INFORMATION MANAGEMENT STRATEGIES TO COMBAT CRIME AND PREVENT LOSSES

***Doraval Govender*[1]**

ABSTRACT

In South Africa, crime is becoming increasingly diverse, sophisticated and difficult to combat. Criminologists believe that specific knowledge, skills and attitudes are required to address crime, criminals and victims. Communities and businesses feel that the police is not coping with the rising crime. High levels of property related crimes have forced communities and business entities to provide for their own security. The terrorist attacks of 9/11 on the World Trade Centre in New York and the Pentagon in Washington have helped shape new policies, strategies and operations of policing agencies and private security services across the world. Poor crime information management was found to be the main weakness in policies, strategies and operations. Crime information and analysis were not considered to be important in the sequence of activities aimed at conceiving, implementing and evaluating measures to combat crime and preventing losses before 9/11 as the focus was on reactive policing. Practitioners have started to view crime information management and analysis from a new paradigm. The information environment has changed the approach of the security practitioner. Information management is now considered fundamental for decision-making and the formulation of security strategies. The aim of this article is to examine information management strategies that have been successfully used to combat crime and prevent losses.

INTRODUCTION

There is a feeling of insecurity and concern by both the citizenry and the business communities on the efforts being made specifically in South Africa of combating property related crimes (Van Rooyen, 2008: 1). Very little success seems to be achieved in combating these crimes. Operational strategies to combat such crimes and prevent losses do not seem to be working. The concerns are on the application and effectiveness of the strategies. The lack of intelligence driven operations based on information management strategies and the negative connotations associated with such practices continue to undermine the tradecraft of information and intelligence management (Ratcliffe, 2009: 5). Successful policing agencies and private security services place a high premium on information collection and analysis to combat crime and prevent losses. The sharing of intelligence and information is encouraged by upholding a culture of 'need to share' rather than a culture of 'need to know'. Hence, more emphasis is placed on value adding and integration of information than on information protection and classification. Law enforcement and private security are turning to fusion centres and war rooms to overcome over classification and excessive compartmentalisation of information among agencies (Ratcliffe 2009: 5). These fusion centres and war rooms are also used to operationally manage efforts to produce different types of information which can be used to drive policy, strategy, and operations at different levels. The role of the fusion centres and war rooms in the United States of America (USA) is to maintain situational awareness for response to current and future security issues (Ratcliffe, 2009: 26-27). According to Fischer, Halibozek and Green (2008:38), similar businesses and industries in the United States of America (USA) created central repositories of security risk information deemed important to all their shared interests nationwide and made it available in various ways to their separate groups. This encouraged information sharing at the highest levels of business.

[1] Dr, Senior Lecturer, Programme Security Management, Department of Criminology & Security Science, School of Criminal Justice, College of Law, University of South Africa. Email: Govend1@unisa. ac. za

Conventional thinking expects information management strategies and information sharing to lead the way for effective policing. This article is a discussion on the different information management strategies that may be successfully used to combat crime and prevent financial losses in South Africa.

RESEARCH METHODOLOGY

Literature, in-depth interviews and the experience of the author as the Area Commissioner/ Cluster commander/Station Commissioner in the South African Police Service was used to conduct this study. During 2011, in depth interviews were conducted with senior police officers from the SAPS and security managers from the private security companies. These persons were purposively sampled for the interviews because of their specialised knowledge and management role at police station level and in the private security companies.

Research objective

The objective of this empirical study was to examine among other things, the design, implementation and applicability of the different information management strategies that may be used to effectively and efficiently combat crime and prevent losses.

INFORMATION TO COMBAT CRIME AND PREVENT LOSSES

Critical to the success of any end user of information is the integrity and substantiality of information gathered. Intelligence officers, information gatherers and investigators need to master the use of information collection as well as analysis. What to look for and whom to ask are perennial issues for the investigator. Information is everywhere. The strategy is how to get it and be assured of its meaningfulness. Collecting the information largely depends upon accessibility to either persons or institutions. In the process of obtaining the information, the collector must respect the law and the fundamental tenets of privacy (Nemeth, 2010: 87). End users of information are interested in two types of information: information as knowledge and information as data. The distinction is an important one, because each one of these types has characteristics, which means that the techniques used to locate, gather and use them are different (Stelfox, 2009: 105).

Investigators must be able to identify those who know something about the offence and to manage the transfer of that knowledge information to the investigation. Investigators need to understand the depth of knowledge people have of an event to establish how to effectively use this in an investigation. Communication skills are key to the success and form the basis of the techniques of investigative interviewing. Knowledge information is obtained from victims and witnesses, suspects, informants, covert sources, surveillance, media and house to house enquiries (Stelfox, 2009:109). Forging complementary and tactful relationships with information sources mentioned above, the investigator will have access to an unlimited supply of information. Despite bureaucratic and legislative obstructions, an inquisitive person will eventually gain access to the desired information, even though the practice is legally incorrect. This can be achieved through networking and building contacts with the right people, employed in the right places (Nemeth, 2010: 91).

In relation to the information used as data, the issues are a great deal different. The difficulties facing investigators are mainly technical and concerned with the legality of gaining access to premises where data may be found or access to the data owned by others, such as financial records. The range of data is extensive and investigators must know the characteristics if they are to successfully locate, recover and use it. Information is obtained during searches, crime scene investigations, forensic investigations, CCTV, financial,

telephone data, and computer data (Stelfox, 2009: 109). With regards to data information, the investigator must know the standard of proof required for the investigation to be successful. The standard of proof will determine the resources necessary to obtain the specific data information. Although data information may seem sufficient by face value, it will still be necessary to interview the concerned subjects, as there may be a possibility that someone else used the subject's computer and left the data information question (Ferraro and Spain, 2006: 21).

According to the police officers who were interviewed, the police use knowledge based information to combat crime rather than data information. Data information is mainly used to obtain forensic evidence and compile crime statistics. Private security officers use data information which is obtained through security assessments, forensic investigations, CCTV monitoring, access control and incident registers to combat crime and prevent losses.

INFORMATION MANAGEMENT STRATEGIES

Information management strategies include the different ways in which information or intelligence may be managed and analysed to achieve a specific result. To stay ahead of trends, it is crucial for security practitioners (police officers and private security officers) to take a proactive approach towards security related information. For security information to be successfully managed, it is necessary that security information be lawfully collected, and analysed, using the correct analytical methods and then effectively applied as strategies to combat crime and prevent losses. The five information management strategies discussed below, relate to the collection of information or intelligence (whichever is tasked), analysis of the information or intelligence and the implementation of information or intelligence strategies to address uncertain future events that may influence the achievement of goals and objectives of the organisation.

Strategy 1: Problem-oriented policing

The problem-oriented policing approach is important to the development of information led policing. It has opened the eyes of a whole generation of security practitioners to the possibilities of using information from crime problems and analysis to develop operational strategies and solve problems. It looks at a specific and often local nature of a crime problem to determine the nature of the solution (Ratcliffe 2003: 70). According to Scott, (2000: 1), problem oriented policing has yielded many benefits for community policing. Problem oriented policing is important to the development of intelligence-led policing, because it has opened the eyes of a whole generation of police mangers to the possibility of doing crime information collection, and using crime analysis to form operational strategies and solve problems.

Over 60 prominent policing agencies internationally, including the South African Police Service have associated themselves with problem-oriented policing. Police practitioners from these agencies used the Scanning, Analysis, Response and Assessment **(**SARA) methodology to carry out problem oriented policing. SARA involves the following cycle:

- **Scanning:** identifying recurring problems and how the ensuing consequences affect community safety;

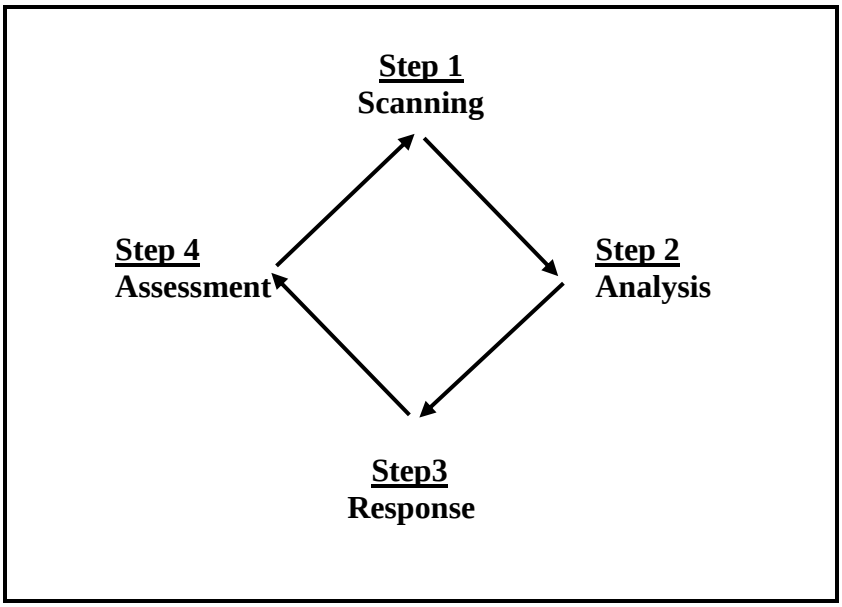
- **Analysis:** collecting and analysing relevant data on the problem, with the object of revealing ways to alter the causes of the problem;

- **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).

Scanning/Analysis/Response/Assessment (SARA) Methodology

Figure 1: SARA Model



(Source: Adapted from Ratcliffe 2003: 74).

According to police officers interviewed, this information led policing model (SARA) was used in South Africa prior to 1995 in the implementation of community policing. Private security officers interviewed during 2011 did not know of the SARA model and its implementation. They are of the view that this model could work if implemented in the private security environment to address security risks confronting assets.

Strategy 2: Intelligence-led policing

Intelligence-led policing is a collective name for a number of techniques that are neither generally used nor well known. These techniques are primarily proactive and are aimed at a person or organisation, rather than at the crime. Intelligence-led policing is used when normal investigations do not produce the desired results. The target is usually unaware of the fact that the police are engaged in an investigation against him or her (Marais, 2003:48).

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).

.

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).

The security officers, who were interviewed for this study, did not use intelligence led policing in the private security environment. According to the police officers interviewed, the South African Police implemented 'Intelligence led policing' in 1995. It was implemented to address organised crime syndicates. Crime analysts were used to identify problem crimes, using the crime pattern analysis matrix, generated through the automated crime reporting process known as the Crime Administration System (CAS). Once a crime problem, for example street robberies, has been identified, the crime analysis unit would be tasked to collect information on previous incidents of street robberies, the arrested persons, victims and the outcome of the adjudication process, using the docket analysis strategy. Intelligence is collected on the associates of the previously arrested street robbers, there different memberships and structures. This is done using overt and covert techniques to collect information/intelligence. The intelligence unit uses this information to develop a linkage analysis chart or an Association Network Analysis Chart (ANAC). The ANAC brings together all the associates of the identified perpetrator/s. It also links the perpetrator/s to specific activities and institutions. The ANAC assists the investigator to conduct a money or paper trail in organised crime investigations. The crime intelligence unit is an organisational structure with skilled personnel in the collection and analysis of crime information/intelligence. The analysis function will include the processing of a product for use by decision-makers.

Even with the ability of new ideas and innovation to spread throughout the policing world at the click of a mouse, there is still a lack of clarity among many security practitioners as to what intelligence-led policing is, what it aims to achieve, and how it is supposed to operate (Ratcliffe 2003: 1).

'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 National Intelligence Model (NIM) of the United Kingdom uses four elements for its tactical tasking in the implementation of intelligence-led policing. These elements includes:

- Targeting offenders (especially targeting of active criminals through overt and covert means)
- The management of crime and disorder hotspots;
- The 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 (NCIS, 2000: 14).

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 produces new information to be fed

back to the intelligence unit for new analysis (Newburn, Williamson & Wright, 2008: 203 and Ratcliffe, 2009: 105).

Direction to collect intelligence

The intelligence cycle starts with direction from decision-makers. A task is received to collect intelligence on a specific target. Collection involves accumulating information on targets from all available sources, including investigative reports; officers field reports, informants, open source documents, and government and court records (Police Chief: 1997: 49).

Apart from standard records of reported crimes, arrests and convictions, the most common form of raw material used by intelligence analysts consists of' 'intelligence logs' produced by other police officers. In many instances these are simply sightings of known offenders by patrol officers – pieces of information which on their own are of little use, but when put together with other information (for example, a spate of burglaries in a specific area at a specific time) may become valuable. Other logs may be based on information from a member of the public, passed on, for example, in conversations with patrol officers or through telephone calls to the police or schemes such as 'crime stoppers'. In addition information may be obtained from registered informants (Newburn et al. , 2008: 205).

While these are the 'traditional' sources of intelligence, recent years have seen an expansion in the range of source available, including regular supplies of information from other agencies (including correctional centres and probation officers, as well as non-criminal justice public and private sector organisations such as local councils, banks and building societies), in many cases facilitated by data sharing protocols (Newburn et al. , 2008: 205).

Evaluation

Once collected, the information must be evaluated. The analyst will examine the data, judging the validity of the information and the reliability of the sources (Police Chief: 1997: 49).

The information is evaluated as part of converting it to intelligence. Operationally this is crucial, in order to be as certain as possible that the information is accurate and that the source (particularly covert sources such as informants) can be relied upon. Law enforcement agencies who deal with intelligence have adopted the '5x5x5' system to evaluate information. This adds an additional dimension, known as a 'handling code' which regulates the dissemination of the information to other parties. This has been described by Sheptycki (2004: 12), as essentially a risk assessment for dissemination. The advantage of the '5x5x5' system is that it allows for the prioritisation of investigative resources according to the quality of the intelligence received. The '5x5x5' system may be described as follows:

Source evaluation

A	Always reliable
B	Mostly reliable
C	Sometimes reliable
D	Unreliable
E	Untested

Intelligence evaluation

1	Known to be true without reservation
2	Information known personally to the source but not to the reporting officer
3	Information is not known personally to the source, but there is corroboration by information already recorded
4	Information that is not known to the source and cannot be corroborated
5	Information that is suspected to be false

Handling code

Code 1	Permit dissemination to other law enforcement and prosecuting agencies (such as the benefits agency) including agencies abroad where there are sufficient safeguards to protect the rights of individuals
Code 2	Permits dissemination to non-prosecuting agencies (such as credit card companies)
Code 3	Permits dissemination to foreign agencies where no or inadequate, legal safeguards to protect the rights of individuals exist; however, this is only on the grounds of substantial public interest
Code 4	Permits dissemination only within originating agency /force with internal recipients
Code 5	Permits dissemination to other agencies but only in accord with specified conditions such as ‘ no further dissemination’ or ‘to be discussed with originator

(Source: Adapted from Shepycki, 2004: 11-12)

If intelligence is to be shared with colleagues or managers there is temptation for those who received the information to give it as high a rating as possible to make themselves look effective, hence objectivity can potentially be lost. To counter this, it is common practice for the information to be evaluated by an independent intelligence officer, usually responsible for the intelligence process as a whole. However, there are some other views that these officers may err in the process or be overcautious in their evaluation of intelligence and its dissemination (Newburn et al. , 2008: 206-207). The additional dimension of the ‘handling code’ which regulates the dissemination of the information to other parties makes it easier to share information / intelligence with trust, without having to worry about the leakage of information.

Collation

The next step will be to collate the data, separating and organising relevant information. Once a targeting decision is made and an analysts had been directed to undertake a particular project (or, as is often the case, the analyst is self-directed), then according to the intelligence cycle, a collation phase is undertaken. In reality, information collation is often conducted as part of the process of deciding which targets law enforcement has the capacity to tackle. Effective information collection and collation, requires communication with the client that originated the tasking and interpretation of their client’s requirements (Ratcliffe, 2009: 127).
Data collation is defined as the indexing, sorting, and storage of raw data, and it is the next step in the intelligence cycle. Raw data, by themselves, are seldom of much value. Only when similar items are collected and considered together, can the analyst provide meaning to the data. Data collation accomplishes this objective (Gottlieb, Arenberg, & Singh, 1994: 127).

Analysis

Finally, analysing the information, compiling it, summarising it, and comparing and organising the materials into a coherent whole to determine the nature and relationship of the target (s) and the criminal group. In short, information is collected and its veracity and importance evaluated before it is analysed in further depth. A 'package' (i. e. an intelligence file on a group of offenders, or a set of criminal activities) may then be developed by the intelligence unit and disseminated back into the field. At this point it may be tactically activated by, for example, a surveillance team following the offenders in the hope of 'catching them in the act' or at least gathering evidence of criminal activities. More often than not, the intelligence will require further development by field intelligence officers or others. In either case, these actions should produce further information to feed back into the system and hence the cycle continues (Newburn et al. , 2008: 204).

Cope (2003:340) sees crime analysis as involving the 'synthesis' of police and other relevant data to identify and interpret patterns and trends in crime, to inform the police and judicial practice. Engaging in the process of analysis patterns of crime, can be identified among offenders, offences, victims, spaces and places. Crime analysis supports the prevention, reduction and investigation of crime by providing law enforcement with information that enables them to prioritise interventions. Crime analysis identifies the situation of crime problems, criminal targets and vulnerable victims to prevent and reduce crime, while investigative analysis assists with investigating crimes and the prosecution of offenders by providing information for presentation at court (Newburn et al. , 2008: 208).

Four modes of intelligence packages that are routinely processed are the following:

1. Criminal intelligence- detailing the activities of a known suspect/suspect.

2. Crime intelligence-enhancing the police's understanding about a specific crime or a series of crimes.

3. Community intelligence- based upon data provided to the police by ordinary members of the public.

4. Contextual intelligence-relating to wider social, economic and cultural factors that may impact upon levels of crime and patterns of offending (Newburn et al. , 2008: 208).

In practice the majority of the analysis work is conducted by crime (tactical) and intelligence (strategic) analysts, based within intelligence units (Newburn et al. , 2008: 208-209).

Dissemination

The function of dissemination, is to ensure that the finished intelligence package is circulated to those that need to see it. An intelligence product which remains locked up in the intelligence unit and is only read by intelligence personnel, fails to achieve the primary objective of intelligence, and is of no use to influence the decision making. The greatest and practical problem associated with the intelligence cycle, particularly in terms of tactical and operational policing, concerns difficulties in ensuring that the criminal intelligence that is produced is actually followed up and used operationally (Newburn et al. , 2008: 209).

Feedback
Feedback is the informing of the crime analyst of the outcome of the information or crime analysis product (Reuland, 1997:36). According to police officers interviewed, the intelligence led policing model was implemented by the South African Police Service in 1995. It was introduced together with the Crime Intelligence Component. This model was used for crime prevention and the investigation of crime. Private security officers who were interviewed, did not use the intelligence model to address risks in the private security environment. They worked with the SAPS to do intelligence led policing to address threats affecting their assets.

Strategy 3: Compstat (Compare statistics)
The 1980s and the 1990s is seen as a period of innovation for problem and community based crime control solutions, but it was also the period that saw the rapid emergence of Compstat as a crime fighting strategy. Compstat began in the Crime Control Strategy meetings of the New York Police Department (NYPD) in January 1994. Police Commissioner William Bratton, newly hired from the city's Transit Police by mayor Rudy Giuliani, created Compstat with the primary aim of establishing accountability among 76 police commanders. The much publicised crime drop in New York around this time cemented the popular view that Compstat was responsible for making the city safer. Major crime in the city fell by half from 1993 to 1998 (Ratcliffe, 2003: 31).

When the Compstat crime reduction meetings started in early 1994, maps of crime in New York City were projected onto a wall. This allowed the meeting participants to concentrate on crime hot spots, and pressure was placed on precinct commanders to address emerging hotspots. Within Compstat the application of the term intelligence is slightly at odds with how the word is more commonly used. Within the Compstat framework, intelligence more frequently refers to mapped data and is more akin to information than the integrated crime intelligence. The crime reduction mechanism of Compstat involves four principles (Ratcliffe, 2003: 76).

- Timely and accurate intelligence
- Effective tactics
- Rapid deployment
- Relentless follow- up and assessment

Compstat was associated with a significant reduction of crime in New York City and as a result the strategy rapidly spread throughout the world, fuelled by the media, public and law enforcement enthusiasm. New South Wales Police introduced Compstat under the heading 'Operation and Crime Review' (OCR). It was based on the Compstat model. The operational room was located in Sydney, the capital city. From August 2001 – June 2004, the Queensland Police Service in Australia used the Compstat model and reduced crime at a cost of AU$ 1 000 000. According to research findings, in practice, the general aim of most of the Compstat sessions is to address street crimes, such as robberies and assaults, and property crimes, such as vehicle theft and burglary. Compstat has not been widely applied to more esoteric crime activity, such as organised crime or transnational crime, and it has not been applied to broader areas that community policing areas may address (Ratcliffe, 2003: 79).

According to the interviews with the police officers, the COMSTAT process was implemented in the South Africa Police Service during 2000. Prior to 2000, the SAPS used Statistical analysis the Crime Pattern Analysis (CPA) to compare crime figures. The

COMPSTAT process is still being practiced nationally, provincially, at cluster and police station levels in the SAPS. The private security officers interviewed do not use the COMPSTAT model in the private security environment, but they use statistical analysis to compare statistics on their losses. The COMPSTAT process is more the management of mapped data, which is information related, waiting to be enriched into crime intelligence.

Strategy 4: Security intelligence cycle

According to Fischer et al. (2008: 31) "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". In the security environment 'private security' includes efforts by individuals and organisations to protect their assets against 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).

Tragic events such as the September 2001 terrorist attacks in New York and Washington and the more recent convictions of individuals in connection with terrorism-related offences, demonstrate the need for effective 'national' security intelligence by government organisations. The need for adequate management of intelligence activities is imperative in the light of the challenges to security posed by events such as the above-mentioned.

Security intelligence encompasses a series of steps called the intelligence cycle. The cycle begins with the *need for intelligence*. Usually it takes the form of a general question from an intelligence customer (one who requests for the intelligence) such as 'how porous our South African Borders are'? (Clark, 2010: 10).

Then comes the *planning, or direction- determining phase*, on how the other proponents of the cycle will address the problem. Collectors will have to be tasked to gather missing bits of information. Analysts will have to be assigned to do research and report on the porous nature of the South African Borders. The cycle then proceeds to *collection, or gathering of information.* Media articles from towns on the South African borders will have to be acquired. Communication intelligence (COMINT) will have to be obtained from the communication media servicing the border towns. Human Intelligence (HUMINT) will have to be obtained from persons with knowledge of the South African borders (Clark, 2010: 10).

The collected information has to be *processed.* Foreign language material has to be translated. Encrypted signals need to be decrypted by language specialists. Film or digital signals must be translated into visible imagery. Responses from the HUMINT sources must be validated and organised into a report format. The newly collected and processed material *must be utelised* to create intelligence in an *analysis phase.* An analyst must create outcome scenarios based on the current situation of the borders, generate profiles of the borders and security incidents and assess the likely recurrence of such incidents. The analysis phase also includes a peer and supervisory review of the finished product. The finished product must be *disseminated* to the client in a written report (electronically) or a briefing. A transition for new requirements or needs is established, and a new cycle begins (Clark, 2010: 10-11).

The police officers interviewed believe that the security intelligence cycle was used for National Security reasons prior to 1995. The private security officers did not use the security intelligence cycle in the private security environment, but were assisted by the South African

Police Force (SAPF) with national security intelligence to provide security at national strategic installations, government buildings and businesses confronting threats.

Strategy 5: Security risk management

According to Blyth & Kovacich (2006:43), the objective of Security risk management (SRM) is the protection of people, assets and earnings by avoiding or minimising the potential for loss against risks and the provision of funds to recover from losses that do occur. It involves the taking of steps to reduce risks to an acceptable level and maintaining that level of risk (Blyth& Kovacich, 2006:43-50). It is a subset and essential part of a broader risk management system. Security Risk Management is simply another management function fitting predominantly within the sphere of risk management. Other disciplines include; Emergency response, Business continuity, Occupational Health and Safety (OHS), Financial management and Project management(Talbot and Jakes, 2008:37). If we look at security as a state of being protected from hazards, danger, harm, loss of injury, it also includes elements of protection from national disasters and concepts of organisational resilience (Talbot and Jakes, 2008:42).

Security Risk Information Management (International)

Security risks management is making the most efficient before- the- loss arrangement for an after- the- loss continuation of business. Security risk management allows risks to be managed in a logical manner, using long held management principles (Fischer et al. , 2008:148).

Establish the context

The importance of fully and comprehensively establishing the Security Risk Management context cannot be understated and stakeholders should be engaged to identify the strategic context, security risk management context and organisational context (Talbot and Jakes, 2008:176). According to Pupura, (1993:20), risk is associated with virtually every activity imaginable. Although security risks are limited to three common categories, such as personal, property and liability it is still important to establish the correct context.

Identify risks

According to Fay, (2006: 111), risks of concern to security practitioner include terrorism, political conflict, military operations and harm from criminals. Risk identification normally arises from the defined context, which is informed by the threat, vulnerability and criticality assessments, as well as historical information management systems and program activities. During the assessment we need to ask the questions what, when, where, how and who for clarity (Talbot and Jakes, 2008:176).

Analyse risks

The first step in the risk analysis process is the identification of the threats and vulnerabilities. Many threats in business are important to security, but some are more obvious than others. The key is to consider the specific vulnerabilities in an organisation (Fischer etal. , 2008: 148). The logistical aspects relating to procurement, implementation and ongoing maintenance of physical protection systems such as alarm systems, fencing, guards and the installation and maintenance of technical solutions, can present significant immediate and ongoing costs to an organisation. A risk register is one of the most practical ways used by security service providers for the cataloguing of identified risks and measuring the costs of preventing their occurrence. It benchmarks the asset criticality against identified risks. It also

provides a framework from which to allocate physical security resources and infrastructure funding. A risk register provides an overview of the following:

- Key risk to the organisation- those that put into jeopardy the delivery of its medium /long term objectives, or its ongoing survival;
- The consequences of the risks materialising;
- The impact and likelihood of the risk materialising;
- The management and control mechanisms to administer risk mitigation strategies, and contingency arrangements if applicable, that would be invoked should the risk materialise;
- A nominated person who takes responsibility for ensuring that the management and control arrangements are in place, operating satisfactorily, and are being improved;
- A brief statement of the further action necessary to minimise risk event occurring and/or to mitigate its effects (Talbot and Jakes, 2008:178).

It is necessary to conduct a risk analysis exercise to determine a company's specific exposure to specific crime threats. The security survey will point out weaknesses which will assist the security risk manager to establish the relative manageability of the identified crime risk (Fay, 2006:111).

According to Hess & Wrobleski (1988:61) the key in analysing risks is for the security practitioner has the ability to identify risks or the physical opportunity for crime and the preparation of recommendations for management to take a decision.

Evaluate risks

After Physical Protection Systems objectives have been established and a new upgraded design has been developed. It is necessary to evaluate the effectiveness of the design in meeting the objectives. The evaluation can be done using the quantitative or qualitative methods or a combination of both the quantitative or qualitative methods (Garcia, 2008: 263). According to Talbot and Jakes (2008:179), one of the most common risk evaluation techniques involves determining likelihood and consequence. Usually these metrics are defined using one or more of three methods:

1. Qualitative – using descriptive terms and phrases to assess and define risk
2. Quantitative – using historical or calculated data
3. Combined qualitative/quantitative – using numbers to provide comparative assessment of likelihood, consequence and/or risk.

According to Talbot and Jakes (2008:179) the latter is the most useful if it can be developed, as it not only allows historical data to be input into the analysis, but also removes some of the subjectivity associated with the risk process (Talbot and Jakes, 2008:179).

Treat risks

Once the security probability and criticality analysis has been completed and the security problems have been identified and ranked in importance, the security manager in cooperation with other members of management must decide on how the risks should be treated (Fischer et al. , 2008:159)

Risk response and controls include a range of measures. The objective is not only to eliminate risks but rather to reduce risks to the point where it is as low as reasonably practicable. Regardless of the organisations or individuals risk tolerance levels, the following risk treatment principles are important according to Talbot and Jakes, (2008:187).

- Do not accept unnecessary risks;
- Accept risk only if the benefits outweigh the costs;
- Risks should be managed at the point in which it occurs.

The risks may be treated by using different alternatives such as risk avoidance, risk reduction, risk reduction, risk spreading, risk transfer, and self assumption of risk (Fischer et al. , 2008: 159-161 & Fay, 2006:114-115).

Security Risk Management Plan

The purpose of a security management plan is to prevent a adversary from successful completion of a malicious act against a facility. The primary functions of such plan should include elements such as detection, delay and response. The establishment of a security risk management plan provides an organisation with an executive support and impetus to manage risk (Garcia, 2008: 8).

A security risk management plan should incorporate strategies to reduce both the cost of risk management relative to identified threats and to assign the most appropriate risk treatment to each identified risk. A key element of the design of security risk management involves the application of treatments that (in priority order) involves the objectives to deter, deny, delay, detect, and respond with respect to a potential attack (Talbot and Jakes, 2008:188-189).

- Deter: A deterrent factor is a device or barrier which controls unauthorised access into a facility. It displays its inherent asset protection capabilities against potential criminals attempting unauthorised entry. Deterrent factors can take many forms. fencing, signposts, visible guards, or a barking dog. They may deter an unauthorised access to an asset.

- Deny: The denial of access to unauthorised parties to an asset is another mechanism used to promote security.

- Delay: A delaying factor is a barrier or scenario that provides time for another protective measure to take effect, should unauthorised access to an asset occur.

- Detect: Detection may occur in a variety of means including alarms, system logs, direct observation, patrols, CCTV or sign of attempted entry.

- Respond: A response must be consistent and appropriate with the level of threat detected against the asset.

- Recovery: Recovery is the final barrier to mitigate the long term consequences of any attack by returning to desired levels of capabilities as quickly as possible (Talbot and Jakes, 2008:188-189)

Security Risk Information Management (South Africa)

Security Service providers in South Africa are currently utilising a Security Risk Management Model (process) to manage security risk information in their environment. This model, developed over the last ten years by the staff members at the former Programme Security Management at the TechnikonSA (after the merger with UNISA renamed the Department of Security Risk Management in 2004 and again renamed Programme Security Managment with the merger in 2009 with the Department of Criminology) is currently being applied by hundreds of security practitioners. The primary aim of the model is the management and analysis of security risk information facing corporations and businesses, whose risks are largely of a criminal nature. The model focuses on ~~the~~ identifying, measurement (establishing probability) and analysis of (vulnerabilities and security measure weaknesses that lead to exploitation of opportunities) of the crime risks. The security risk management model is based on the following process:

1. Identifying the problem posed by the crime;
2. Considering the security policy and mandate in relation to the problem;
3. The orientation phase;
4. The risk analysis exercise;
5. The comprehensive security survey;
6. Security risk control measures;
7. Return on investment;
8. The crime risk management report;
9. Implementation, evaluation and maintenance of security measures.

Risks are identified and the data is collected by conducting a Risk Analysis exercise and a comprehensive Security Survey. Thereafter security risk control measures are put into place to counteract identified risks. A return on investment exercise is also undertaken, to ensure that the security control measures are cost effective, in that the security solution should save the company instead of making the company lose more money. A report containing findings and recommendations is submitted to the top management of the company for a decision on implementation on security measures. On approval by management the security measures are implemented and then tested by means of a penetration exercise (Rogers, 2008:151-154).

Other Security Risk Analysis Models are also used to calculate the annual cost of losses. One such Crime Risk Analysis Model, used to determine the frequency of losses and the frequency of exposure to specific risks, is that of Fay (2006:114). This model tests the Probability, Impact and Frequency of specific criminal acts. The common questions tested in this model are the following:

1. What is the probability of a criminal act being committed? Is the probability of the occurrence, unknown, unlikely, likely or certain?

2. What will be the impact of such a criminal act in terms of costs of replacement, repair, lost productivity, forfeiture of business opportunity, clean up, litigation, damage to reputation and undermining of customer goodwill be?

3. Frequency is different from probability, in that the police will be able to provide the security manager with a record of all such occurrences for the period in question (daily, weekly, monthly yearly or longer).

According to Fay, (2006:114–115), it is important for management to be aware of the relative manageability of a crime risk. Manageability is the capacity to reduce the probability and/or impact of a risk. The principle methods of managing risks include the following:

- *Avoiding the risk by removing the target*. Laptop theft can be avoided entirely by choosing not to provide laptops to employees. A trade secret, such as the formula for a popular soft drink, can be kept in a high-security vault. Some businesses avoid crime-related risks by choosing not to operate in high-crime areas.

- *Reducing the risk by decreasing the target*. A convenience store robbery loss can be reduced by placing all cash receipts above a designated amount in a floor safe. The store's shoplifting risk can be reduced by placing high-value merchandise in locked cabinets and easily concealed high-demand items, such as packs of cigarettes, behind the cashier's counter.

- *Diffusing the risk* involves the use of barrier systems such as perimeter fences, access control and intrusion detection equipment such as card readers and CCTV; locks, safes and vaults; and standard control procedures such as property removal passes and inventory counts.

- *Transferring the risk* is possible by purchasing insurance or by raising prices so that the purchasers of the product or service pay for the losses. Another technique is to outsource risk-heavy functions to another party. An example is the transfer of liability when an employer replaces an in-house guard force with a contract guard force. If misconduct by a contract guard causes a serious accident, the employer may be able to escape liability under the terms of the contract.

- *Accepting the risk* is also an option. Management may decide that a particular risk is worth a gamble, or that the cost of loss does not justify the cost of prevention. Another deciding factor may be the intractability of the risk (i. e. that despite the best efforts, the risk cannot be controlled to an acceptable degree).

According to the private security officers interviewed, the Security Risk Information Management Model is used by many security service providers in South Africa. It has been implemented by private security companies since 2000. The police officers interviewed had knowledge of the security risk information management model. It is used to do Security Risk Analysis of parliamentarians and other dignitaries by the VIP Protection Unit in SAPS and for the planning of major events especially sporting events. It is used as a management tool for the collection of risk information, conducting criticality analysis and implementing appropriate security risk control measures.

SHARING OF INFORMATION

Information sharing among private security service providers and the SAPS takes place on a daily basis. Big business in South Africa is represented by Business Against Crime (BAC) and by security information coordinating companies such as South African Banking Risk Information Centre (SABRIC), Petroleum Security Initiative (PSI) and the Consumer Goods

Council of South Africa (CGCSA). These information coordinating companies attend meetings on an ad hoc basis at police station level, cluster level and at Provincial level sharing information on threats and criminal incidents. These meetings share information on crime and strategies to combat crime and to prevent losses at businesses. These strategies are proposed to management of businesses as security risk control measures to reduce or eliminate the risks confronting the businesses. Information and strategies are also shared at Community Policing Forums and at Sector Policing meetings held at respective police station areas. According to Provincial Commissioner Mzwandile (2011:28-29), the South African Police Service (SAPS) in Gauteng, relies completely on the sharing of crime information between the South African Banking Risk Information centre (SABRIC), and Business against Crime (BAC). The SAPS also has a war room (cluster operations room) which coordinates all activities for the joint policing of high crime areas in the Province. The war room concept also exists at most of the other Provincial offices of the SAPS. The Information coordinating companies and the BAC also hold their own information sharing meetings.

Fusion centres and war rooms

Fusion centres and war rooms in the United States of America (USA) are designed to coordinate information from a variety of sources, an array of disciplines, and from different levels of government. The challenge is enormous and necessitates allied agencies to appoint officers to carry out the fusion centre responsibilities and to bring about changes to their existing policies and procedures that in the past may have obstructed information and intelligence sharing. Many of these fusion centres concentrate solely on terrorism, while others adopt an all crimes, all hazards and and all threats approach. Regardless of their focus, each agency has to confront the obstacles inherent to change. The fusion centre is the first attempt to introduce the concepts of intelligence and intelligence-led policing to an underdeveloped network of potential information collectors and intelligence producers and consumers (Ratcliffe, 2009: 26-27).

Current intelligence is synthesised (fast synthesis) as quickly as possible to support ongoing tactical operations and to allow for the collection of missing information to be done in a short period of time. This so called, "fast synthesis "differs from normal synthesis and analysis only by the emphasis: "Fast synthesis" is aimed at using all available data sources to develop a more complete picture of a complex event, usually with a short time frame. The target model exists, and the job of the analyst is to fit in any new data. Analysts work only with the incoming data and anything that is immediately accessible to them in a data base or in memory. "Fast synthesis" or the concept "fusion" is commonly used by intelligence analysts when time is the critical element-such as in support of military operations, crisis management, law enforcement, and similar direct operations (Clark, 2010: 54).

According to the police officers and security officers interviewed, they hold continuous discussions with private security companies and daily crime combating meetings where private security companies are invited to share crime information. Private security companies also attend Community Policing Forum (CPF) meetings where they share information on an ongoing basis. These meetings are similar to fusion centre meetings. In specific policing areas, where there is strategic installations and high volume economic activity, for example mining, monthly fusion centre meetings are held between the SAPS and private security providers who are responsible for the safeguarding of such installations.

CONCLUSION

Cyber-crime, property related crimes, corruption, organised crime and transnational organised crime, require–law enforcement and private security to respond with information management strategies. Information management strategies are central to the task of combating crime and preventing losses. Analysed data related to the vulnerability of a target and the modus operandi, presents the opportunity to address the exploited weaknesses of an asset/victim. The five information management strategies discussed, may be effectively used by the SAPS and the private security industry. The five information management strategies have been implemented in the UK, Australia, USA and to a lesser extent in South Africa. According to the police officers interviewed all five information management strategies have been implemented by the SAPS. It is not known if the implementation is being sustained nationally.

The private security officers interviewed only experienced the implementation of the security risk management model. The sharing of information in South Africa is ongoing. Information on crime incidents, threats and strategies are shared at different levels between BAC, SABRIC, PSI, CGCSA, other role players and the SAPS. These shared strategies are implemented by businesses according to the risks confronting their businesses, organisations or assets. The information management strategies will help the police and the private security service providers to put in place a preventive program to combat crime successfully? and to reduce losses.

LIST OF REFERENCES

Australian Custom Service (ACS). 2000. *Intelligence Doctrine.* Canberra: Australian Customs Service.

Bosch, J. G. S. 1999. The role and structure of the private security industry in South Africa. *ISSUP Bulletin*. Pretoria.

Cope, N. 2003. Crime analysis: Principles and practice. In T. Newburn (ed.), *Handbook of policing*. Cullompton: Willan

Clark, R. M. 2010. *Intelligence analysis: A target centric approach*. Third edition. Washington: CQPress.

Ferraro, E. F. & Spain, N. M. 2006. *Investigations in the workplace.* New York: Auerbach.

Fay, J. J. 2006. *Contemporary security management*. Oxford: Elsievier: Butterworth Heinneman

Fischer, R. J. , Halibozek, E. , and Green. G. 2008. *Introduction to security.* Eighth edition. Boston: Elsevier.

Garcia, M. L. 2008. *The design and evaluation of physical protection systems*. 2nd edition. Boston: Butterworth/Heinemann.

Gottlieb, S. , Arenberg, S. & Singh, R. 1994. *Crime Analysis: From first report to final arrest.* Montclair, CA: Alpha.

Hess, KM & Wrobeleski, H. M. 1988. *Introduction to private security*. 2nd edition. New York:West.

Marais, C. W. 2003. *Crime investigation. Only study guide for CJS308-E*. Pretoria: UNISA

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, UK: Willan

Parpura, PP. 1993. *Retail security and shrinkage protection*. Stoneham:Butterworth-Heinemann

Peterson, M. B. 1994. *Applications in criminal analysis: A sourcebook*. Westport, Conn.: Greenwood Press.

Rapp, B. 1989. *Deep cover: Police intelligence operations*. Boulder: Paladin Press.

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. H. 2009. *Intelligence led policing*. Cullompton: Willan

Reuland, M. M. 1997. *Information management and crime analysis*. Washington, DC: Police Executive Research Forum.

Rogers, C. 2008. A security risk management approach to the measurement of crime in a private security context. *Acta Crimnologica: Southern African Journal of Criminology: CRIMSA Conference 2007 Special Edition 3:* 155-166

Scott, M. S. 2000. Problem-*orientedpPolicing: Reflections on the first 20 years*, October 2000. Washington, DC: COPS Office.

Sheptycki, J. 2004. Organisational pathologies in police intelligence systems: Some contributions to the lexicon of intelligence led policing. *European Journal of Criminology*, 1(3): 307-332.

Stelfox, P. 2009. *Criminal Investigation: An introduction to principles and practice*. Cullompton: Willan

Talbot, J. & Jakeman, M. 2008. *Srmbok. Security Risk Management Body of Knowledge*. First edition. Australia: Ligare

Van Rooyen, H. J. N. 2008. *The practitioner's guide to forensic investigation in South Africa*. Pretoria: Henmar Publications.