business opportunity, cleanup, litigation, damage to reputation and undermining of customer goodwill. Even when the impact is upon human life, the yardstick is in Rand value (Fischer et al., 2008: 157).

7.4.2.5 Analysis result

Analysing the information needed by clients can also pose problems, especially in terms of needs, the level of training of the analyst and the technical support in terms of the operating systems, hardware and software. The skills required may be considerably different for which they were initially employed (Block et al., 1995: 161).

'Relationship management' is not a term that many analysts are probably familiar with, but perhaps they should be. Managing the relationship between the analysts and the end user of the results – the client – is essential if the knowledge possessed by the analyst is to be converted into actionable results. The need to manage this analyst –client relationship is the most vital skill that analysts should possess. "Relationship management" will help to overcome mistrust and misunderstanding between analyst, management and the end user (Ratcliffe, 2009: 98).

Clarke and Eck (2003: 1) are of the view that personnel appointed as analysts should be able to provide the kind of strategies, actionable information products and recommendations on physical protection systems needed to support the end user.

There are a range of analytical techniques that can be used by analysts. Some of the analytical techniques include the following:

1. Crime pattern analysis: provides trends and hotspot analysis.
2. Network analysis: provides an understanding of the direction, frequency and strength of links between criminal collaborators in a criminal network.
3. Market profiles: assessment of the market for a specific commodity e.g. physical protection system.
4. Demographic/social trend analysis: an assessment of the impact of socio-economic and demographic changes on criminality.
5. Criminal business profiles: determine and understand the business models and techniques used by organised crime groups.
6. Target profile analysis: provides an understanding of the lifestyles, networks, criminal activities, and potential interdiction points in the life of a targeted offender.

7. Operational intelligence assessment: evaluation of information collection to inform decision-making about an existing operation.
8. Risk analysis: assesses the scale of risks or threats posed by offenders or organisations to individual potential victims, police and the public.
9. Results analysis: a process used to evaluate the effectiveness of law enforcement activities (Ratcliffe, 2009: 135).

7.4.2.6 Analysis report (result)

Once the evaluation and interpretation have been completed and having determined how the analysis results should best be presented to management, the analysis results now need to be packaged. The analysis result should only consist of the answer to the original question and should not include comprehensive reports in which the answer is indiscernible. An effective analysis report should contain the following:

- a clear, concise and objective message that is responsive to the original key information need;
- be timely and in appropriate format;
- contain varying predictions indicating most probable outcome;
- propose various proactive or counter-strategies;
- indicate information gaps and the effect thereof;
- comment on the credibility of information and reliability of sources;
- use persuasive presentation skills (Muller, 2002b: 14-15).

7.4.3 Phase 3: Implementation of security risk control measures

Upon receipt of the analysis report top management may decide on the application thereof. They may use the analysis result to design appropriate security risk control measures that would deter, detect, delay and respond to an intruder or institute a disciplinary enquiry, civil/criminal prosecution. Management may want to make personnel aware of specific activities. They may use it as deterrence or to authorise further collection of security information using physical surveillance or other forms of non conventional methods. Ultimately, they may want to address the organisational security strategy by the implementation of security risk control measures in the form

of physical protection systems (PPS), strategies and actionable crime information products (Garcia, 2008: 6).

7.4.3.1 Objectives

No company can protect everything all the time. This would be unrealistic, impossible and unnecessary. We need to recognise that most organisations already have security measures in place e.g. access control, firewalls etc. There is no need to double these efforts. Although there is limited linkage between an organisation's Strategic plan and security functions, security risk control measures are often made the responsibility of security personnel. Once the vulnerable assets have been identified those crucial elements in the assets should then be identified in order to design appropriate security risk control measures (Muller, 2002a: 5).

To formulate these objectives, the designer must understand the organisational operations and conditions, define the threat and identify the target. The ultimate objective of a security plan should be to reduce crime, increase detection and prevent losses. Typical objectives will be to prevent sabotage of critical equipment, theft of assets or information from within the facility, and protection of people. The envisaged security risk control measures must be able to accomplish its objectives by either deterrence or a combination of detection, delay, and response (Garcia, 2006: 8-23).

According to Garcia (2008: 3), a proper description of the facility will provide an understanding of the PPS requirements for the facility as well as an appreciation for the operational and safety constraints. A thorough description of the facility and the processes within the facility is an absolute necessity. This information can be obtained from different sources, including the facility design blueprints, process descriptions, safety analysis reports and environmental impact statements. An orientation of the organisation and interviews with personnel is crucial.

Adversaries can be separated into three classes: outsiders, insiders and outsiders who are working in collusion with insiders. For each class of adversary, the full range of tactics (deceit, force, stealth, or any combination of these) should be considered.

Deceit is the overriding of a security system by using fraudulent authorisation and identification; force is the overt, forcible attempt to overcome a security system; and stealth is any attempt to defeat the detection system and enter the facility covertly (Garcia, 2008: 4). Security information management is about ensuring the identification, authentication, authorisation, confidentiality, integrity and non-repudiation of information (Kritzinger, 2006: 74).

7.4.3.2 Design

Using the objectives for security risk control measures obtained in the organisation characterisation, threat definition and target identification, the specialist can design security risk control measures. The security risk control measure design must be able to detect and detain (arrest) the adversary, prevent the criminal conduct or irregularity of the adversary from occurring and create awareness to prevent losses (Garcia, 2008: 4).

According to Garcia (2008: 5), in designing a specific physical protection system to avert the threat identified in the analysis's report, management must ensure that the new physical protection system will detect the adversary, delay the adversary, and alert the response force to interrupt the adversary.

Security risk control measures may be designed to include strategies encompassing Crime Prevention Through Environmental Designing (CPTED), business watch, car guard watch, neighbourhood watch, awareness, sharing of information, electronic networking with other service providers and organisations. Many of these have served as best practices in the law enforcement environment. The challenge is for security managers to make themselves aware of current and innovative design strategies. This knowledge should be coupled with the latest information on issues of changes in cultural values, crime, technology, market conditions, and political conditions (Opolot, 1999: 229).

7.4.3.3 Dissemination

Dissemination can be carried out in several different ways, namely, by attending briefings and strategy sessions, presenting verbal reports, providing written reports, having face-to-face contact whenever the need arises and public information systems – written and electronic media (Reuland, 1997: 35). To ensure that a paper trail exists, dissemination should take place in a regulated written format.

7.4.3.4 Implementation

The recommended security risk control measure is received from management by the end user for implementation. The security risk control measure may take the form of strategies, physical protection systems or actionable information products. There should be open communication between the management, the analyst and the end user. This is important, especially where the end user needs to discuss a new trend or some additional design elements with the analyst or management regarding the specific threat (Garcia, 2008: 64-65).

7.4.3.5 Feedback

The last aspect after the implementation of the security risk control measure is feedback and reaction. Management and the analyst need to know what works and what does not work. Feedback may be given verbally or in written format. A survey form may be used to obtain feedback and reaction of the analysis result (Reuland, 1997: 36-37).

7.4.3.6 Monitoring and evaluation

Once the security risk control measures have been implemented they must be periodically evaluated to determine the effectiveness or lack thereof (Rogers, 2008: 163). There are two main types of evaluations. They are outcomes and process evaluations. An outcome evaluation is to determine if the security risk control measure had the desired effect, such as, ‘was crime reduced?’ or ‘was an intruder disrupted?’ (Ratcliffe, 2008: 189). Monitoring and evaluation should be carried out by

line management. It has to begin with a review and thorough understanding the of the protection objectives the designed security risk control measure must meet. The PPS should be quantitatively and qualitatively monitored and evaluated for vulnerabilities on a continuous basis (Garcia, 2008: 5).

7.5 CONCLUSION

Security information management is a fundamental part of security management. This concept needs proper planning, organising, leadership, co-ordination and control to be successful. The concept ensures that policy follows strategy. Standing operating procedures have proven to be working well in security information management companies such as SABRIC, CGRI and the PSI. It is suggested that standard operating procedures should follow policy, so that the security information management model may be implemented by all security service providers. This security information management model should be seen as a concept separate from security risk management which was introduced to prevent losses so that insurance premiums may be reduced. The Security Information Management Model should be seen as a concept to reduce crime, increase detection and reduce losses. The model was developed using reliable information obtained in the literature study, case studies and interviews. If security information management is researched by another researcher he/she will also be able to produce a similar model. Due to sensitivity of some of the information being managed in the security environment, there was some reluctance to discuss some of the techniques used in practice to gather security information for example in undercover operations. This had to be cleared with security managers, before this information could be shared with the researcher.

CHAPTER 8

FINDINGS AND RECOMMENDATIONS

8.1 INTRODUCTION

The security industry operates within a diverse and multi-disciplinary knowledge base, with security risk management being a fundamental knowledge domain within security. Over the past decade, the concept of security risk management as a formal discipline has emerged throughout the private and government sectors of security. Security risk management is now a well-established discipline, with its own body of knowledge. The standards and compliance requirements for security risk management only considers security risk management and not security information management. In security risk management, security risk assessment is carried out to identify areas that need security intervention. The security risk management framework currently used by the security industry provides for the collection of information on vulnerabilities and incidents, whenever the need arises. This does not include the day to day collection of security information on threats, vulnerabilities and incidents for the purpose of reducing crime, increasing detection rates and preventing losses. In the absence of a security information management framework for the security industry, this research was focussed on developing an effective model for the management of security information. The security information management model will among other things, provide for incident pattern analysis, threat assessment, vulnerability assessment and criticality assessment.

This study used the mixed methods research approach to obtain scientific knowledge and insight for the development of a model for the management of security information in the security industry. This chapter concludes with findings and recommendations made in this study. It also highlights limitations in the model and future research work that could further enhance this study.

8.2 RESEARCH OVERVIEW

The security industry comprises of private and government security service providers. They are divided into different sectors according to the security service function they perform. Each sector has a specific goal and emphasis in respect of security related functions.

The substantive grounded theory which was developed in this research describes how security information is managed in the Security Industry. The substantive grounded theory also forecasts that if security information is not correctly managed, there will be continuous recurrence of losses. Strauss and Corbin (1990: 5), are of the opinion that the grounded theory should explain, describe and to a certain extent be able to predict. The substantive grounded theory in this research was developed by obtaining qualitative data through focussed semi-structured interviews and focus group interviews. The primary data was obtained directly from the participants. The collected data was manually coded and categorised by the researcher. A continuous theoretical discussion, supported by the codification of categories and themes with emphasis on the theory as a process was used. It was not difficult for the researcher to develop a 'story line' which started with the collection of security information, the analysis and ended with the implementation of security risk control measures.

Selective coding resulted in the following conclusion: the core category that emerged after coding was the security officials' 'management of security information'. The category was developed in the same way as all the other categories and a substantive grounded theory emerged (De Vos, 2007: 345). The theory is that security officers operate without a standardised framework to manage security information.

A self-administered questionnaire survey was conducted with security officials from different sectors of the security industry in Gauteng. The data was quantitatively analysed by a statistician and interpreted by the researcher. The grounded theory was verified using the analysed data from the questionnaires (Strauss and Corbin (1990: 23). It was found that there was a need for a security information

management model for the management of security information in the security industry.

The aim of this study was to explore the management of security information in the security industry in Gauteng. The outcome resulted in the development of a Security Information Management Model for the security industry. The research rationale, research problem, research questions, research goal, research objectives and the case study were evaluated with the view to making findings and recommendations.

8.3 RESEARCH FINDINGS

8.3.1 Findings related to the research rationale

The research rationale in Chapter 1 suggests that security information is not being managed in the same way as security risk management and the management of crime information and intelligence.

Awareness on the importance of security information: It has been found that in the Western Australian (WA) casino industry, the collection of security information is everyone's responsibility. An information awareness culture is created by the distribution of pamphlets, holding awareness workshops and using a common code of conduct for all employees at the Casino. LCD television screens are also used to encourage the general public to provide information to specific control points (Interview no 23).

Collection of security information: It has been found that in law enforcement both in South Africa and Western Australia, intelligence and crime information is collected using crime information/intelligence collection units. They have their own collection capacity within the crime information/intelligence units. Intelligence is collected when a specific need arises as directed by management. On the other hand, crime information is collected according to a specific crime problem as directed by crime analysts. A collection plan is used to collect crime-specific elements that distinguish both one criminal incident from another and one group of offences, related in one or more ways, from a larger group of similar offences. The collection units collect crime

information/intelligence using different sources, methods and techniques. Security risk management requires the use of a security survey instrument to identify risks confronting assets in a facility. The security industry collects security information on incidents of crime and policy violations as they occur. Very seldom do security service providers use different sources, methods and techniques to collect security information.

Sharing of security information: It has been found that the Constitution of the Republic of South Africa provides for Community Police Forums (CPFs) and the National Intelligence Coordinating Committee (NICOC) to share crime information and intelligence. According to the National Strategic Intelligence Act, No. 39 of 1994, private security service providers shall provide crime information/intelligence in support of the SAPS' policing function in terms of section 205 (3) of the Constitution. Poor working relationships and mistrust among security personnel and between law enforcement and security service providers hinders the sharing of security information.

Workplace investigations: It has been found that in two High Court cases (of the Witwatersrand and Natal divisions) the Judges expressed their acceptance that workplace investigations can occur (see *State vs Botha and others (1) 1995 (2) SACR 598 (W);* and *State vs Dube 2000 (1) SACR 53 (N)*). The court referred to the fact that various institutions conduct their own investigations and then hand the evidence over to the police for further action and possible criminal prosecution. This development has created new opportunities for all investigators whether in private, business (corporate) or government service. All indications are that the scope will increase. The Private Security Industry Regulatory Act, No. 56 of 2001 provides for the functions of an investigator in the security service. Workplace investigations include the collection of information in search for evidence of a crime or irregularity. Information collected during workplace investigations may give rise to security information which may enlighten management on the extent of incidents, vulnerabilities and threats against the organisation/company being protected.

Analysis of security information: It has been found that the change from manual analysis to automated analysis is important. It supplements the expertise of an

experienced official. It is also because the knowledge and techniques accumulated over the years do not retire with a veteran official. They are there for others to build on. Automated analysis helps to obtain an accurate picture of a problem. It enables practitioners to know the exact nature of the problem and the characteristics of the incidents. It helps to determine the underlying causes of the problem and to develop effective strategies, measures and actionable crime information products. According to Gottlieb et al. (1994: 27), there are four types of analysis most often used by law enforcement analysts. They include crime analysis, intelligence analysis, operations analysis and investigative analysis. Crime information analysis plays a significant role in producing intelligence through the systematic collection, evaluation, analysis, integration, and dissemination of information on criminals, especially related to their associations and their identification with criminal activity of an organised nature. The use of accurate analysis results to reduce crime, increase detection rates and prevent losses is not unique to modern times.

Development of a Security Information Management Model: It has been found that most police practitioners from law enforcement used the traditional problem oriented policing model to manage crime information in their environments. This involved scanning, analysis, response and assessment (SARA). The stages in the SARA model include the following:

- **scanning:** identifying recurring problems and how the ensuing consequences affect community safety;
- **analysis:** collecting and analysing relevant data on the problem, with the object of revealing ways to alter the causes of the problem;
- **response:** seeking out responses that might have worked elsewhere, identifying a range of local options, and then selecting and implementing specific activities that will resolve the problem;
- **assessment:** testing data collected before and after the response phase in order to determine whether the response reduced the problem and, if not, to identify new strategies that might work (Ratcliffe 2003: 74).

An advancement to the traditional problem oriented policing model of crime information management is ‘Intelligence-led policing’ (also known as ‘intelligence-driven policing’) model, which had its origins in the United Kingdom (UK) in the

1990s.The UK, National Intelligence Model (NIM) used four elements for its tactical tasking in the implementation of intelligence-led policing. These elements focus on:

- targeting offenders (especially targeting of active criminals through overt and covert means)
- management of crime and disorder hotspots;
- investigation of linked series of crimes and incidents; and
- application of preventative measures, including working with local partnerships to reduce crime and disorder.

The production of intelligence in intelligence-led policing has different stages: this includes **direction to collect intelligence**, **evaluation, collation, analysis, dissemination and feedback** (NCIS, 2000: 14).

Security Risk Management Cycle (SRMC) is commonly used by security service providers in Australia. This cycle begins with the security risk manager identifying the assets to be protected. The risks associated with the asset are prioritised. It is followed by the analysis of the effects of the risks according to probability, impact and frequency. This results in the identification of alternative actions to reduce the risks (Clark 2010: 260).

During the period 1995-1997, the Programme Group: Security Management at the Technikon South Africa (TSA)[8] developed a Security Risk Management Model (SRMM) for their National Diploma in Security Management and for the newly instituted (1999) BTech in Security Risk Management. This model is based on the following steps:

- identification of the problem of security (crime risks);
- studying the policy of the organisation and obtaining a mandate;
- conducting an orientation exercise;
- undertaking a risk analysis exercise;
- conducting a security survey;

[8] In January 2004 the TSA merged with the University of South Africa (UNISA) and the Programme Group became the Department of Security Risk Management which in January 2009 merged with Criminology to become The Department of Criminology & Security Science.

- doing a return on investment exercise to implement security risk control measures; and
- submitting a crime risk management report to top management of the company for a decision on the implementation of security measures (Rogers, 2008: 151-154).

The SRMM was further adapted to the residential security environment with an additional step namely ‘maintenance and upgrade’ (Olckers, 2007: 103). Kole (2010: 20) further adapted the SRMM with the addition of another step, namely ‘service level agreements’ which emanated from his masters research study on the protection of petrol stations.

Security risks are identified using the SRMM if the need arises or if the financial situation warrants such an exercise (Kole, 2010:16). The SRMM is only implemented by security service providers on approval by management (Rogers, 2008: 151-154).

At agency level crime information in the law enforcement sphere is collected, analysed and implemented in a logical and structured manner to produce different types of analysis products such as crime analysis, intelligence analysis, operations analysis and investigative analysis (Newburn et al., 2008: 204; Reuland, 1997: 7).

The modern day crime information management strategy commonly used by law enforcement is the Compstat model which originated in New York City, USA during 1994. It involves four principle stages, namely:

- Collection of timely and accurate information,
- Effective tactics,
- Rapid deployment,
- Relentless follow-up and assessment

(Ratcliffe, 2003: 76).

Presently, there is no Security Information Management Model (SIMM) for the security industry.

8.3.2 Findings related to the problem statement

An issue of concern that needed to be addressed in this study was the collection, and analysis of security information and the implementation of security risk control measures in the security industry.

The "*status quo"* of the collection and analysis of security information and the implementation of security risk control measures was established. The nature and extent of problems experienced in the collection and analysis of security information and the implementation of security risk control measures were identified. Solutions to to address the problems experienced in the collection and analysis of security information and the implementation of security risk control measures was determined.

8.3.3 Findings related to the research questions

The first question was to establish, the "*status quo"* of the collection and analysis of security information and the implementation of security risk control measures in practice. By means of this question, the researcher intended to establish the current situation of security information management in the security industry.

The second question was to identify, the nature and extent of problems experienced in the collection and analysis of security information and the implementation of security risk control measures. By means of this question, the researcher intended to identify the nature and extent of the problems being experienced in the collection and analysis of security information and the implementation of security risk control measures by security officials.

The third question was to determine solutions to address the problems experienced in the collection and analysis of security information and the implementation of security risk control measures. By means of this question, the researcher intended to find solutions to address the problems experienced in the collection and analysis of security information and the implementation of security risk control measures

The following findings are based on the responses received from the respondents in the semi-structured interviews, focus group interviews, and the self-administered questionnaire survey. The research findings were evaluated in relation to the research questions of this study.

Research question 1: What is the "*status quo"* of the collection and analysis of security information and the implementation of security risk control measures in practice?

Collection of security information: It was found that security information is collected whenever an incident takes place, for example an act of crime or a policy violation using specific personnel and electronic technology. The most common sources from which security information is collected include information from a victim/complainant and witnesses. Voluntary information is sometimes received from a third party on specific incidents, threats and vulnerabilities. Security information received by security officials is recorded in their pocket books and entered into a register (occurrence book) at the control room. It is also reported to the shift supervisor on duty.

In some organisations/companies security information is not openly recorded in a register due to mistrust among security officials. Each security service provider applies his/her own method of protecting security information. Security service providers implement different ways to protect security information. Some government departments use the Minimum Information Security Standards (MISS) document for the classification and protection of security information. Sharing of security information is done on a need to know basis, because of business interests and fear for the leakage of information. Security information collected during workplace investigations is not stored in data base for future use.

Analysis of security information: It was found that many security service providers use clerks and investigators as data capturers to carry out the basic analysis functions such as the capturing and verifying of data. The collected security information is considered by security managers and not analysed by qualified analysts. Security managers make a decision on security information which can be

used by SAPS and security officials for operational purposes. Some organisations/companies in South Africa use private security information management companies (SABRIC, PSI, CGRI) to analyse the incident information. In some instances the quality of the collected security information is also questionable. Sometimes a follow up is needed to collect missing information. This is not possible in the absence of a collection unit and an analysis capability.

Many organisations/companies do not make use of computer technology, computer hardware and software for the purpose of analysis. The automated analysis function is only used by some of the big organisations/companies who have qualified analysts in their employ. Only in exceptional and sensational incidents will security information be out-sourced to qualified analysts for analysis reports. Many organisations/companies have found this to be more beneficial and cost effective than investing on an in-house analysis capability.

Implementation of security risk control measures: It was found that in some organisations/companies the collected security information is handled by security management without the support of qualified analysts. The security information on incidents of crime is handed to SAPS, and the incident information on policy violations is given to security officials for internal investigation. Threat information which is seldom received is also given to the SAPS for investigation. Security management also provides actionable crime information products and tactical strategies to proactively address specific threats to security officials on static and mobile duty. Security information on vulnerabilities is addressed when a security risk assessment is conducted on the organisation/company being protected.

The implementation of specific security risk control measures by security service providers are quantitatively driven in terms of cost. The qualitative designing of the security risk control measure to deter, detect, delay and respond to the intruder is not taken into consideration. If funding is not forthcoming from the organisation/company being protected, then the security information to enhance the the security measures is either shelved or a more cost-effective measure is implemented.

Security information management companies, who manage security information on incidents of crime for organisations/companies, generate actionable crime information products and tactical strategies for implementation by the respective organisations/companies being protected. Verbal and written communication methods are sometimes used to give feedback. Feedback is given as determined by individual end users of the security information.

Research question 2: What is the nature and extent of problems experienced in the collection and analysis of security information and the implementation of security risk control measures?

Collection of security information: It was found that security officials collect security information without considering the strategic plan, operational security strategy, security plan or a collection plan of the organisation/company being protected. Personnel, budget and other resources are not specifically linked to the collection of security information. No specific effort is made to collect security information on specific matters within a specific context to address a specific threat.
Security officials collect many different types of information with no goal or objectives in mind. They do not have a description of the security information they need to collect. The collected security information does not add value to the core business of the organisation/company because it is collected without any policy direction. This results in information overload. No communication between the client and the collector of the security information. Funding, human resources and technology is wasted on collecting security information which is not a need for the organisation/company.

There is an absence of awareness on the importance of security information in reducing crime, increasing detection rates and preventing losses. Security officials, clients and the public are not made aware of their ethical obligations to report security information on incidents, threats and vulnerabilities to the organisation/company. Security desks and toll free numbers are not used for reporting security information. The mass media is also not used to encourage the public to provide security information on the organisation/company being protected. Security officers collect security information on threats and vulnerabilities when a

situation presents itself. Threats and vulnerabilities are not a priority for the collection of security information on a daily basis. Personnel do not have a responsibility in terms of a job description, service level agreement or a collection plan to collect security information relevant to specific threats.

Very little use is made of sources, methods and techniques for collecting security information (e.g. mass media and undercover contracted operatives). External sources are also neglected. Fear of victimisation is seen as the biggest intimidating factor in the collection of security information. Personnel are reluctant to provide information due to intimidation and fear of being labelled as an *'impimpi'* (derogatory Zulu term for informer or 'sell-out' from the pre-1994 era of political contestation in the townships). Security service providers do not use a standardised operational procedure for the protection of information. Security information received for analysis is sometimes not protected to prevent leakage of information.

Security information is not always stored and maintained on a computer database. In many instances security information is manually recorded in registers. These registers are kept in the storage rooms. At smaller companies security information is not recorded but retained in the memory of investigators and security officers rather than data systems. Investigators possess a wealth of information. Computer access is not given to all security personnel to input security information personally collected by them.

In some organisations/companies security officials working at lower levels are not trusted with information, neither are they tasked to collect security information for the purpose of investigations. There is mistrust between management and lower level security personnel. Management suspects that many of the lower level security officers work with criminal elements. There is a perception that they may sell the collected security information to criminal elements.

Legal restrictions on the collection of intelligence are an impediment for private security service providers. They are unable to collect intelligence on threats and incidents of crime. Even if intelligence comes to their attention, they need to refer the intelligence to SAPS or to the National Intelligence Coordination Committee for

attention by legally mandated intelligence agencies. The collection of security information sometimes infringes on the rights of people. The handling of the collected security information is not standardised and streamlined which results in information overload. Security information is shared on a need to know basis. Not all information is made available to law enforcement; neither does law enforcement make information readily available to security service providers.

In most instances, security officials have insufficient knowledge on the collection of security information. Many security officials do not have skills to identify security related information. Some of the security officials are unable to record information or statements as a result of poor communication and writing skills. Training is not given to security officials on the use of the different collection sources, methods and techniques.

Analysis of security information: It was found that many organisations/companies do not have an analysis capability or qualified analysts in their employ; neither do they out-source the analysis function. Security information received by these organisations/companies is not evaluated/verified and interpreted. In many instances, no indexing, sorting and storage of collected security information takes place. Many security service providers do not have computer technology and specific computer software for analysis.

Certain organisations/companies which have an analysis capability sometimes have problems with the integrity of their information. In many instances the information is insufficient, unreliable and inaccurate. The security information is not tested to determine if it meets the key information needs of the analyst. Analysts experience problems in obtaining missing information in the absence of a collection capacity. In most cases the analysis results are not directed at addressing specific threats or vulnerabilities. The threat assessment, vulnerability assessment and the incident pattern analysis of the organisation/company are not considered in the analysis process. In many instances actionable information products are often found not to be relevant, reliable or timely. Management sometimes undermines and generalises the analysis results before it is disseminated. No ongoing communication between analyst and user of analysis results. Dissemination of analysis results not being done

by analysts. Analysis results takes too long. In many instances the analysis results are not relevant to the security risk prevalent at the time. Management does not do much to manage data integrity and quality control of the analysis result before it is passed onto the end users for implementation.

Implementation of security risk control measures: It was found that there is no policy framework for the implementation of security risk control measures. Security risk control measures take the form of prevention measures (more body and property searches during access control), disciplinary action and criminal prosecution. Very seldom do they take the form of physical protection systems, strategies and actionable crime information products. Security risk control measures are implemented without giving due consideration to the reduction of crime; increase in detection rates and the prevention of losses. The implementation of security risk control measures is not needs driven. Clients are unwilling to pay for additional resources to implement security risk control measures which is not needs driven.

In many instances there is no communication between the analyst and the security official responsible for the implementation of the security risk control measures. The intended users are not always in a position to operationalise the security risk control measures, as the measures are sometimes outdated. If the services of a qualified analyst is used the results and recommendations are in some instances undermined and generalised by management, to down play the seriousness of the threat or vulnerability. Many of the personnel are inexperienced to implement security risk control measures. No training is provided for the implementation of security measures. In many instances the resources are insufficient to implement analysis results.

Feedback is seldom given to management. Much the feedback is given informally to management on the progress of implementation. The implementation of the security measures is not monitored and evaluated by line management**.** There is no evaluation on the implementation of the security risk control measures.

Research question 3: Which solutions should be implemented to address the problems experienced in the collection and analysis of security information and the implementation of security risk control measures?

Collection of security information: Policies are needed to guide the collection of security information in the security industry. Management should provide the required human, physical and financial resources for the collection of security information. Collection of security information should be included in service level agreements and job descriptions. Security officials should be trained in the collection of security information. Communication skills of security personnel to be enhanced. Security personnel to be made aware of all technological advancement for the collection of security information. Computer technology and computer software programmes should be provided to personnel. Computer access should be given to all security personnel. The correct persons to be employed for the job.

Personnel to be made aware of the importance of security information. They should be motivated to collect the required security information. Security information to be protected through classification. Information sources to be protected. Payment of incentives for information should be encouraged. Proper rewarding of informers is essential. All collected information should be placed on a database.Sharing of information to be encouraged. There should be a closer working relationship with the South African Police Service (SAPS) and National Prosecuting Authority (NPA). Improve networking with service providers. Accessibility to external databases to be negotiated. Security personnel should be trusted in the collection of security information.

Analysis of security information: Qualified, experienced personnel to be used to do analysis. Management should not undermine analysis results. There should not be mistrust between management and lower level security personnel. Analysis results should not be generalised by management. Management should not interfere with the analysis function. Security information to be analysed in a structured way. Regular communication should take place between analyst and end user of the analysis result. The end user of the analysis result should be allowed to request additional analysis on the result. Data integrity of analysis results should not be

compromised. Establish a data analysis centre to monitor incidents. Dissemination should also take place formally by means of reports.

Implementataion of security risk control measures: There should be a separate unit for the implementation of the security risk control measures. Security risk control measures should include strategies to mitigate risks. There is a need to have a structured way of implementing security risk control measures. Implementation of analysis results should be cost effective. Experienced security personnel should be used in the implementation of security risk control measures. Project management approach to be followed in the implementation of security risk control measures.

8.3.4 Findings related to the research goal

The research goal was based on the need to explore the management of security information in the security industry.

The exploratory study of the management of security information in the security industry was successfully conducted in the Gauteng province of South Africa and Perth in Western Australia.

8.3.5 Findings related to the research objectives

The first objective was to establish the "*status quo"* of the collection and analysis of security information and the implementation of security risk control measures in practice.

The second objective was to identify the nature and extent of problems experienced in the collection and analysis of security information and the implementation of security risk control measures.

The third objective was to discover a new Security Information Management Model (SIMM).

Objective no. 1: It was found that the collection and analysis of security information and the implementation of security risk control measures takes place without any strategic direction and infrastructure in place. No standardised framework is used to manage security information in the security industry.

Objective no. 2: It was found that management does not provide an organisational security strategy, security plan or collection plans for the collection of security information. In most cases no analysis capability exists in organisations/companies. The implementation of security risk control measures is not designed to meet the strategic objectives of the organisation/company being protected.

Objective no. 3: It was found that there was a need for a Security Information Management Model (SIMM) for the management of security information in the security industry.

8.3.6 Findings related to the case study

Collection of security information: It was found that the SAPS and the WAP have a formalised way of managing crime incident information and intelligence. They use collection units and investigators to collect information and intelligence. Collection plans are specifically structured for each project, so that only the required information and intelligence is collected. The information flows from the bottom upwards to the highest decision maker in the organisation. The crime incident information/intelligence is shared with interested networks such as private security companies, intelligence structures and other information networks. Only persons who have the level of security clearance have the authority to access the information. Private security service providers in Western Australia have individual ways of collecting security information on threats, vulnerabilities and incidents. Specific collection plans are developed for the collection of security information. The Western Australian government departments use the complaints management unit to collect information on incidents of policy violations.

Analysis of security information: It was found that in South Africa crime information management companies have a well-structured, regulated way to analyse crime incident information. The process is controlled by standing operating procedures which is agreed upon by the clients and the service provider. The analysis and recommendation of strategies to clients and stakeholders is coordinated, monitored and evaluated. Security information management companies in South Africa are private initiatives. They do not collect security information, but coordinate incident information received from their clients. They collate the crime incident information received from their clients, analyse the crime incident information. In Australia they do not make use of security information management companies to coordinate and analyse incident information. Private security service providers in Western Australia make use of a risk register to record all risks. The risk register informs on asset criticality against identified risks and provides a framework from which to allocate the needed physical security resources and funding. Qualified analysts are used to analyse intelligence in the WAP.

All crime incident information/intelligence in the SAPS and WAP that enters the system is analysed by analysis units. The WAP sanitises the information and declassifies the level before information/intelligence is shared. Only the relevant portions of the information/intelligence are shared.In both SAPS and WAP decisions are made by management to operationally and strategically implement the information/intelligence. In addition to actionable crime information products, they also generate a Crime Threat Analysis (CTA) document with all the information/intelligence they receive. All threat information received by the police is also included in the CTA.

Implementation of security risk control measures: It was found that the information management companies in South Africa provide actionable crime information products, threat assessment reports and tactical strategies aimed at mitigating serious crimes confronting their clients. The sharing of crime incident information by crime information management companies helps enrich the existing repository and avoids duplication of strategies to address the same problem. Networking assists in coming up with one formidable strategy for recommendation to the client and the police.

8.4 RECOMMENDATIONS FOR THE SECURITY INDUSTRY

After exploring the management of security information in the security industry in the Gauteng province of South Africa and Perth in Western Australia the following recommendations are proposed:

A Security Information Management Model should be used as a tool to reduce crime, increase detection rates and prevent losses in organisations and companies. This is the first study into the management of security information in the security industry. The management of security information relates to security information pertaining to incidents, threats and vulnerabilities impacting on an organisation/company being protected. This research has opened a number of new avenues for the collection, and analysis of security information and the implementation of security risk control measures. Hence, a Security Information Management Model was developed. This model differs from the following models:

- Intelligence Model, where a specific need for intelligence is identified for intelligence management. Mainly used by Intelligence agencies.
- Security Risk Information Management Model, where risks are identified for risk assessment. Mainly used by Security companies.
- Crime Information Management Model, where crime information is managed to identify crime trends and criminals. Mainly used by law enforcement.

The stages of the Security Information Management Model should include the following:

- timely collection of security information on incidents, threats and vulnerabilities;
- rapid analysis of security information; and the
- designing of strategies, actionable crime information products and physical protection systems to deter, detect, delay, and respond to an adversary.

The organisation/company being protected should consider the role of security as important in protecting its assets and providing sustainability to its business activities. Security information should be seen as the life blood of any organisation. if

the circulation of this life blood is cut, the organisation/company will not be able to sustain itself. It is important that the board of directors include security threats as part of their strategic plan. The board of directors of the organisation/company should provide the organisational security strategy to address the identified threats. The organisational security strategy should indicate the prioritised threats, projected costs and time frames to address the specific threats. The Security Head should be a stakeholder on the board of directors, for the purpose of providing security advice and direction. The management of security information should be a permanent point on any board of director's agenda.

Security information should be managed by the Security Head in three phases namely; collection of security information; analysis of security information; and the implementation of security risk control measures. A Security Information Management Centre (SIMC) should be established to equally manage the three phases. The collection and the analysis of the security information should be handled by a Security Information Management Centre (SIMC) and referred to top management as an analysis report (result). The analysis report is handled by top management and referred to the operational manager or the human resources manager for the implementation of management's decision. The operational manager will need to project manage the implementation of security risk control measures within the context of physical protection systems, strategies and actionable crime information products. The human resources manager will need to manage all workplace investigations. All feedback reports on the implementation of management's decision should be managed by the SIMC.

The Security Head responsible for all security related matters in the organisation should develop a security plan to address the security threats using the organisational security strategic objectives as a directive. The security plan which should consist of the threats affecting the organisation, information on vulnerabilities and incident related information relevant to the threat should be used to address the prioritised threats in terms of the allocated budget. In essence, the security plan will consist of a Threat Assessment document, A Vulnerability Assessment document and an Incident Pattern Analysis document. These assessment documents should be prepared by a qualified security analyst and used as part of the security plan. The

assessment documents should serve as tools to manage security risks, conduct performance management as well as impact studies on the physical protection systems. A target-centred approach should be followed to identify a shared target.

A collection plan should be prepared to focus on the identified threat. The senior security officer should develop and manage this collection plan in accordance with project management principles. Collection capability should be intensified by making use of personnel from the organisation being protected, clients and security personnel. If feasible, organisations should consider establishing security information collection units. Responsibilities of security officials to collect security information pertaining to specific threats should be included in their contracts, job descriptions and service level agreements, whichever is applicable.

An awareness ethos should be created, so that personnel, clients and stakeholders become involved in the collection of security information. Security awareness procedures to encourage voluntary collection of security information should be advertised in the organisation being protected. Motivational programs should be presented to personnel to intensify the collection of security information. Security personnel need to be skilled in the collection of security information. On the job training should be encouraged. The training curriculum should focus on the needs of the individual to perform the collection function. Psychologists should become involved in team building and life skills survival training, to address the fear and victimisation that might occur during the collection of security information. There should be policies in place for the protection of witnesses against victimisation, so that people are protected against intimidation by criminals. The Witness Protection Programme should include an anonymous call number. Management should provide sufficient human, technical and physical resources to collect security information.

Policy and Standardised operating procedures similar to that used by SAPS, SABRIC, PSI and the CGRI should be designed for the collection of security information. The standard operating procedure should be inclusive of ethical standards to guide security personnel in the lawful collection of security information.
In this way all personnel will be aware of the collection cycle and the process to be followed. Security information protection measures should be put in place as a

safeguard against leakage of information and to overcome mistrust. Once the collector feels trusted he should provide more information. This should enhance mutual relations. A cell phone system should be explored to enter all actionable information in SMS text and have it electronically relayed to the automated system in the control room, SAPS crime control room and to the response team.

Workplace investigations should be made part of the private security provider's infrastructure as it will help in the collection of security information. The focus should be on collecting information by making use of informers, surveillance and undercover operations. Information collected during workplace investigations will enlighten management on the extent of unlawful activities and misconduct in their organisation.

A standardised framework should be used for the collection of security information. In this way all personnel will be aware of the collection process to be followed.

The sharing of information should be encouraged by management. Sharing of information between management and grassroots personnel and with SAPS, NDPP and other security service providers with similar interests will go a long way in intensifying the collection of security information. External sources of information should be explored through networking and the signing of a memorandum of understanding to access each other's databases. This will add value to the information on hand. Fusion Centres should be established by security service providers with similar interests so that joint sharing of information can take place. Security service providers should also participate in community policing structures and in the SAPS war room strategy established by SAPS provincial offices for the sharing of information.

Every security service provider should create an analysis capability at their organisations/companies. The organisational security strategy, the security plan and the needs of the clients should be considered for the purpose of analysis. This is important to determine the projected costs allocated to address the specific threat confronting the organisation. This will help the analyst to prepare a recommendation based on the projected costs. Following this process will save the organisation

human resources, technical and physical resources and money. Qualified analysts should be employed to conduct security information analysis according to the organisational security strategy and the security plan of the organisation.

The analyst should generate a threat assessment document, vulnerability assessment document and an incident pattern analysis document. All security information collected on a daily basis should be used to populate these documents. These documents should serve as live documents, which will continue to inform the designing and development of future collection plans. Security management should engage with analysts for the development of collection plans. The analysis of security information by qualified analysts will help in the identification of the correct vulnerability areas, so that the most appropriate operational responses may be provided to mitigate the risks. Personnel responsible for analysis should be given the necessary computer hardware and software resources to perform their tasks effectively. There should be adequate resources for the analysis of security information. There is a need for analytical computer software programmes to assist analysts to generate innovative strategies and actionable information products. The organisational security strategy should indicate the type of hardware and software requirements to perform specific types of analysis.

Analysts should be given continuous training to keep them updated with technological advancements. Data analysis capability should be established by all security service providers. The analysis of security information function should be closely managed by line management. Management should enjoy a relationship of trust with their analysts. Qualified analysts with operational experience should be utilised to design actionable information products, strategies, and recommendations for the PPS in consultation with the end users. Management should not interfere with the analysis function.

The reliability of the information source should be assessed on criteria such as the previous quality of information supplied by the source, the situation, the location and likely access of the source at the time the information was collected. All security information received should be reviewed by data capturers or information managers. They are to ensure that the information is reliable, accurate and timely. The collected

security information should be tested to determine if the collected information is sufficient for the analyst to conduct the relevant analysis.

There should be a collection capacity to assist the analysts to obtain missing information or any other information need to enrich the information on hand. The completed document with all the relevant information should be sent to the analyst. Standard operating procedures should help in the data mining of all the collected security information. This should help in overcoming the problem of information overload and overburdening analysts from achieving the organisational security strategy. The focus should be on threat and vulnerability information, as proactive action will result in the prevention of incidents from taking place. Methods used for the classification of information should be improved by enforcing a code of ethics among personnel and introducing information protection standards to control access where necessary. A standardised framework should be used for the analysis of security information. In this way all personnel will be aware of the analysis cycle and the process to be followed.

The analysis report should be sent to management to make a decision on the implementation of the recommended security risk control measures.Security risk control measures should be implemented according to the organisational security strategy and the security plan. In this way decisions will be made to give priority to specific threats that were not previously addressed or possibly not identified as such. Implementation of security risk control measures should be done in accordance with the allocated budget. Costs should not be an impediment to address the threat, Money spent on security risk control measures should be regarded as an investment and not a cost, because the purpose is to protect life and property, prevent losses and to finally ensure business continuity. The aim, therefore, should be to reduce the threat with the available budget and not shelve the application of security risk control measures.

In making a decision on the implementation of specific security risk control measures management must consider the security strategy, the security threats and the strategic objectives as identified in the organisational security strategy. In many instances security service providers use the reduction of crime, increase in detection

rates and the prevention of losses as the strategic objectives to decide on the implementation of the most appropriate security risk control measures. Security risk control measures should be considered for implementation in conjunction with the organisational security strategy and the security plan. The security risk control measures should be directed at addressing specific threats, vulnerabilities and the re-currence of incidents according to the security plan.

The strategic objectives of the organisational security strategy should direct the implementation of the security risk control measures. The design of the security risk control measures should be considered by management. The security risk control measures should be designed to address the strategic objectives. To design a specific security risk control measure, the security practitioner must take into consideration the organisation's operations and conditions define the threat and identify the target. Security risk control measures need to be designed to deter, detect, delay and respond to intrusions. Organisations need to safeguard themselves against incorrect and illegally obtained information which may be detrimental to the implementation of security risk control measures. Security risk control measures relating to crime should be immediately operationalised by the security personnel with the assistance of the SAPS. The sharing of information on security risk control measures should take place at the Community Police Forums and at special meetings held with SAPS. This will benefit the broader South African community by creating a much safer and secure environment. The challenge is for security managers to stay current on innovative design strategies. This knowledge should be coupled with the latest information on issues of changes in cultural values, crime, technology, market conditions and political conditions.

The approved implementation of security risk control measure should be disseminated in a formalised manner. It should preferably be a written communication. Experienced security personnel should be used for the implementation of security risk control measures. Project management approach to be used in the implementation of security risk control measures. Resources should be made available for the implementation of security risk control measures. The design of the security risk control measure should be quantitatively or qualitatively evaluated for deterrence of the adversary, detection of the adversary, delay of the

adversary and response by security personnel. Some situations may require immediate action and prompt intervention. Some are cyclical, managerial and are amenable to technical solutions and problem solving methods. Others are chronic, endemic difficulties that require the application of strategies over time, to change conditions and move an organisation ahead. There should be regular communication between the analyst and the end user. The end user should be allowed to request additional analysis of the security risk control measure. There should be a formalised manner in dealing with feedback from the end-user. It should preferably be a written communication. There should be continuous monitoring and evaluation of the implemented security risk control measure by line management. A standardised framework should be used for the implementation of security risk control measures. In this way all personnel will be aware of the implementation cycle and the process to be followed.

Government departments, employing contract security companies, and those with in-house security services should have the Security Head as part of top management. The Security Head should be there to give strategic direction and guidance on security threats affecting the organisation, organisational security strategy, strategic objectives and the security plan. Top management should make a commitment in terms of budget and resources to address the identified threats confronting the organisation. The procedures outlined above should be followed in the implementation of the Security Information Management Model.

The security industry should consult with academic institutions responsible for providing academic qualifications in security management to offer a qualification in security information management, so that the qualification in security information management becomes compulsory for employment of security officials.

The Security Information process outlined above should be used to address legislative gaps in the Private Security Industry Regulatory Act No. 56 of 2001 and other related legislative frameworks.

8.5 RECOMMENDED SECURITY INFORMATION MANAGEMENT MODEL

The grounded theory indicates that there is the need for security officials to use a Security Information Management Model (SIMM) to manage security information. This theory was verified by conducting a self-administered questionnaire survey with security officials from different sectors of the security industry in Gauteng. Based on the findings, the researcher has come to a conclusion that 'security officials need a Security Information Management Model to manage security information in the security industry'. The researcher proposes a Security Information Management Model as indicated in Paragraph 7.3. This model may be used as a standardised framework to manage security information in the security industry. The advantages of the model include the following:

- The model is based on a common body of knowledge for security information management specifically suited for the security industry. It includes in-house private security service providers, contracted security service providers and also those who provide a security service to government departments. This model introduces a new dimension to the security industry in the sphere of collection and analysis of security information and the implementation of security risk control measures.

- In the collection phase the model introduces the security practitioner to Strategic Planning, organisational security strategy, a security plan and a collection plan. These plans if implemented accordingly will help manage security information effectively and efficiently within a specific budget. In the analysis phase it introduces the security practitioner to the organisational security strategy, security plan, qualified analysts capability, key information needs, tasking to collect missing information, evaluation and interpretation and analysis results. Documents relevant to the analysis phase are the Threat Assessment, Vulnerability Assessment and the Incident Pattern Analysis. These are 'real-time' live documents which can be continuously used by all levels of the security industry. The implementation of the security risk control measures phase reflects on the strategic objectives, design and the

implementation of security risk control measures. All of these are new concepts.

- This SIMM relates to the collection of security information on threats, incidents and vulnerabilities and it is not confined to the identification of crime risks. The analyst is responsible to conduct a threat analysis, vulnerability analysis and incident pattern analysis to prepare an assessment of threats, vulnerabilities and incidents. The analyst should provide the analysis results with recommendations to the top management of the organisation/company which is being protected, to address specific threats, vulnerabilities and prevalent incidents to reduce crime, increase detection rates and prevent losses. Management may decide on how best to use the analysis result to develop a strategy, actionable crime information product or enhance its physical protection systems to achieve its objectives.

- The SIMM model may be applied using the security information management cycle. The cycle includes three important stages, namely; the timely collection of security information on incidents, threats and vulnerabilities; the rapid analysis of security information, and the designing of strategies, actionable crime information products and physical protection systems to deter, detect, delay, and respond to an adversary.

- The model provides a broad standardised framework, which needs to be entrenched in a policy framework supported by standard operating procedures for implementation.

- The Threat Assessment, Vulnerability Assessment and the Incident Pattern Analysis documents will be introduced to the security industry by this model. Threat assessments are used by the WAP and SAPS to provide operational and strategic direction in policing. For the sake of this model and to avoid confusion with law enforcement, my suggestion is, that the threat assessment document, hereinafter be referred to as the ‘Security Threat Assessment’. All three of these documents will help guide the Security Head of an organisation/company to strategically manage threats, vulnerabilities and

incidents. These documents will also assist the Security Head in preparing a projection of costs for a security budget. They may also serve as base documents to conduct performance assessments of personnel.

- The model also ensures that all role-players are made aware of the importance of security information. It involves all employees, security officials and customers to become involved in the collection of security information.

- The strategic objectives of this model are to reduce crime, increase detection rates and prevent losses. The model encourages the sharing of security information with all stakeholders and role-players.

- Government sectors may implement this model to manage security information, within their environment.

- This model will aid government in bringing about changes to the Private Security Industry Regulatory Act, No.56 of 2001, so that security information may be stored at a central database for use by all registered security service providers and law enforcement.

- Academia will able to use the model to develop a learning programme in security information management, so that education, training and development may be provided to security officers in the security industry. This will help in equipping security officers in knowledge and skills with the object of professionalising the security industry.

The proposed model, however, has the following limitations:

- It may be used to enhance service delivery to clients with the necessary adaptations.

- It cannot be used to replace the UNISA developed Security Risk Management Model (SRMM). According to Blyth and Kovacich, (2006:43-50), Security Risk Management is the process of assessing risk, taking steps to reduce risks to an acceptable level and maintaining that level of risk. The Security Risk

Management Model as discussed in Paragraph 1.2.6 is the one being applied by most security risk managers within Gauteng. In this SRMM security (crime) risks are identified by conducting a risk analysis and security survey. Security risk control measures are identified to counteract the identified risks. A return-on-investment exercise is undertaken to ensure that the security control measures are cost effective. A report containing findings and recommendations is submitted to top management of the company for a decision on the implementation of security measures. On approval by management the security measures are implemented and then tested by means of a penetration exercise (Rogers, 2008: 151-154).

- It is not an intelligence driven model. It may, however, be used for that purpose with the necessary adaptations.

- See Figures 7.1, 7.2 and 7.3 for the schematic representation of the SIMM model.

8.6 RECOMMENDATIONS FOR FURTHER RESEARCH

This study provides a new approach towards improving security information management in the security industry. The limitations discussed in the above paragraph uncover potential areas for future research. Another area that will benefit from further research will be the Fusion Centres and War Rooms presently being used by private security and law enforcement. Further research should also be considered on the information flow to develop a 'Security Threat Assessment.' Research should include such issues as the use of digital technology for security officials in order to allow them to more efficiently electronically collect security information and have it electronically routed to control centres and the SAPS. Owing to the dynamic nature of security information management, more advanced security information management models should be continuously investigated. This will contribute towards professionalising the discipline.

8.7 CONCLUSION

The Security Industry needs to create the right environment for the collection and analysis of security information to flourish, so that, security information is valued and understood. Security managers must be ready to respond to the outcomes of analysis, by designing appropriate security risk control measures for implementataion. The standardised framework proposed by the researcher will help regulate the collection and analysis of security information and the implementation of the security risk control measures. The proposed standardised framework ought to be reinforced with a policy framework and standardised operating procedures. Monitoring and evaluation should be used to measure the success of the application of the security risk control measures. The findings and recommendations took into consideration the responses of the participants and the literature study for the purpose of reliability and validity. The researcher experienced limitations with regard to literature, and the voluntary participation of security official working at lower levels in the security industry. This was overcome by using national and international literature pertaining to law enforcement information and intelligence. The lower level participation of security officials were encouraged by their senior managers to participate in the study.

LIST OF REFERENCES

Abrie, S. 2008. *Security risk management. Study guide for PSMN03X.* Pretoria: UNISA Press.

Addison, S. 2002. *Introduction to security risk analysis and the cobra approach. C & A security system report (Online serial).* Available: www.security-risk-analysis.com. (accessed on 21 September 2010).

Ainsworth, P.B. 2001. *Offender profiling and crime analysis*. Portland, Or: Willan

Akrava, M.L. & Lane, T.A. 1983. *Beginning social work research.* Boston: Allyn & Bacon.

Allen, R.E. 1992. *Concise oxford dictionary*. 8th edition. Oxford: Clarendon Press.

Altbeker, A. 1998. *Solving crime: The state of the SAPS detective service.* ISS Monograph No. 31. Pretoria: Institute for Security Studies. Available at: http://www.iss.co.za/pgcontent.php?UID=1587.

Atkin, H. 2000. Criminal intelligence analysis: A scientific perspective*. IALEI Journal,* 13(1), May: 3-7.

Australian Security Industry Association Ltd. (ASIAL). 2011. *Who should hold a security licence?* Available at: http://www.asial.com.au/. (Retrieved: 09 August 2011).

Babbie, E.R. 2001. *Basics of social research*. 9th edition. Belmont, Calif.: Wadsworth.

Bailey, K.D. 1987. *Methods of social research.* 3rd edition. London: MacMillan.

Baker, T.L. 1988*. Doing social research,* 4th edition. New York: Free Press.

Berg, B.L. 2009. *Qualitative research methods for the social sciences.* 7th edition. Boston: Allyn & Bacon.

Bless, C. & Higson-Smith, C. 1995. *Fundamentals of social research methods: An African perspective*. 2nd edition. Lansdowne: Juta.

Block, C., Dabdoub, M., & Fregly, S. 1995. *Crime analysis through computer mapping*. Washington, DC: Police Executive Research Forum.

Blyth, A. & Kovacich, G.L. 2006. *Information assurance. Security in the information environment.* Second edition*.* USA: Springer.

Bosch, J.G.S. 1999. The role of structure of the private security industry in South Africa. *ISSUP Bulletin*. Pretoria.

Bozza, C.M. 1978. *Criminal investigation*. Chicago: Nelson Hall.

Brooks, D.J. 2008. *The development and presentation of psychometric concept maps within the knowledge domain of security risk management*. DLit et Phil thesis, Curtin University of Technology, Perth, Australia.

Broder, J.F. 2000. *Risk analysis and the security survey.* Johannesburg: Butterworth/Heinemannn.

Burt, V. 2004. *Test your management skills*. London: Hodder & Stoughton.

Clark, R. 2010. *Intelligence analysis. A target centric approach*. 3rd edition. Washington: CQ press.

Clarke, R.V. & Eck, J. 2003. *Become a problem solving crime analyst in 55 small steps*. London: Jill Dando Institute of Crime Science, University College.

Creswell, J.W. 2003. *Research design: Qualitative, quantitative and mixed methods approach.* 2nd edition. Thousand Oaks: Sage.

Creswell, J.W. 2007. *Qualitative inquiry and research and design: Choosing among five approaches.* Thousand Oaks: Sage.

Creswell, J.W. 2009. *Research design: Qualitative, quantitative and mixed methods approach.* 3rd Edition. Thousand Oaks: Sage.

Delport, C.S.L. & Fouché, C.B. 2011. Mixed methods research. Pp. 433-448. In De Vos, A.S., Strydom, H., Fouché, C.B. & Delport, C.S.L. 2011. *Research at grassroots: For the social sciences and human service professions.* 4th edition. Pretoria: Van Schaik.

Delport, C.S.L. & Roestenberg, W.J.H. 2011. Quantitative data-collection methods: Questionnaires, checklists, structured observation and structured interview schedules. Pp.171-205. In De Vos, A. S., Strydom, H., Fouché, C.B. & Delport, C.S.L. 2011. *Research at grassroots: For the social sciences and human service professions.* 4th edition. Pretoria: Van Schaik.

Delport, C.S.L, Fouché, C.B. & Schurink, W. 2011. Theory and literature in qualitative research. Pp. 297-306. In De Vos, A.S., Strydom, H., Fouché, C.B. & Delport, C.S.L. 2011. *Research at grassroots: For the social sciences and human service professions.* 4th edition. Pretoria: Van Schaik.

Denscombe, M. 2002. *Ground rules for good research: A 10 point guide for social researchers*. Philadelphia: Open University Press.

De Vos, A.S. 2007. Qualitative data analysis and interpretation. Pp. 333-349. 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.

Du Preez, G.T. 1996. *Forensic criminalistics: Criminal investigation.* 2nd edition, Pretoria: UNISA.

Edwards, C.2011.Changing *policing theories for 21st century societies.*3rd edition.Sydney: The federation press.

Ekblom, P. 1988. *Getting the best out of crime analysis.* London: Crown.

Ferraro, E.F. & Spain, N.M. 2006. *Investigations in the workplace.* New York: Auerbach.

Fennely, L.J. 2004. *Effective physical security*. Elsevier: Butterworth Heinemann.

Fay, J.J. 2002. *Contemporary security management.* Woburn: Butterworth Heinemann.

Fischer, R.J., Halibozeck, E. & Green, G. 2008. *Introduction to security*. (8th edition). Boston: Butterworth Heinemann.

Fischer, B.A.J. 2004. *Techniques of crime investigation*. 7th edition. Washington, DC: CRC.

Fouché, C.B., Delport, C.SL. & De Vos, A.S. 2011. Quantitative research designs. Pp. 142-158. In De Vos, A.S., Strydom, H., Fouché, C.B. & Delport, C.S.L. 2011. *Research at grassroots: For the social sciences and human service professions.* 4th edition. Pretoria: Van Schaik.

Fouché, C.B., & Delport, C.S.L. 2011a. Introduction to the research process. Pp. 61-76. In De Vos, A.S., Strydom, H., Fouché, C.B. & Delport, C.S.L. 2011. *Research at grassroots: For the social sciences and human service professions.* 4th edition. Pretoria: Van Schaik.

Fouché, C.B. & Delport, C.S.L. 2011b. In-depth review of literature. Pp.133-141.In De Vos, A.S., Strydom, H., Fouché, C.B. & Delport, C.S.L. 2011. *Research at grassroots: For the social sciences and human service professions.* 4th edition. Pretoria: Van Schaik.

Fouché, C.B. & Schurink, W. 2011. Qualitative research designs. Pp. 307-320. In De Vos, A.S., Strydom, H., Fouché, C.B. & Delport, C.S.L. 2011. *Research at grassroots: For the social sciences and human service professions.* 4th edition. Pretoria: Van Schaik.

Garcia, M.L. 2001. *The design and evaluation of physical protection systems.* Boston: Butterworth Heinemann.

Garcia, M.L. 2006. *Vulnerability assessment of physical protection systems.* Boston: Butterworth Heinemann.

Garcia, M.L. 2008. *The design and evaluation of physical protection systems*. 2nd edition. Boston: Butterworth/Heinemann.

Gardner, R.M. 2005. *Practical crime scene processing and investigation: Practical aspects of criminal and forensic investigation series*. Washington, DC: CRC Press.

Gerring, J. 2007. *Case study research: Principles and practices*. USA: Cambridge University Press.

Glaser, B.G. 1978. *Theoretical sensitivity.* Mill Valley, Calif.: Sociology Press.

Glaser, B.G. 1992. *Basics of grounded theory analysis*. Mill Valley. Calif.: Sociology Press.

Goldsmith, V., Mcguire, P.G., Mollenkopf, J.H. & Ross, T.A. 2000. *Analysing crime patterns: Frontiers of practice.* Thousand Oaks, Calif: Sage.

Gottlieb, S., Arenberg, S. & Singh, R. 1994. *Crime analysis: From first report to final arrest*. Montclair, CA: Alpha.

Greef, M. 2007a. Sampling and sampling methods. Pp.192-204. In De Vos, A.S., Strydom, H., Fouché, C.B. & Delport, C.S.L, *Research at grassroots: For the social sciences and human service professions.* 3rd edition. Pretoria: Van Schaik.

Greef, M. 2007b. Information collection and interviewing. Pp.286-313. In De Vos, A.S., Strydom, H., Fouché, C.B. & Delport, C.S.L, *Research at grassroots: For the social sciences and human service professions.* 3rd edition. Pretoria: Van Schaik.

Greef, M. 2011. Information collection: interviewing. Pp.341-375. In De Vos, A.S., Strydom, H., Fouché, C.B. & Delport, C.S.L. 2011. *Research at grassroots: For the social sciences and human service professions.* 4th edition. Pretoria: Van Schaik.

Hirschfield, A. & Bowers, K. 2001. *Mapping and analysing crime data: Lessons from research and practice*. London: Taylor and Francis.

Horne, J.S. 2009. Crime information analysis within a public service organization: An assessment. *Acta Criminologica: Southern African Journal of Criminology, 22(1):68-80.*

Irish, J. 1999. *Policing for profit: The future of South Africa's Private Security Industry*. ISS Monograph No. 39. Pretoria: Institute for Security Studies.

Jacobs, T., Sheperd, J. & Johnson, G. 1998. Strengths, weaknesses and opportunities (SWOT) analysis. Pp. 122-138. In Ambrosini, V. Johnson, G. & Scholes, K. 1998. *Exploring techniques of analysis and evaluation in strategic management*. Paris: Prentice Hall.

Johnson, B.R. 2005. *Principles of security management*. New Jersey: Prentice Hall

Jordaan, J. 2003a. The role of intelligence in investigations (part 1). *Servamus,* 96(4), April: 56-59.

Jordaan, J. 2003b. The role of intelligence in investigations (part 2). *Servamus,* 96(5), May: 58-59.

Kerlinger, F.N.1986.Foundations of behavioural research, 3rd ed.Fort Worth: Harcourt.

King, M.E. 1994. *The King report on corporate governance*. Parklands: Institute of Directors in South Africa.

Kole, O.J. 2010. *An examination of security measures for the protection of petrol stations: An analysis of case studies in Gauteng.* MTech dissertation. University of South Africa, Pretoria.

Kritzinger, E. 2006. *An information security retrieval and awareness model for industry.* Phd thesis. University of South Africa, Pretoria.

Kruger, D.J., De Vos, A.S., Fouché, C.B. & Venter, L. 2007. Quantitative data analysis and interpretation. Pp.217-245. 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.

Leedy, P.D. & Ormrod, J.E. 2001. *Practical research: Planning and research.* 7th edition. Upper Saddle River, NJ.: Prentice Hall.

Leedy, P.D. & Ormrod, J.E. 2005. *Practical research: Planning and design.* 8th edition Upper Saddle River, NJ.: Prentice Hall.

Le Roux, G.J. 2004. *A quantitative risk analysis model for private security managers*. DLit et Phil thesis, University of South Africa, Pretoria.

Louw, A. 2001. Understanding police crime statistics. *Crime Index South Africa*, 5(3), May/June: 1-5.

Lyman, M.D. 1988. *Criminal investigation: The art and the science.* Upper Saddle River, NJ.: Prentice Hall.

Machovec, F. 2006. *Private investigation and security science: A scientific approach.* USA: Charles C Thomas.

Marais, C.W. & Van Rooyen, H.J.N. 1990. *Misdaadondersoek*. Pretoria: Pro-media.

Marais, A. 1995. *Die modus operandi van die bankrower: ń Kriminologiese introspeksie*. DLit et Phil thesis, University of South Africa, Pretoria.

Mashall, C. & Rossman, G.B. 1999. *Designing qualitative research,* 2nd edition. London: Sage.

Matthews, A. 1986. *Freedom, state security and the rule of law: Dilemmas of apartheid Society.* Cape Town: Juta.

Minnaar, A. & Nogoveni, P. 2004.The relationship between the South African Police Service and the Private Security Industry: Any role for outsourcing in the prevention of crime? *Acta Criminologica: Southern African Journal of Criminology, 17(1): 42-65.*

Minnaar, A. 2005. Private-public partnerships: Private security, crime prevention and policing in South Africa, *Acta Criminologica: Southern African Journal of Criminology, 18(1): 85-114*

Minnaar, A. 2007. *A review of the issues and challenges facing the private security industry in South Africa.* Unpublished research report. Pretoria: Department of Security Risk Management, University of South Africa/Open Society Foundation.

Minnaar, A. 2010. What has happened to 'Community Policing' in South Africa post-1994? *Acta Criminologica: Southern African Journal of Criminology*. CRIMSA 2009 Conference Special Edition No.2/2010: 189-210

Merriam, S.B. 1988. *Case study research in education: A qualitative approach.* San Fransico: Jossey-Bass.

Montgomery, R.J. & Majeski, W.J. 2005. *Corporate investigations*. 2nd edition. Arizona: Lawyers and Judges Publishing Company.

Montesh, M. 2007. *A critical analysis of the crime investigation system within the South African Criminal Justice System: A comparative study*, Phd thesis. University of South Africa, Pretoria.

Morgan, D.L. 1997. *Focus groups as qualitative research*, 2nd edition. Thousand Oaks: Sage.

Morrison, C.J. 2004. *A criminological study of women in the South African Police Service.* Phd thesis. University of South Africa, Pretoria.

Mouton, J. & Marais, H.C. 1990. *Research methodology: Basic concepts in the methodology of the social sciences*. Pretoria: HSRC.

Mouton, J. & Marais, H.C. 1996. *Understanding social research.* Pretoria: HSRC.

Mouton, J. & Marais, H.C., Prinsloo, U.D. & Rhoodie, N.J. 1985. Metodologie van die geesteswetenskappe. Pretoria: RGN.

Muller, M.L.2002a. *Defending against hostile competitive intelligence. Nuts and bolts business series/competitive intelligence series: A practical guide for leaders.* Randburg: Knores.

Muller, M.L., Whitehead, C. 2002. *What is competitive intelligence? Nuts and bolts business series/competitive intelligence series: A practical guide for leaders: Guide1.* Randburg: Knores.

Muller, M.L. 2002b*. Gathering competitive information. Nuts and bolts business series/competitive intelligence series: A practical guide for leaders: Guide3.* Randburg: Knores.

Muller, M.L. 2002c. *Creating Intelligence. Nuts and bolts business series/competitive intelligence series: A practical guide for leaders: Guide 4.* Randburg: Knores.

Mzwandile.P. 2011. Collaboration is crucial. *High Tech Security Solutions. The Journal for Security, Operations and Risk Management.* 17(9): 28-29

National Criminal Intelligence Service (NCIS). 2000. *The National Intelligence Model.* London: Home Office, National Criminal Intelligence Service.

Nemeth, C.P. 2010. *Private security and the investigative process.* 3rd edition. United States: CRC Press.

Newburn, T. Williamson, T. & Wright, A. 2008. *Handbook of criminal investigation*, Cullompton: Willan.

Noak, I. & Wincup, E. 2004. *Criminological research: Understanding qualitative methods*. London: Sage.

O'Block, R.L 1981. Security and crime prevention, Stoneham: Butterworth.

Olckers, C. 2007. *An examination of the impact of residential security measures on the incidents of residential burglary in two selected northern suburbs of Johannesburg: A security risk management approach*. MTech dissertation. University of South Africa, Pretoria.

Opolot, J.S.E. 1999. *An introduction to private security: A comparative introduction to an international phenomenon*, New York: Austin & Winfield.

Patton, M.Q. 2002. *Qualitative research and evaluation methods*. 3rd edition. Thousand Oaks, CA: Sage.

Paulsen, D.J. 2004. To map or not to map: Assessing the impact of crime maps on police officer perceptions of crime. *International Journal of Police Science and Management*, 6(4), August: 234-246.

Peterson, M.B. 1994. *Applications in criminal analysis: A sourcebook*. Westport, Conn: Greenwood Press.

Powers, G.T., Meenaghan, T.M. & Toomey, B.G. 1985. *Practice focussed research: Integrating human service practice and research.* New Jersey: Prentice hall.

Private Security Regulatory Authority. 2012. Private Security Industry in South Africa. Available at: www.psira.sa.co.za. (Retrieved: 10 February 2012).

Prenzler, T. Earle, K. & Sarre, R. 2009. Private security in Australia: Trends and key characteristics. *Trends and issues in crime and criminal justice No. 374.* Canberra. Institute of Criminology.

Ratcliffe, J.H. 2003. Intelligence led policing. *Trends and Issues in Crime and Criminal Justice.* Canberra: Australian Institute of Criminology. April: 1-6.

Ratcliffe, J. 2009. Intelligence led policing. Cullompton: Willan

Redpath, J. 2004. *The Scorpions: Analysing the Directorate of Special Operations: Justice in action*. ISS Monograph No. 96. Pretoria: Institute for Security Studies.

Reuland, M.M. 1997. *Information management and crime analysis*. Washington, DC.: Police Executive Research Forum.

Ribaux, O., Girod, A., Walsh, S., Margot, P., Mizrahi, S. & Clivaz, C. 2003. *Forensic intelligence and crime analysis, law, probability and risk*. Washington, DC.: CRC.

Robson, C. 2000. *Small scale evaluation: Principles and practice*. London: Sage.

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.*

South African Banking Risk Information Centre (SABRIC).Business presentation at Midrand SAPS 10111 centre. Available at: https: www. sabric.co.za. (Retrieved: 07 June 2011).

Shaw, G. 2002.Effective security analysis*. IT-Security journal*. April 2002

Simonsen, C.E. 1998. *Private security in America: An introduction.* New Jersey: Prentice Hall.

Smit, P.J & Cronjé, G J de J. 2002. *Management principles: A contemporary edition for Africa.* Cape Town: Juta.

Smit, B.F. 1989. *Police Science: Only study guide for POL 203-P (security).* Pretoria: UNISA.

Smith, P. & Nataliier, K. 2005. *Understanding criminal justice: Sociological perspectives.* Great Britain: Cromwell Press.

Straus, A. & Corbin, J. 1990. *Basics of qualitative research: Grounded theory procedures and techniques.* London: Sage.

Strydom, H. 2007. Sampling and sampling methods. Pages 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.

Steyn, J. 2002. *The effect of "group think" in the South African Police Service: An experimental analysis.* MTech: Policing dissertation: Pretoria: Technikon Pretoria.

Stelfox, P. 2009. Criminal investigations: an introduction to principles and practice. Cullompton: Willan.

Talbot, J. & Jakeman, M. 2008. *Srmbok: Security risk management body of knowledge.* Australia: Ligare.

University of South Africa (UNISA): Muckelneuk Library. *Security information management and analysis topics.* Available at: http://www.unisa.co.za. (Retrieved: 2 November 2010).

Van Heerden, T.J. 1982. *Introduction to Police Science.* Pretoria. UNISA.

Van Heerden, T.J. 1986. *Inleiding tot die Polisiekunde*. Pretoria: UNISA.

Van Rooyen, H.J.N. 2001. *Practical guide for private investigators*. Pretoria: Henmar.

Van Rooyen, H.J.N. 2008. *The practioner's guide to forensic investigation in South Africa*. Pretoria: Henmar.

Van Vuuren, J.W.J. 1992. *Beveiliging in die plaaslike owerheidsektor.* MA dissertation. Pretoria: University of South Africa.

Valsamakis, A.C., Vivian, R.W. & DuToit, G.S. 1996. *The theory and principles of risk management.* Johannesburg: Heinemann.

Vellani, K.H. & Nahoun, J. 2001. *Applied crime analysis*. Boston: Butterworth–Heinemann.

Whitt, E.J. 1991. Artful science: a primer on qualitative research methods. *Journal of the College Student Development,* 32(5): 406-415.

Zedner, L. 2003. The concept of security: An agenda for comparative analysis, *Legal Studies,* 23(1): 153-176.

Decided Cases

State *vs Botha and others (1) 1995 (2) SACR 598 (W)*

State vs Dube 2000 (1) SACR 53 (N)

Acts

Australia. 1996. The Australian Security and Related Activities (Control) Act 1996. Australia: Government Printer.

Australian. 1997. Security and Security and Related Activities (Control) Regulations 1997. Australia: Government Printer.

South Africa. 1977. Criminal Procedures Act 51 of 1977. Government Gazette 5827. Pretoria: Government Printer. 27 December.

South Africa. 1980. National Key points Act 102 of 1980. Pretoria: Government Printer.

South Africa. 1982. Protection of Information Act 84 of 1982. Pretoria: Government Printer.

South Africa. 1987. South African Security Officer's Act 92 of 1987. Pretoria: Government Printer.

South Africa. 1992. Interception and Monitoring Act 127 of 1992. Pretoria: Government Printer.

South Africa. 1994. National Strategic Intelligence Act 39 of 1994. Government Gazette 16128. Pretoria: Government Printer. 2 December.

South Africa. 1995. South African Police Service Act 68 of 1995. Government Gazette 16731. Pretoria: Government Printer.6 October.

South Africa. 1996. The Constitution of the Republic of South Africa 108 of 1996. Government Gazette 17678. Pretoria: Government Printer.18 December.

South Africa. 2000. Promotion of Access to Information Act 2 of 2000. Government Gazette 20852. Pretoria: Government Printer.3 February.

South Africa. 2000. Protected Disclosures Act 26 of 2000. Government Gazette 21453. Pretoria: Government Printer. 7 August.

South Africa. 2001. Private Security Industry Regulatory Act 56 of 2001. Government Gazette 23051. Pretoria: Government Printer.25 January.

Interviews

Conradie, S., CEO of Security Industry Alliance. 2010. Interview with author. 18 November. Johannesburg, Gauteng, South Africa.

De Kock, C., Deputy Divisional Commissioner, SAPS Crime Intelligence Division. 2011. Interview with author. 14 January. Pretoria, Gauteng, South Africa

Interview 1. Senior security officer from a government department.2010. Confidential interview with author. 8 April. Johannesburg, Gauteng, South Africa.

Interview 2. Senior security officer from a government department.2010. Confidential interview with author. 20 April. Pretoria, Gauteng, South Africa.

Interview 3. Crime Intelligence officer SAPS.2011. Confidential interview with author. 11 March, Pretoria, Gauteng, South Africa.

Interview4. Security manager of a contract security service provider.2010. Confidential interview with author. 11 May. Pretoria, Gauteng, South Africa.

Interview 5. Security manager of an in-house security service provider (complex security).2010. Confidential interview with author. 19 March. Pretoria, Gauteng, South Africa.

Interview 6. Security manager of an in-house security service provider (petroleum company).2010. Confidential interview with author. 23 March. Johannesburg, Gauteng, South Africa.

Interview 7. Security manager of an in-house security service provider (banking security).2010. Confidential interview with author. 8 July. Johannesburg, Gauteng, South Africa.

Interview 8. Security manager of an in-house security service provider (campus security).2010. Confidential interview with author. 9 April. Pretoria, Gauteng, South Africa.

Interview 9. Security manager of an in-house security service provider (retail security).2010. Confidential interview with author.15 April. Pretoria, Gauteng, South Africa.

Interview 10. Security manager of an in-house security service provider (mining security).2010. Confidential interview with author. 24 March. Johannesburg, Gauteng, South Africa.

Interview 11. Security manager of an in-house security service provider (casino security).2010. Confidential interview with author. 21 April. Johannesburg, Gauteng, South Africa.

Interview 12. CEO of a contract security service provider.2010. Confidential interview with author. 29 April. Pretoria, Gauteng, South Africa.

Interview 13. CEO of an in-house security service provider (mining security).2010. Confidential interview with author. 24 March. Johannesburg, Gauteng, South Africa.

Interview 14. CEO of a contract security service provider (residential Security) 2010. Confidential interview with author. 6 December. Pretoria, Gauteng, South Africa.

Interview 15. Investigator of a contract security service provider (insurance investigations).2010. Confidential interview with author. 19 May. Johannesburg, Gauteng, South Africa.

Interview 16. Security manager of a contract security service provider (retail security).2010.Confidential interview with author. 22 June. Johannesburg, Gauteng, South Africa.

Interview 17. Security manager of an in-house security service provider (campus security).2010. Confidential interview with author. 15 March. Pretoria, Gauteng, South Africa.

Interview 18. Head of Security of a government department in.2011. Confidential interview with author. 26 May. Perth, Western Australia.

Interview 19. Head of Security of a government department.2011. Confidential interview with author. 26 May. Perth, Western Australia.

Interview 20. Investigation and Enforcement Head of a government department. 2011. Confidential interview with author.18 May. Perth, Western Australia.

Interview 21. Senior police official from the WA Police.2011. Confidential interview with author.10 May. Perth, Western Australia.

Interview 22. Senior police official from the WA Police. 2011. Confidential interview with author.13 May. Perth, Western Australia.

Interview 23. Director of a contract security service provider (industrial security). 2011. Confidential interview with author. 18 May. Perth, Western Australia.

Interview 24. Senior academic from ECU. School of computing and security science. 2011. Confidential interview with author. 17 May. Perth, Western Australia.

Interview 25. Senior academic from ECU: School of computing and security science. 2011. Confidential interview with author. 17 May. Perth, Western Australia.

Interview 26. Senior academic from ECU: School of computing and security science. 2011. Confidential interview. 23 May. Perth, Western Australia.

Interview 27. Senior academic from ECU: School of computing and security science. 2011. Confidential interview with author. 24 May. Perth, Western Australia.

Interview 28. Associate Research Professor from ECU: School of computing and security science.2011. Confidential interview with author. 13 May. Perth, Western Australia.

Interview 29. Director of a contract security service provider (commercial/residential security.2011.Confidential interview with author. 18 May. Perth, Western Australia.

Interview 30. Security manager of a contract security service provider (banking security).2011. Confidential interview. 19 May. Perth, Western Australia.

Interview 31. Security advisor of a contract security service provider (mining security).2011. Confidential interview with author. 23 May. Perth, Western Australia.

Interview 32. Security manager of an in-house security service provider (campus security).2011. Confidential interview with author. 23 May. Perth, Western Australia.

Interview 33. Security manager of an in-house security service provider (casino security).2011. Confidential interview with author. 25 May. Perth, Western Australia.

Interview 34. Security manager of an in-house security service provider (casino security).2011.Confidential interview with author.25 May. Perth, Western Australia.

Interview 35. Senior academic from UNISA. Department of Criminology and Security Science, Programme Security Management.2011. Confidential interview with author. 15 March. Pretoria, Gauteng, South Africa.

Interview 36. Senior managers, Violent Crime Office. SABRIC.2010. Confidential interview with author. 16 April. Johannesburg, Gauteng, South Africa.

Interview 37. Senior managers from CGRI. 2010. Confidential interview with author. 22 June. Johannesburg, Gauteng, South Africa.

Interview 38. Senior managers from PSI.2010. Confidential interview with author. 6 July. Pretoria, Gauteng South Africa.

Maree, A., Senior Manager, Violent Crime Office SABRIC.2010. Interview with author. 25 June. Johannesburg, Gauteng, South Africa.

Reddy, O.D., Assistant Commissioner, SAPS Honeydew Cluster commander.2010. Interview with author. 5 March. Johannesburg, Gauteng, South Africa.

APPENDICES

APPENDIX 1: INTERVIEW GUIDE USED FOR SEMI-STRUCTURED INTERVIEWS

COVER LETTER

UNISA

PO BOX 392

PRETORIA 0003

Dear Participant/Respondent

PARTICIPATION IN RESEARCH PROJECT: SEMI-STRUCTURED INTERVIEW

I am currently a student in the Department of Criminology & Security Science, School of Criminal Justice at the University of South Africa (UNISA), busy with my studies for a ***DLITT et PHIL*** (doctorate) degree in Criminology (Security Risk Management). My research title is "***AN EVALUATION OF THE COLLECTION and ANALYSIS OF SECURITY INFORMATION AND THE IMPLEMENTATION OF SECURITY RISK CONTROL MEASURES IN THE SECURITY INDUSTRY IN GAUTENG, SOUTH AFRICA".***

I will be conducting an interview with you on the collection and analysis of security information and the implementation of security risk control measures. The interview should take about an hour.

The purpose of this research is to:

The purpose of this research is to:

- Evaluate the *"security service environment"* with reference to the status quo and the nature and extent of problems being experienced in the collection and analysis of security information and the implementation of security risk control measures.
- Explore literature and other sources to discover new knowledge that can be used to improve the existing methods of collection and analysis of security information and the implementation of security risk control measures.;
- Apply the collected knowledge by formulating and developing recommendations with specific reference to solutions which will enhance the performance of the security service providers (and their security personnel) in the collection and analysis of security information and the implementation of security risk control measures.

You are kindly requested to please answer all the questions that follow, 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 need any further verification or clarity of any other information, you can contact my supervisor Prof. Anthony Minnaar (Tel: 012-429 2160; Cell: 083 8949485; email: aminnaar@unisa.ac.za).

Thank you for your time and participation!

Mr DORAVAL GOVENDER Tel: (012 429-2164 Cell no: 082 8174111 Email: govend1@unisa.ac.za

APPENDIX 1: INTERVIEW GUIDE USED FOR SEMI-STRUCTURED INTERVIEWS

AN EVALUATION OF THE COLLECTION AND ANALYSIS OF SECURITY INFORMATION AND THE IMPLEMENTATION OF SECURITY RISK CONTROL MEASURES IN THE SECURITY INDUSTRY IN GAUTENG, SOUTH AFRICA

SECTION A: Collection of Security Information

1. Do you have a policy for the collection of security information in your organisation/company?
2. Who are tasked to collect security information in your organisation/company?
3. What steps are followed for the collection of security information in your organisation/company?
4. What sources are used for the collection of security information in your organization/company?
5. What collection method/s does your organisation/company use to collect security information?
6. What types of security information are commonly collected in your organisation/company?
7. What levels of classification are commonly used for the protection of security information in your organisation/company?
8. What are the advantages of collecting security information in your organisation/company?
9. What are the disadvantages of collecting security information in your organisation/company?
10. What problems are experienced in the collection of security information in your organisation/company?
11. What solutions do you suggest to overcome the problems in the collection of security information in your organisation/company?

SECTION B: Analysis of Security Information

12. Do you have a policy for the analysis of security information in your organisation/company?
13. How is security information analysed in your organisation/company?
14. What steps do you follow in the analysis of security information in your organisation/company?
15. Which analysis products are commonly used by your organisation/company?
16. What are the advantages of analysing security information in your organisation/company?
17. What are the disadvantages of analysing security information in your organisation/company?

18. What problems are experienced in the analysis of security information in your organisation/company?
19. What solutions do you suggest to overcome the problems in the analysis of security information in your organisation/company?

SECTION C: Implementation of security risk control measures

20. Do you have a policy for the implementation of security risk control measures in your organisation/company?
21. How is security risk control measures applied in your organization/company?
22. Who are the intended users of the security risk control measures in your organisation/company?
23. How are the recommendations for the implementation of security risk control measures disseminated in your organisation/company?
24. Do you get feedback on the implementation of security risk control measures in your organisation/company?
25. What are the advantages of the implementation of security risk control measures for your organisation/company?
26. What are the disadvantages of the implementation of security risk control measures for your organisation/company?
27. What problems are experienced in the implementation of security risk control measures in your organisation/company?
28. What solutions do you suggest to overcome the problems in the implementation of security risk control measures in your organisation/company?

SECTION D: General

29. Is there any other matters on the collection and analysis of security information and the implementation of security risk control measures you want to discuss?

Thank you for answering my questions.

Reference number of respondent**.....** Date**.....**

APPENDIX 2: CONSENT FORM USED TO CONDUCT INTERVIEWS

CONSENT FORM

I, _____ (Name of respondent. PLEASE print legibly) Hereby agree to freely and voluntarily participate in the following DLitt et Phil (doctorate) studies research project:

TITLE: "**AN EVALUATION OF THE COLLECTION AND ANALYSIS OF SECURITY INFORMATION AND THE IMPLEMENTATION OF SECURITY RISK CONTROL MEASURES IN THE SECURITY INDUSTRY IN GAUTENG, SOUTH AFRICA".**

1. By participating in the interview YES NO
2. By granting permission to be audio taped YES NO
3. By agreeing that the information I provide may be YES NO used in the research report

I, **Doraval Govender** hereby agree to treat all information received from the respondent in a confidential manner and to preserve his/her anonymity (i.e. identity will NOT be divulged).

Signed at Date: _____ _____

Signature of respondent: _____

Signature of researcher: _____

APPENDIX 3: PERMISSION REQUEST LETTER TO CONDUCT RESEARCH AT SAPS

SECURITY SCIENCE PROGRAMME
(incorporating Security Risk Management)
DEPT. OF CRIMINOLOGY & SECURITY SCIENCE
SCHOOL OF CRIMINAL JUSTICE, COLLEGE OF LAW
Prof. A.deV. Minnaar
Tel: (+27) (0)12-429 2160 Cell: 0838949485
Fax: (+27)(0)12-429 6609 Fax2email: 0865190625
e-mail: aminnaar@unisa.ac.za

Muckleneuk Campus
Preller St
Muckleneuk Ridge, Pretoria
PO Box 392
UNISA 0003
City of Tshwane
Gauteng, South Africa

18 February 2010

Mr Johan Schnetler
Head: Strategic Management (Research)
South African Police Service
PRETORIA
0001

Dear Mr Schnetler

RE: REQUEST FOR PERMISSION TO CONDUCT RESEARCH IN SAPS FOR PHD STUDIES

Mr **DORAVAL GOVENDER**, is currently busy with research for a DLitt et Phil (doctorate) registered with the University of South Africa (UNISA) (Department of Criminology & Security Science, School of Criminal Justice, College of Law). His research title is: ***AN INVESTIGATION OF THE COLLECTION, ANALYSIS AND UTILISATION OF SECURITY RISK INFORMATION IN GAUTENG.***

As part of his research for his doctoral studies Mr Govender would like to undertake research on the SAPS' Crime Information Analysis Centre (CIAC) as a comparative case study for the best practices used in the collection, analysis and utilisation of security risk information by the CIAC. In support of the application, I attach a copy of the approved research proposal.

Accordingly we hereby request permission and your written approval to conduct this case study.

Thanking you
Regards

(Prof)
A. de V. Minnaar
Programme Head: Security Science
Department of Criminology & Security Science
School of Criminal Justice, College of Law

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone +27 12 429 3111 Facsimile +27 12 429 4150
www.unisa.ac.za

APPENDIX 4: APPROVAL TO CONDUCT RESEARCH IN THE SAPS

South African Police Service | Suid-Afrikaanse Polisiediens

Private Bag X301
Privaatsak X301

E-mail:
E-pos: MdluliRichard@saps.org.za

DIVISIONAL COMMISSIONER
CRIME INTELLIGENCE
AFDELINGSKOMMISSARIS
MISDAADINTELLIGENSIE
PRETORIA
0001

Your reference / U verwysing:

My reference / My verwysing: 3/21/3

Enquiries / Navrae: Lieutenant General R.N. Mdluli
Lt. Colonel N.A. Zonke

Tel: (012) 360-1408

Fax/Faks (012) 347-8661

2010-08-23

The Component Head
STRATEGIC MANAGEMENT

RESEARCH PROPOSAL: AN INVESTIGATION OF THE COLLECTION, ANALYSIS AND UTILISATION OF SECURITY INFORMATION IN GAUTENG: MR DOROVAL GOVENDER

1. Your email dated 20 August 2010 refers

2. Kindly be informed that approval for the proposed research on the above mentioned area is hereby granted.

3. However due to the sensitive nature of the Crime Intelligence environment, the research will be limited to unrestricted information. Component Heads within Crime Intelligence will avail themselves to provide the necessary assistance.

Regards,

LIEUTENANT GENERAL
DIVISIONAL COMMISSIONER: CRIME INTELLIGENCE
RN MDLULI (SOE)

CONFIDENTIAL

APPENDIX 5: INTERVIEW GUIDE USED FOR FOCUS GROUP INTERVIEWS

COVER LETTER

UNISA

PO BOX 392

PRETORIA 0003

Dear Participant/Respondent

PARTICIPATION IN RESEARCH PROJECT: FOCUS GROUP INTERVIEWS

I am currently a student in the Department of Criminology & Security Science, School of Criminal Justice at the University of South Africa (UNISA), busy with my studies for a ***DLITT et PHIL*** (doctorate) degree in Criminology (Security Risk Management). My research title is "***AN EVALUATION OF THE COLLECTION AND ANALYSIS OF SECURITY INFORMATION AND THE IMPLEMENTATION OF SECURITY RISK CONTROL MEASURES IN THE SECURITY INDUSTRY IN GAUTENG, SOUTH AFRICA".***

I will be conducting a focus group interview with you on the collection and analysis of security information and the implementation of security risk control measures. The focus group interview should take about an hour.

The purpose of this research is to:

- Evaluate the *"security service environment"* with reference to the status quo and the nature and extent of problems being experienced in the collection and analysis of security information and the implementation of security risk control measures.
- Explore literature and other sources to discover new knowledge that can be used to improve the existing methods of collection and analysis of security information and the implementation of security risk control measures.
- Apply the collected knowledge by formulating and developing recommendations with specific reference to solutions which will enhance the performance of the security service providers (and their security personnel) in the collection and analysis of security information and the implementation of security risk control measures.

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. Anthony Minnaar (Tel: 012-429 2160; Cell: 083 8949485; email: aminnaar@unisa.ac.za).

Thank you for your time and participation!

Mr DORAVAL GOVENDER Tel: (012 429-2164 Cell no: 082 8174111 Email: govend1@unisa.ac.za

APPENDIX 5: INTERVIEW GUIDE USED FOR FOCUS GROUP INTERVIEWS

FOCUS GROUP INTERVIEW GUIDE

AN EVALUATION OF THE COLLECTION AND ANALYSIS OF SECURITY INFORMATION AND THE IMPLEMENTATION OF SECURITY RISK CONTROL MEASURES IN THE SECURITY INDUSTRY IN GAUTENG, SOUTH AFRICA

SECTION A: Collection of Security Information

1. Do you have a policy for the collection of security information in your organisation/company?
2. Who are tasked to collect security information in your organisation/company?
3. What steps are followed for the collection of security information in your organisation/company?
4. What sources are used for the collection of security information in your organization/company?
5. What collection method/s does your organisation/company use to collect security information?
6. What types of security information are commonly collected in your organisation/company?
7. What levels of classification are commonly used for the protection of security information in your organisation/company?
8. What are the advantages of collecting security information in your organisation/company?
9. What are the disadvantages of collecting security information in your organisation/company?
10. What problems are experienced in the collection of security information in your organisation/company?
11. What solutions do you suggest to overcome the problems in the collection of security information in your organisation/company?

SECTION B: Analysis of Security Information

12. Do you have a policy for the analysis of security information in your organisation/company?
13. How is security information analysed in your organisation/company?
14. What steps do you follow in the analysis of security information in your organisation/company?
15. Which analysis products are commonly used by your organisation/company?
16. What are the advantages of analysing security information in your organisation/company?
17. What are the disadvantages of analysing security information in your organisation/company?
18. What problems are experienced in the analysis of security information in your organisation/company?
19. What solutions do you suggest to overcome the problems in the analysis of security information in your organisation/company?

SECTION C: Implementation of of security risk control measures

20. Do you have a policy for the implementation of security risk control measures in your organisation/company?
21. How is security risk control measures implemented in your organization/company?
22. Who are the intended users of the security risk control measures in your organisation/company?
23. How are the recommendations for the implementation of security risk control measures disseminated in your organisation/company?
24. Do you get feedback on the implementation of security risk control measures in your organisation/company?
25. What are the advantages of the implementation of security risk control measures for your organisation/company?
26. What are the disadvantages of the implementation of security risk control measures for your organisation/company?
27. What problems are experienced in the implementation of security risk control measures in your organisation/company?
28. What solutions do you suggest to overcome the problems in the implementation of security risk control measures in your organisation/company?

SECTION D: General

29. Is there any other matters on the collection and analysis of security information and the implementation of security risk control measures you want to discuss?

Thank you for answering my questions.

APPENDIX 6: PERMISSION REQUEST LETTER TO CONDUCT RESEARCH AT SABRIC

SECURITY SCIENCE PROGRAMME
(incorporating Security Risk Management)
DEPT. OF CRIMINOLOGY & SECURITY SCIENCE
SCHOOL OF CRIMINAL JUSTICE, COLLEGE OF LAW
Prof. A.deV. Minnaar
Tel: (+27) (0)12-429 2160 Cell: 0838949485
Fax: (+27)(0)12-429 6609 Fax2email: 0865190625
e-mail: aminnaar@unisa.ac.za

Muckleneuk Campus
Preller St
Muckleneuk Ridge, Pretoria
PO Box 392
UNISA 0003
City of Tshwane
Gauteng, South Africa

18 February 2010

Ms Kalyani Pillay
CEO: SABRIC
PO Box 3682
Halfway House 1685
GAUTENG, MIDRAND

Dear Ms Pillay

RE: REQUEST FOR PERMISSION TO CONDUCT RESEARCH ON SABRIC FOR PHD STUDIES

Mr **DORAVAL GOVENDER**, is currently busy with research for a DLitt et Phil (doctorate) registered with the University of South Africa (UNISA) (Department of Criminology & Security Science, School of Criminal Justice, College of Law). His research title is: ***AN INVESTIGATION OF THE COLLECTION, ANALYSIS AND UTILISATION OF SECURITY RISK INFORMATION IN GAUTENG.***

As part of his research Mr Govender would like to undertake research on a case study on the best practices used in the collection, analysis and utilisation of security risk information by SABRIC. In support of the application, I attach a copy of the approved research proposal.

Accordingly we hereby request permission and your written approval to conduct this case study.

Thanking you
Regards

(Prof)
A. de V. Minnaar
Programme Head: Security Science
Department of Criminology & Security Science
School of Criminal Justice, College of Law

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone +27 12 429 3111 Facsimile +27 12 429 4150
www.unisa.ac.za

APPENDIX 7: APPROVAL TO CONDUCT RESEARCH AT SABRIC

sabric

Making South African banking safe, secure and fraud free

16 April 2010

Department of Criminology and Security Science
UNISA

Your Ref:
File Ref
Direct Tel No. 011 847 3105
Direct e-mail

Dear Sir/Madam

ACCESS TO SABRIC INFORMATION FOR RESEARCH PURPOSES: DOROVAL GOVENDER

A research proposal was received from student number 05383640; Doroval Govender. Titled an "Investigation of the Collection, Analysis and Utilisation of Security Risk Information in Gauteng, SA".

The aim of the research is to evaluate the current situation in the security service environment, with reference to the nature and extent of problems experienced in the collection, analysis and utilisation of security risk information by security service providers.

SABRIC hereby gives Mr Doroval Govender permission to conduct the research and undertakes to assist him with relevant information pertaining the functioning of SABRIC in terms of collection, analysis and utilisation of security risk information to be used in the case study.

The SABRIC information will be provided on condition that the same may only be used for the purposes of the case study, and that SABRIC is permitted to review this information before the thesis is submitted for examination.

Reg No 2002/017376/08
Building 14 Thornhill Office Park
94 Bekker Road
Midrand
P.O. Box 2682
Halfway House, 1685
T +27 11 847 3000
F +27 11 847 3001
Website: www.sabric.co.za

In the event that submission of the thesis is successful, it is anticipated that SABRIC be provided with a copy thereof.

KALYANI PILLAY
CEO

APPENDIX 8: PERMISSION REQUEST LETTER TO CONDUCT RESEARCH AT CGRI

SECURITY SCIENCE PROGRAMME
(incorporating Security Risk Management)
DEPT. OF CRIMINOLOGY & SECURITY SCIENCE
SCHOOL OF CRIMINAL JUSTICE, COLLEGE OF LAW
Prof. A.deV. Minnaar
Tel: (+27) (0)12-429 2160 Cell: 0838949485
Fax: (+27)(0)12-429 6609 Fax2email: 0865190625
e-mail: aminnaar@unisa.ac.za

Muckleneuk Campus
Preller St
Muckleneuk Ridge, Pretoria
PO Box 392
UNISA 0003
City of Tshwane
Gauteng, South Africa

27 May 2010

Mr Michael Broughton
Manager: Crime Prevention Programme
Consumer Goods Council (CGCSA)
PO Box 41417
Craighall 2024

CC: Mr James Oosthuizen
Manager: Crime Prevention Strategies
Consumer Goods Council (CGC)

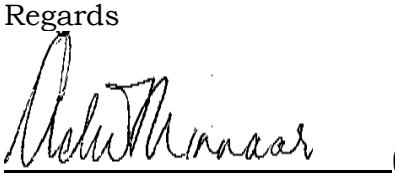
Dear Mr Broughton

RE: REQUEST FOR PERMISSION TO CONDUCT RESEARCH ON CONSUMER GOODS COUNCIL of SOUTH AFRICA (CGCSA) FOR PHD STUDIES

Mr **DORAVAL GOVENDER**, is currently busy with research for a DLitt et Phil (doctorate) registered with the University of South Africa (UNISA) (Department of Criminology & Security Science, School of Criminal Justice, College of Law). His research title is: ***AN INVESTIGATION OF THE COLLECTION, ANALYSIS AND UTILISATION OF SECURITY RISK INFORMATION IN GAUTENG.***

As part of his research Mr Govender would like to undertake research on a case study on the best practices used in the collection, analysis and utilisation of security risk information by the Consumer Goods Council (CGCSA). In support of the application, I attach a copy of the approved research proposal.

Accordingly we hereby request permission and your written approval to conduct this case study research on the CGCSA.
Thanking you
Regards



(Prof)
A. de V. Minnaar
Programme Head: Security Science
Department of Criminology & Security Science
School of Criminal Justice, College of Law

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone +27 12 429 3111 Facsimile +27 12 429 4150
www.unisa.ac.za

APPENDIX 9: APPROVAL TO CONDUCT RESEARCH AT CGRI

consumer goods council of south africa

Prof. A. de V. Minnaar
Programme Head: Security Science
Security Science Programme
Dept. of Criminology & Security Science School of Criminal Justice, College of Law
Muckleneuk Campus
Preller Street
Muckleneuk, Pretoria

1 June 2010

Dear Prof Minnaar,

Re: Permission to conduct research on Consumer Goods Council of South Africa's Crime Prevention Programme for PHD Studies.

As per your request in your letter dated 27th May 2010, and your discussion with James Oosthuizen in a meeting on 28th May 2010; I hereby permit you to conduct research on CGCSA Crime Prevention Programme.

Kindly inform us of the dates in which you'd like to conduct this research and the subject matter that it entails so we can ensure the information is available.

Should you have any further queries, please do not hesitate to contact me.

Yours sincerely

Michael Broughton
Director
CGC Crime Prevention Programme

Consumer Goods Council of South Africa
Block B, Hurlingham Office Park, Woodlands Avenue, Hurlingham Manor, 2196
Tel: +27 (0) 11 789 5777
Fax: +27 (0) 11 515 0066
e-mail: mb@cgcsa.co.za
Web site: www.cgcsa.co.za

APPENDIX 10: PERMISSION REQUEST LETTER TO CONDUCT RESEARCH AT PSI

SECURITY SCIENCE PROGRAMME
(incorporating Security Risk Management)
DEPT. OF CRIMINOLOGY & SECURITY SCIENCE
SCHOOL OF CRIMINAL JUSTICE, COLLEGE OF LAW
Prof. A.deV. Minnaar
Tel: (+27) (0)12-429 2160 Cell: 0838949485
Fax: (+27)(0)12-429 6609 Fax2email: 0865190625
e-mail: aminnaar@unisa.ac.za

Muckleneuk Campus
Preller St
Muckleneuk Ridge, Pretoria
PO Box 392
UNISA 0003
City of Tshwane
Gauteng, South Africa

27 May 2010

Mr M. Myburgh
Manager: Security & Crime Prevention
c/o South African Petroleum Industry Association (SAPIA)
PO Box 783482
Sandton 2146
South Africa

Dear Mr Myburgh

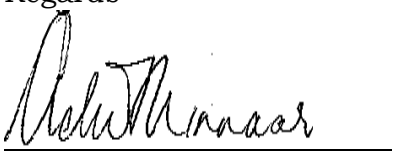
RE: REQUEST FOR PERMISSION TO CONDUCT RESEARCH ON THE SOUTH AFRICAN PETROLEUM INDUSTRY ASSOCIATION (SAPIA) FOR PHD STUDIES

Mr **DORAVAL GOVENDER**, is currently busy with research for a DLitt et Phil (doctorate) registered with the University of South Africa (UNISA) (Department of Criminology & Security Science, School of Criminal Justice, College of Law). His research title is: ***AN INVESTIGATION OF THE COLLECTION, ANALYSIS AND UTILISATION OF SECURITY RISK INFORMATION IN GAUTENG.***

As part of his research Mr Govender would like to undertake research on a case study on the best practices used in the collection, analysis and utilisation of security risk information by the South African Petroleum Industry Association (SAPIA). In support of the application, I attach a copy of the approved research proposal.

Accordingly we hereby request permission and your written approval to conduct this case study research on SAPIA.

Thanking you
Regards



(Prof)
A. de V. Minnaar
Programme Head: Security Science
Department of Criminology & Security Science
School of Criminal Justice, College of Law

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone +27 12 429 3111 Facsimile +27 12 429 4150
www.unisa.ac.za

APPENDIX 11: APPROVAL TO CONDUCT RESEARCH AT PSI

Govender, Doraval

From: Minnaar, Anthony
Sent: 07 June 2010 13:04
To: Govender, Doraval
Subject: FW: Permission letter to conduct research on SAPIA?

From: Mossie Myburg [mailto:mossiem@absamail.co.za]
Sent: Friday, June 04, 2010 3:40 PM
To: Minnaar, Anthony
Subject: RE: Permission letter to conduct research on SAPIA?

Dear Prof Minnaar,

Your request has been referred to the Director of SAPIA, Mr Avhapfani Tshifularo, who responded by approving the concept for the research. He did however, requested me to interview the student. He also insist on approval of the final product before publishing.

In liaising with some of the Oil Companies they requested

- that all information should be treated as confidential and therefore the applicant should sign a confidentiality agreement.
- The final product should also not be an open source document.
- The competition act has an important influence on these type of interventions and therefore a proper analysis of the act should form a part of the study.
- In the application document reference was made to investigations. It might be of value to take cognisance of the fact that SABRIC, CGC, PSI and various other industry representative bodies do not undertake any investigations but rather support the authorities to be more effective
- It was also noted that no mention was made to comparative studies in other industries.

Your student is welcome to make contact.

Kind regards,

Mossie Myburg

Security Consultant
Petroleum Security Initiative

Tel +27 12 361 6416
Fax +27 12 544 0601
Mobile +27 82 784 6824

mossiem@absamail.co.za

psi Petroleum Security Initiative

APPENDIX 12: PERMISSION REQUEST LETTER TO CONDUCT RESEARCH IN PERTH, WESTERN AUSTRALIA

SECURITY SCIENCE PROGRAMME
(incorporating Security Risk Management)
DEPT. OF CRIMINOLOGY & SECURITY SCIENCE
SCHOOL OF CRIMINAL JUSTICE, COLLEGE OF LAW
Prof. A.deV. Minnaar
Tel: (+27) (0)12-429 2160 Cell: 0838949485
Fax: (+27)(0)12-429 6609 Fax2email: 0865190625
e-mail: aminnaar@unisa.ac.za

Muckleneuk Campus
Preller St
Muckleneuk Ridge, Pretoria
PO Box 392
UNISA 0003
City of Tshwane
Gauteng, South Africa

21 January 2011

Dr David Brooks
School of Computing & Security Science
Edith Cowan University
Joondalup, Perth
Western Australia

Dear Dr Brooks

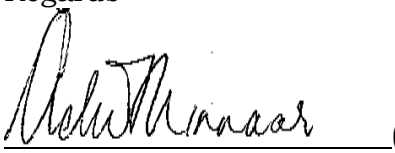
RE: REQUEST FOR RESEARCH SUPPORT DURING MR D. GOVENDER'S RESEARCH TRIP TO ECU, 8-29 MAY 2011

As discussed with you please see below the detailed information and formal request for assistance from you and ECU for Mr Govender's Phd research studies.

Mr **DORAVAL GOVENDER**, is currently busy with research for a DLitt et Phil (doctorate) registered with the University of South Africa (UNISA) (Department of Criminology & Security Science, School of Criminal Justice, College of Law). His research title is: ***AN INVESTIGATION OF THE COLLECTION, ANALYSIS AND UTILISATION OF SECURITY RISK INFORMATION IN GAUTENG.***

As part of his research Mr Govender would like to undertake research interviews, focusing on the best practices used in the collection, analysis and utilisation of security risk information by security practitioners in Western Australia. In addition, he would like your assistance in identifying suitable persons/practitioners and the setting up of such meetings during the period (8-29 May 2011) he will be spending in Western Australia based at your Department. In support of this request, please find attached a copy of the approved research proposal.

Thanking you
Regards



(Prof)
A. de V. Minnaar
Programme Head: Security Science
Department of Criminology & Security Science
School of Criminal Justice, College of Law

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone +27 12 429 3111 Facsimile +27 12 429 4150
www.unisa.ac.za

APPENDIX 13: APPROVAL TO CONDUCT RESEARCH IN PERTH, WESTERN AUSTRALIA

SECAU
Securing Australia's Future

ECU
EDITH COWAN UNIVERSITY

JOONDALUP CAMPUS
270 Joondalup Drive,
Joondalup
Western Australia 6027
Telephone 134 328
Facsimile (08) 9300 1237
CRICOS 00279B
ABN 54 361 485 361

DATE: 28th January 2011
REF: Mr. DORAVAL GOVENDER
Staff No.: 90162749
ID: 5802245124084
Passport No.: 477034122

TO WHOM IT MAY CONCERN

I hereby confirm that Mr. DORAVAL GOVENDER will be visiting Edith Cowan University for a research trip to Perth, Australia, from the 8th May to 29th May 2011. The purpose of the proposed research trip is to undertake research meetings and interviews for a current research project (Phd studies).

The project is titled: An investigation of the collection, analysis and utilisation of security risk information in Gauteng, South Africa. During this period, Mr. Govender will be hosted by the School of Computing and Security Science at Edith Cowan University.

It is my understanding that the full cost for the research visit to Australia will be borne by the University of South Africa (UNISA), South Africa.

Yours Sincerely

Dave Brooks

Dr. David Brooks
Chief Investigator
Security Research Centre (secau)
Edith Cowan University
Phone: (61 8) 6304 5788
Email: d.brooks@ecu.edu.au

ACS Centre of Expertise - Security

APPENDIX 14: SELF-ADMINISTERED QUESTIONNAIRE USED IN QUANTITATIVE SURVEY

QUESTIONNAIRE SURVEY: SECURITY SERVICE PERSONNEL

RESEARCH PROJECT: *AN EVALUATION OF THE COLLECTION AND ANALYSIS OF SECURITY INFORMATION AND THE IMPLEMENTATION OF SECURITY RISK CONTROL MEASURES IN THE SECURITY INDUSTRY, IN GAUTENG, SOUTH AFRICA*

Instructions:

Please answer all the questions as honestly as possible. The information collected for this study will be collated and analysed in order to form an accurate picture of this research project on the collection and analysis of security information and the implementation of security risk control measures in Gauteng, South Africa. It will assist the researcher to make findings and propose recommendations to improve security information management in the security industry. You do not need to identify yourself and, similarly, the researcher will uphold anonymity in that there will be no possibility of any respondent being identified or linked in any way to the research findings in the final research report. Where required please indicate your answer with a cross (X) in the appropriate box or write a response in the space provided, using a black ballpoint pen. For the open-ended questions, please write your responses clearly and legibly in the space provided. If there is not sufficient space for your response please number a blank sheet of paper with the question number and continue writing your response on the extra piece of paper.

SECTION A: (Demographic details)

Indicate your choice by marking the appropriate selected blank block with an "X".

The following questions are **for statistical purposes only**.

1. Gender:

Male	1	
Female	2	

2. Age:

16–20 years	1	
21–25 years	2	
26–30 years	3	
31–35 years	4	
36–40 years	5	
41–45 years	6	
46–50 years	7	
51 years and above	8	

3. Race:

Indian	1	
Asian (other than Indian)	2	
Black	3	
Coloured	4	
White	5	

4. Educational qualification:

Standard 8/Grade 10 and below	1	
Standard 9/Grade 11	2	
Standard 10/Grade 12	3	
Certificate	4	
Diploma (1 year)	5	
Diploma (2 years)	6	
Diploma (3 years)	7	
Advanced diploma	8	
Degree	9	
Postgraduate degree	10	

SECTION B: (Security service details)

Indicate your choice by marking the appropriate selected blank block with an "X".

5. Security service working experience in the private security industry:

1 year and below	1	
1–2 years	2	
2–3 years	3	
3–4 years	4	
4–5 years	5	
5–10 years	6	
10 years and above	7	

6. Security service position occupied at present:

Security guard	1	
Patrol officer	2	
Investigator	3	
Security officer	4	
Administration official	5	
Trainer	6	
Supervisor	7	
Manager	8	
Other (Specify)		
	9	

7. Security service work with which you are involved at present:

Protecting or safeguarding a person or property	1	
Giving advice on the protection or safeguarding of a person or property, on any type of security service, or on the use of security equipment	2	
Providing a reactive or responsive service in connection with the safeguarding of a person or property	3	
Providing a service aimed at ensuring order and safety on the premises used for sporting, recreational, entertainment or similar purposes	4	
Manufacturing, importing, distributing or advertising monitoring devices contemplated in section 1 of the Interception and Monitoring Prohibition Act 127 of 1992	5	
Performing the functions of an investigator	6	
Providing security training or instruction to a security service provider	7	
Installing, servicing or repairing security equipment	8	
Monitoring signals of transmissions from electronic security equipment	9	
Performing the functions of a locksmith	10	
Making a person or the services of a person available, whether directly or indirectly, for the rendering of any security service	11	
Managing, controlling or supervising the rendering of any security-related services	12	
Control room operator	13	
Other (Specify)		
	14	
	15	

8. Security service sector with which you are involved at present (mark one):

City and metropolitan councils	1	
Transport services (rail, road, marine, aviation)	2	
Public services entities (Telkom, Eskom, post office, hospitals, other parastatals)	3	
Protection services (military, air force, intelligence services, correctional services, other government departments)	4	
Financial and insurance institutions	5	
Industrial sector	6	
Mining sector	7	
Retail sectors (shops, casinos, shopping centres and hotels)	8	
Private security contract companies	9	
In-house security (university, complex, etc.)	10	
Other (Specify)		
	11	
	12	

9. Security service training which you have undergone:

Patrol security officer (grade E)	1	
Access control officer (grade D)	2	
Asset and reaction officer (grade C)	3	
Security first-line supervision (grade B)	4	
Security supervisor (grade A)	5	
Risk management (risk analysis, security survey, risk assessment)	6	
Security threat assessment	7	
Firearm handling	8	
Emergency preparedness training	9	
Fire risk assessment training	10	

Occupational health and safety training	11	
Specialised security training	12	
Specialised investigation training	13	
Collection of security risk information	14	
Analysis of security risk information	15	
Utilisation of security risk information	16	
Intelligence training	17	
Other (Specify)		
	18	
	19	
	20	

SECTION C: (Collection of security information)

Mark with a cross (x) either the "Agree" or "Do not agree" block at each response option.

	Agree	Do not agree
10. "Security information" relates to information which may expose an individual/group or a stable, relatively predictable environment to the chance or probability of injury or loss.	1	2
11. "Collection (gathering)" is the act of gathering information that will be used to mitigate security risks.	1	2
12. "Overt means (open source techniques)" of collecting security information takes place inter alia through personal interaction with people (complainants, witnesses, victims, suspects, law enforcement personnel, clients and the general public), public agencies and institutions, mass media (internet, television, radio, literature, newspapers, academic public reports), public databases, maps, government public information, libraries, private companies, scenes of crimes/incidents.	1	2
13. "Covert means (closed source techniques)" of collecting security information takes place through agents, agent handlers, informants, surveillance officers, undercover operatives, monitoring and interception personnel, etc.	1	2
14. "Internal security information sources" include pocket book entries, occurrence book entries, statements, risk analysis reports, security survey reports, security risk solutions reports, security risk management reports, approved security measures reports, investigation reports, crime incident reports, loss reports, field interview report cards, suspicious activity reports, forensic reports, fingerprint reports, selected calls for service, arrest reports, traffic citations, admissions from arrestees, intelligence files, etc.	1	2
15. "External security information sources" include incident database reports under the control of other institutions and agencies, for example banks, government departments, private security providers, informers, the mass media, embassies, the public, community police forums, the e-natis database, cellphone providers, etc.	1	2
16. "Collection plan" is a formally defined approach, describing the information needed and the means of acquiring it.	1	2

Indicate your choice by marking the appropriate selected blank block with an "X".

17. How do you regard your knowledge about the collection of security information?

Excellent	1	
Good	2	
Average	3	
Poor	4	
Very poor	5	

18. Do you need permission from your supervisor/manager to collect security information on behalf of your organisation/company?

Yes		No	
1		2	

19. Do you understand the steps to be followed when collecting security information?

Yes		No	
1		2	

20. In the space provided, outline all the steps to be followed when collecting security information.

……

……

Indicate your choice by marking the appropriate selected blank block with an "X".

21. Have you previously collected security information?

Yes		No	
1		2	

22. Do you collect security information whenever a situation presents itself?

Yes		No	
1		2	

23. Have you previously collected security information by making use of a 'collection plan'?

Yes		No	
1		2	

24. If you answered "Yes" to question 23, what kind of collection plan did you use?

……

Indicate your choice by marking the appropriate selected blank block with an "X".

25. Please indicate if you have previously received security information in any of the following situations?

Voluntary information from a third party	1	
Information about a crime/incident from a victim/complainant	2	
Information while investigating a crime/incident	3	
Information while at a crime/incident scene from observers	4	
Information from informants	5	
Information through interaction with clients	6	
Information through interaction with personnel	7	
Information through interaction with the general public	8	
Information while investigating a suspicious activity report	9	
Forums (explosives, illegal mining forum, illegal special metals forum)	10	
Other (Specify)		
	11	
	12	
	13	
	14	

26. Please indicate if you have previously used any of the following method/s to gather security information:

Physical surveillance (observation, tailing, etc.)	1	
Electronic surveillance (cameras, biometrics, hi-tech, etc.)	2	
Research (external sources for example South African police, Home affairs, etc.)	3	
Internal audit (internal sources for example risk analysis, security survey, etc.)	4	
Forensics	5	
Undercover	6	
Interviews (briefing, debriefing, etc.)	7	
Interrogations	8	
Hacking into computer databases for information	9	
Other (Specify)		
	10	
	11	

27. In the past month, how many times did you personally collect security information?

0	1	
1–5 times	2	
6–10 times	3	
11–20 times	4	
Over 20 times	5	

28. Please indicate the type of security information you personally collected during the past month:

Crime threats	1	
Company policy breaches/violations, etc.	2	
Physical security breaches	3	
Electronic security breaches	4	
Other (Specify)		
	5	
	6	

29. Please indicate the item that best describes how you handled the collected security information:

Informed immediate manager/supervisor	1	
Informed the unit that handles all collected information	2	
Informed the analysis unit	3	
Informed the investigation unit	4	
Entered the information into an electronic database (computer)	5	
Recorded information in the control room OB	6	
Recorded information in personal pocket book	7	
Recorded information in an incident register	8	
Informed the supervisor on the duty parade	9	
Utilised information to perform task	10	
Forwarded the information to law enforcement	11	
Forwarded the information to human resource management for disciplinary investigations	12	
Did nothing with the information	13	
Other (Specify)		
	14	

30. Are there security measures in place in your organisation/company for the protection of information (data)?

Yes		No	
1		2	

31. If you answered "Yes" to question 30 please indicate which of the following information (data) protection measures are being used by your organisation/company:

Information Protection Act	1	
Minimum Information Security Standards (MISS) approved by Cabinet	2	
Organisation/company policy on the classification of information, for example confidential, secret, restricted	3	
Access to the information database is not allowed to employees below management	4	
Access is allowed on a need-to-know basis	5	
Access to Information Act	6	
Security clearance to access classified information	7	
Other (Specify)		
	8	
	9	

32. Does your organisation/company have the necessary resources to collect security information?

Yes		No	
1		2	

33. Does your organisation/company store the collected security information in a database?

Yes		No	
1		2	

34. If you answered "Yes" to question 33, in which database is the collected security information stored?

Electronic database (computer system)	1	
Manual database (handwritten in a register, document, etc.)	2	
Both electronically and manually	3	

35. If the collected security information is stored in a database (computer or manual), who is responsible for entering the data onto the database?

Self	1	
Data typist	2	
Data analyst	3	
Clerk	4	
Admin official	5	
Data administrator	6	
Investigating officer	7	
Supervisors	8	
Security managers	9	

36. Please indicate what kind of database the person indicated above inputs the information into:

	Computer		**Manual**		**Combination of both**	
Self	1		10		19	
Data typist	2		11		20	
Data analyst	3		12		21	
Clerk	4		13		22	
Admin official	5		14		23	
Data administrator	6		15		24	
Investigating officer	7		16		25	
Supervisors	8		17		26	
Security managers	9		18		27	

37. Do you ever get feedback from your supervisor/manager on the security information collected by you?

Yes		No	
1		2	

38. If you answered "Yes" to question 37, how frequently do you receive such feedback?

……

……

Indicate your choice by marking the appropriate selected blank block with an "X".

39. Have you previously experienced any problems in the collection of security information?

Yes		No	
1		2	

40. If you answered "Yes" to question 39, please indicate the nature and extent of the problems (shortcomings) experienced in the collection of security information.

……

……

41. What solutions do you suggest for solving the problems (shortcomings) you encountered as indicated in question 40?

……

……

Indicate your choice by marking the appropriate selected blank block with an "X".

42. Do you think the collection of security information can be improved in your organisation/company?

Yes		No	
1		2	

43. What recommendations do you suggest for improving the collection of security information in your organisation/company?

……

……

<u>SECTION D: (Analysis of security information)</u>

Mark with a cross (x) either the "Agree" or "Do not agree" block at each response option.

	Agree	**Do not agree**
44. "Evaluation (verification) of security information" is the assessment of the reliability of the source and the quality of the information.	1	2
45. "Collation of the security information" is the sorting, indexing and storing of information into a format from which it can be retrieved and analysed.	1	2

46. "Analysis of the security information" involves the careful examination of the information to discover its meaning and essential features.	1	2
47. "Operational analysis" provides day-to-day information to assist operational personnel in the identification of specific and immediate security risks. These include, but are not limited to, syndicate networks, individuals or groups involved in unlawful activities: methods used (modus operandi, or MO); specific details about the capabilities, limitations, vulnerabilities and intentions of the likely perpetrators; and their sources of support and finance.	1	2
48. "Strategic analysis" is concerned with long-range problems and projections of long-term increases or decreases in security risks. It provides the organisation/company with an overview of criminal capabilities, vulnerabilities, trends and intentions.	1	2

Indicate your choice by marking the appropriate selected blank block with an "X".

49. Have you previously evaluated (verified) security information?

Yes		No	
1		2	

50. Have you previously collated security information?

Yes		No	
1		2	

51. How do you regard your knowledge about the analysis of security information?

Excellent	1	
Good	2	
Average	3	
Poor	4	
Very poor	5	

52. Do you know how to analyse security information?

Yes		No	
1		2	

53. Have you previously analysed security information?

Yes		No	
1		2	

54. If you answered "Yes" to question 53, please indicate which of the following stages of the analysis process you have previously been involved with:

Identifying assets (people, material, legalities) deserving of protection	1	
Identifying the security risks to the assets	2	
Estimating the probability that security risks will materialise	3	
Estimating the impact of security risks occurrences	4	
Estimating the frequency of event occurrences	5	
Assessment of the manageability of security risks	6	
Identification of countermeasures that will prevent or mitigate security risks occurrences	7	

55. Who in your organisation/company is tasked by the analysts to obtain additional information to enrich the collected information?

Self	1	
Supervisors	2	
Security managers	3	
Risk managers	4	
Investigators	5	
Crime risk officers	6	
Collection unit	7	
Information/intelligence unit	8	

56. Have you previously experienced any problems in the analysis of security information?

Yes		No	
1		2	

57. If you answered "Yes" to question 56, please indicate the nature and extent of the problems (shortcomings) you encountered when analysing security information.

……

……

58. What solutions do you suggest for solving the problems (shortcomings) you encountered as indicated in question 57?

……

……

Indicate your choice by marking the appropriate selected blank block with an "X".

59. Do you think the analysis of security information can be improved in your organisation/company?

Yes		No	
1		2	

60. What recommendations do you suggest for improving the analysis of security information?

……

……

SECTION E: (Implementation of security risk control measures)

Mark with a cross (x) either the "Agree" or "Do not agree" block at each response option.

	Agree	Do not agree
61. "Dissemination" is the release of the "results of the analysis" to the intended user under certain conditions and protocols, usually based on the security classification of the information and the security clearance of the user.	1	2
62. "Implementation" refers to the use of the "results of the analysis" to target a specific security risk with the object of reducing or eliminating it.	1	2
63. "Strategic application" refers to the strategic application of the results of the analysis in order to allow for the formulation of organisational policies and plans to mitigate security risks.	1	2
64. "Operational application" is aimed at directly meeting the organisation/company objectives and responsibilities, by focusing on security risks, individuals and modus operandi.	1	2
65. "Feedback" is defined as information resulting from the establishment of formal and informal communication processes implemented to determine the accuracy, reliability, validity, timeliness and overall usefulness of the results of the analysis.	1	2
66. "Evaluation" is the cooperative review of the security risk to determine if it has been reduced or eliminated.	1	2

Indicate your choice by marking the appropriate selected blank block with an "X".

67. Indicate the "analysis result" provided to you:

Profiles	1	
Security assessments	2	
Target analysis reports	3	
Statistical analysis reports	4	
Crime analysis reports	5	
Security risk mitigating strategies/products	6	
Security awareness products	7	
Alerts	8	
Other (Specify)		
	9	
	10	

68. Indicate in what manner (way) the "analysis result" was communicated to you:

Briefings	1	
Meetings	2	
Handouts	3	
Reports	4	
Other (Specify)		
	5	

69. Have you previously encountered any problems in the communicating of the " analysis result " to you?

Yes		No	
1		2	

70. If you answered "Yes" to question 69, please indicate the nature and extent of the problems (shortcomings) experienced in the dissemination of the "analysis result" to you.

……

……

71. What solutions do you suggest for solving the problems (shortcomings) indicated in question 70?

……

……

Indicate your choice by marking the appropriate selected blank block with an "X".

72. Have you in the past provided feedback to the analysts on the implementation of the "analysis result" information provided (disseminated) to you?

Yes		No	
1		2	

73. If you answered "Yes" to question 72, please indicate the type of feedback you provided to the analysts.

Formal (feedback forms, etc.)	1	
Informal (informal discussions)	2	
Both (formal and informal)	3	
Other (Specify		
	4	
	5	
	6	

74. Have you previously experienced any problems (shortcomings) in the implementation of the "analysis result " that was provided to you?

Yes		No	
1		2	

75. If you answered "Yes" to question 74, please indicate the nature and extent of the problems (shortcomings) experienced in the implementation of the "analysis result".

……

……

76. What solutions do you suggest for solving the problems (shortcomings) indicated in question 75?

……

……

Indicate your choice by marking the appropriate selected blank block with an "X".

77. Do you think the implementation of security risk control measures can be improved in your organisation/company?

Yes		No	
1		2	

78. What recommendations do you suggest for improving the implementation of security risk control measures in your organisation/company?

……

……

SECTION F: (General)

79. Please indicate any other matters on the collection and analysis of security information and the implementation of security risk control measures you wish to discuss.

……

……

Thank you for answering my questions.

Reference number of respondent..... Date.....