AN INVESTIGATION OF THE BOMBING OF AUTOMATED TELLER MACHINES (ATMs) WITH INTENT TO STEAL CASH CONTENTS: CASE STUDY FROM GAUTENG

BY

SARIKA SEWPERSAD

Submitted in fulfilment of the requirements for the degree of

MAGISTER TECHNOLOGIAE

in the subject

Security Management

at the

UNIVERSITY OF SOUTH AFRICA

Supervisor: Prof A. deV. Minnaar

March 2010
COPYRIGHT

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

Student number: 45509239

I, SARIKA SEWPERSAD, declare that this dissertation: AN INVESTIGATION OF THE BOMBING OF ATMs WITH INTENT TO STEAL CASH CONTENTS: CASE STUDY FROM GAUTENG is my own work and that all the sources that I have quoted have been indicated and acknowledged by means of complete references.

___________________________                                                             ___________________
SIGNATURE                                                                                                       DATE
(S. SEWPERSAD)
### TABLE OF CONTENTS

COPYRIGHT .................................................................................................................. i
DECLARATION BY STUDENT ....................................................................................... ii
ACKNOWLEDGEMENTS ................................................................................................. x
EXECUTIVE SUMMARY ................................................................................................. xi

| Chapter 1: MOTIVATION FOR RESEARCH ................................................................. 1 |
| 1.1 INTRODUCTION ................................................................................................. 1 |
| 1.2 RATIONALE OF THE STUDY ............................................................................ 2 |
| 1.2.1 Reported extent of the crime ................................................................. 2 |
| 1.2.2 Charges ATM bombers can face ............................................................ 5 |
| 1.2.3 Cost to the banking industry and/or businesses ....................................... 7 |
| 1.2.4 Danger to society ..................................................................................... 8 |
| 1.2.5 Inconvenience to bank clients ............................................................... 9 |
| 1.3 RESEARCH AIMS ......................................................................................... 9 |
| 1.4 KEY THEORETICAL/OPERATIONAL CONCEPTS ........................................ 10 |
| 1.4.1 Automated Teller Machine (ATM) .......................................................... 10 |
| 1.4.2 ATM attack/bombing ............................................................................. 10 |
| 1.4.3 ATM safe .................................................................................................. 10 |
| 1.4.4 ATM throat .............................................................................................. 10 |
| 1.4.5 Commercial explosives .......................................................................... 10 |
| 1.4.6 Detonator ................................................................................................. 11 |
| 1.4.7 Igniter cord .............................................................................................. 11 |
| 1.4.8 Connector capped fuse ........................................................................... 11 |
| 1.4.9 Integrated security system (risk control measures) ................................ 11 |
| 1.4.10 Security Risk Management Model ....................................................... 11 |
| 1.5 VALUE OF THE RESEARCH ...................................................................... 12 |
Chapter 2: RESEARCH METHODOLOGY ................................................................. 13
2.1 INTRODUCTION .......................................................................................... 13
2.2 THE RESEARCH DESIGN ........................................................................... 14
2.3 POPULATION AND SAMPLING PROCEDURES ....................................... 14
  2.3.1 Risk categorisation .............................................................................. 15
  2.3.2 Criteria for risk ratings according to ‘Hot Spot Model’ ....................... 16
  2.3.3 Sampling of SAPS case dockets ......................................................... 16
2.4 DATA COLLECTION METHODS ................................................................. 17
  2.4.1 One-on-one unstructured interviews .................................................. 17
  2.4.2 Document study as an information collection technique .................... 18
    2.4.2.1 Clustering and coding of media reports ....................................... 19
  2.4.3 Analysis of closed circuit television (CCTV) footage as a form of data collection... 19
  2.4.4 ATM site audit as a form of observation ............................................ 20
2.5 PROBLEMS ENCOUNTERED DURING RESEARCH ............................... 20
  2.5.1 Sensitivity of information .................................................................. 20
  2.5.2 Availability of candidates .................................................................. 21
  2.5.3 Time constraints ................................................................................ 22
  2.5.4 Issues with regard to docket analysis ................................................ 22
    2.5.4.1 Accessibility of dockets ................................................................. 22
    2.5.4.2 Language barriers ........................................................................ 23
    2.5.4.3 Illegible handwriting ................................................................... 23
  2.5.5 Issues regarding ATM site audits ....................................................... 23
  2.5.6 Challenges in transcribing interviews ................................................. 23
2.6 DATA ANALYSIS ........................................................................................ 24
2.7 VALIDITY, RELIABILITY AND ACCURACY OF COLLECTED INFORMATION... 25
  2.7.1 Ensuring validity .............................................................................. 25
2.8 ETHICAL CONSIDERATIONS .................................................................... 25
2.9 CONCLUSION ............................................................................................ 26
Chapter 3: AN OVERVIEW OF BANK SECURITY THREATS

3.1 INTRODUCTION

3.1.1 Reasons pertaining to non-disclosure of information regarding banking security

3.2 BANK SECURITY THREATS

3.2.1 Armed robbery

3.2.2 Bank robbery

3.2.3 Cash-in-transit attacks/robbery

3.2.4 ATM attacks

3.2.4.1 Ram raids

3.2.4.2 Gas attacks

3.2.5 Client robbery

3.2.5.1 Mugging

3.2.5.2 ‘Forced withdrawal’

3.2.5.3 ‘Non-violent threats’ (theft) at or from ATMs

3.2.6 Threat of vandalism

3.3 METHODS OF PROTECTION

3.3.1 Human element

3.3.1.1 Guarding aids

i. Firearms

ii. Dogs

iii. Metal detectors

3.3.2 Armed reaction

3.3.3 Staff (procedures)

3.3.4 A central command centre

3.3.5 Physical security equipment

3.3.5.1 CCTV surveillance

3.3.5.2 Alarm systems

3.3.5.3 Time delay locks/doors

3.3.5.4 Safes

3.3.5.5 Turnstiles

3.3.5.6 Interlocking doors
Chapter 4: ATM SITE AUDIT AND AN ANALYSIS BASED ON LOCATION OF ATM BOMBING

4.1 INTRODUCTION

4.2 ATM SITE AUDIT

4.3 LIMITATIONS EMANATING FROM SITE AUDITS

4.4 THE SECURITY RISK MANAGEMENT MODEL

4.5 ANALYSIS OF INCIDENT REPORT PER LOCATION

4.5.1 Towns/suburbs most affected

a) East Rand
b) Greater Johannesburg
c) Pretoria
d) Vaal Rand (Southern Gauteng)
e) West Rand

4.5.2 Type of areas most affected

4.6 ATM SITE AUDIT

4.6.1 The importance of ATM site security and security risk control measures

4.6.2 The on-site orientation phase

4.6.3 Findings from ATM site audits

4.6.3.1 Lighting

4.6.3.2 CCTV surveillance

4.6.3.3 Customer awareness

4.6.3.4 Panic/alarm buttons

4.6.3.5 ATM Alarm

4.6.3.6 Additional security measures/devices

4.6.3.7 Presence of security guard

4.6.3.8 ATM intercom
Chapter 6: SUMMARY OF FINDINGS, RECOMMENDATIONS
AND CONCLUSION........................................................................................................ 99
6.1 INTRODUCTION........................................................................................................ 99
6.2 SUMMARY OF RESEARCH FINDINGS.................................................................... 100
  6.2.1 Summary findings related to ATM site security........................................... 100
  6.2.2 Summary of finding related to modus operandi........................................... 101
6.3 RECOMMENDATIONS.......................................................................................... 102
  6.3.1 Recommended security survey sheet......................................................... 103
  6.3.2 Recommendations on the use of special security devices....................... 107
    6.3.2.1 Tear gas/Dye pack devices................................................................. 107
    6.3.2.2 Use of pepper spray in ATMs............................................................. 108
    6.3.2.3 ATM alarm, surveillance cameras and systems integration........... 108
    6.3.2.4 TXRTL-60 safes..................................................................................... 109
  6.3.3 Other recommendations............................................................................ 109
    6.3.3.1 Need more for research................................................................. 109
    6.3.3.2 The need for proper recording and classification of ATM bombings
          as a crime................................................................................................. 110
6.4 CONCLUSION....................................................................................................... 110
BIBLIOGRAPHY............................................................................................................. 111
LIST OF ANNEXURES
ANNEXURE A: PROFORMA SHEETS........................................................................ 119
ANNEXURE B: EXAMPLE OF ATM SECURITY TIPS............................................... 121
ANNEXURE C: NUMBER OF REPORTED INCIDENTS PER POLICE STATION IN
  GAUTENG.................................................................................................................. 122
ANNEXURE D: TABLE INDICATED STATIONS WITH MOST NUMBER OF REPORTED
  CASES (IN DESCENDING ORDER)................................................................. 126
ANNEXURE D: IMAGES – DAMAGE CAUSED BY ATM BOMBINGS....................... 130
ANNEXURE E: MAPS................................................................................................. 134
  1. GREATER JOHANNESBURG................................................................. 135
  2. WEST RAND..........................................................
ACKNOWLEDGEMENTS

To my partner-in-all Zaid, the completion of the dissertation would not have been possible without your help, motivation and support. Thank You.

My supervisor and mentor, Professor Anthony Minnaar, I really appreciate the continued support and understanding you provided. You remained patient and empathetic with me whilst I struggled to complete this dissertation. You were also there every step of the way and assisted me extensively in gaining approval from SAPS and SABRIC as well as other information I required from them. I thank you.

Supt Kola of SAPS SOCS (Serious Organised crime section) and everyone else there, thank you for your help. Snr Supt Naicker and Dulcie Matula in helping to speed up the process of approval.

ATM Solutions, in particular, Schalk Burger and Riaan du Preez, you came to me in a desperate time and your assistance really added value to this research.

I thank the Lord Almighty for giving me the strength to complete this research. Without the strength of God and His continuous blessings at times when this research seemed impossible, I would have not had the ability to complete this.
EXECUTIVE SUMMARY

This research was approached and written from a security risk management position. The main aim was to determine the nature and extent of the theft of cash contents by means of the bombing of Automated Teller Machines (ATMs) in Gauteng. Security measures that currently exist at ATMs with the specific focus on crimes associated with the bombing of ATMs were examined and evaluated. This was done in order to determine if current security measures at ATMs are sufficient to curb ATM bombings.

The research provides an examination of the modus operandi of perpetrators of ATM bombings, inter alia looking at such issues as explosives used, time, location, cash stolen, and the use of weapons. This modus operandi was researched in order to develop an understanding of the perpetrators behaviour and to compile a profile of the perpetrator. The methods used in the perpetration of the crime were also researched, so that recommendations with regard to improving ATM security measures could be made. In addition, due to the specific focus of the problem of ATM bombings in Gauteng, a detailed analysis of the areas’ most affected in Gauteng was made.

In South Africa, there is no such crime as ATM bombings per se, and perpetrators of such attacks are often charged with various other crimes, including those under the explosives act. The lack of evidence at the scene of a bombing often leads to cases being filed as undetected. This results in perpetrators still walking the streets waiting for law enforcement personnel to turn their focus to another crime, so that they can once again target ATMs. This research may assist investigators/detectives. For example, if CCTV cameras are installed at all ATMs, it will provide more evidence for them. By comparing and studying footage from different ATMs, the detectives will be able to determine which ATMs were attacked by the same gangs.

The first two chapters’ set out the background and motivation for the study as well as the research methodology and the limitations experienced during the research. Chapter one in particular provides details on the need for such a study and outlines the extent of ATM bombings in Gauteng as well as in South Africa. It delineates the major issues associated with the bombing
of ATMs. This is inclusive of the impact on society (banks clients) and banking institutions as well as the danger it poses to the general public and public and private law enforcement personnel.

Since there is little literature available on the subject of ATM bombings, the third chapter outlines the various bank security threats that banking institutions face. In addition, it looks closely at the numerous other ATM crimes carried out by perpetrators both locally and internationally, suggesting that ATMs be equipped with sufficient security measures to secure ATMs from all sorts of crimes that can be perpetrated against it.

Chapter three and four, provide the research findings on the areas in Gauteng most affected, the current state of security measures at ATMs and the modus operandi of the ATM bomber.

In the fifth chapter, focus is primarily on the modus operandi of ATM bombing syndicates. It discusses the detailed findings from planning to the execution of an ATM bombing.

Finally, chapter six provides a summary of the findings, conclusions are drawn and recommendations made.

The following objectives were fulfilled in this study:

- Areas, towns/suburbs and type of locations most affected were identified,

- Findings in relation to security measures at ATMs were made with regard to lighting, CCTV, ATM alarms, physical barriers, customer awareness and other special devices. It was also established where ATMs were lacking in security measures that specifically address the problem of ATM bombings,

- The type of ATMs most affected was established
• The modus operandi of ATM bombers was established. This also addressed issues regarding the amount and frequency of cash stolen; the use of violence; death and injuries resulting from ATM bombings; banks most affected; weapons used; size of gangs; use and purchasing of commercial explosives; most popular days and times for attacks; the use of expert members and other tools and vehicles used.

Moreover, this study provides a framework for banking institutions to understand what is lacking in ATM security measures and the methods used by ATM bombers to successfully gain access to the cash stored at ATMs. In addition, the police, ATM distributors and private security personnel can use the information provided in order to improve methods of investigation as well as protecting themselves against ATM bombers and bombings. The banking industry may also use the recommendations to improve the security at ATMs by restructuring it to their specific needs.

This dissertation covers (extensively) the extent of ATM bombings in Gauteng; the current state of security measures at ATMs; the modus operandi of ATM bombing gangs and the use of explosives. Recommendations are made regarding the improvement of ATM security measures in an attempt to curb the problem of ATM bombings in Gauteng.
Chapter 1
MOTIVATION FOR RESEARCH

1.1 INTRODUCTION

South Africa has increasingly facing new crime trends. Criminals have become highly organised, sophisticated and dangerous in the commission of their crimes. In cases where a relatively different or “out-of-the-ordinary” crime appears in society, the police, as well as the specific affected industry (banking, retail, casino etc.), are often inadequately prepared or not prepared at all to deal with the consequences of such a ‘new or different form’ of crime.

This research deals with one such crime: Attacks on Automated Teller Machines (ATMs), which by definition involves the “unlawful, intentional causing of damage to an automated teller machine or any part thereof, with the intent to obtain cash, through any means whatsoever, with specific inclusion of the use of explosives” (Maree, 2008:2). The focus is on the bombing of an ATM by means of ‘the use of explosives’ (thereby ‘breaking it open for the illegal removal of the cash stored inside it’).

On Wednesday, 27 June 2007, the Automated Teller Machine (ATM), invented by John Shepherd-Barron celebrated its 40th birthday. The original machines, described during the 1960s in the UK as ‘mini-banks’, were intended to permit customers access to cash 24 hours a day, outside of the restricted opening times of banks. The machine was designed to dispense an amount of only £10 against a special paper voucher which the customer inserted into the machine, followed by a unique four digit personal identification number, or PIN code, in much the same way as today (ANON., Nd.).

The first two ATMs in South Africa were installed by the United Building Society (UBS). It is also known as the ‘United’ and was a banking financial services institution specialising in the provision of home loans to customers/clients). The UBS is a predecessor and constituent member of the ABSA banking group with its main branch in Johannesburg in 1977. The terminals, called ‘Help U Auto Tellers’, enabled customers to make deposits, withdrawals and certain account
enquiries with the use of a transaction card and PIN. By the mid-1980s, there were approximately 700 ATMs in South Africa, the fifth largest number in the world after the USA, Japan, UK and France (ABSA, Nd.)

To date, there are approximately 15 000 ATMs across South Africa and a number of methods of gaining cash illegally from ATMs have been developed by criminals and conmen. These are tricksters using fraudulent methods of obtaining cash from an ATM directly or ‘conning’ a customer busy with a transaction.

Improved policing methods in reaction to ATM crime, in particular the bombing of these machines, may assist police in tracing perpetrators and increasing the number of arrests (and in turn convictions). However, these actions tend to deter certain criminals only for a while – thereby causing a decrease in incidents – but criminals soon adapt and design new or different methods in response to police preventative or detection methods. Accordingly, the new and changing measures do not stop perpetrators from committing the crime altogether in the future, as the preventative measures and modus operandi of criminals tend to be changing all the time.

ATM crime costs the banking industry millions a year and poses a serious threat to law enforcement personnel and civilians alike. Accordingly, this crime needs to addressed in such a way that even if an ATM is bombed, the security measures put in place on ATMs and their surroundings will make it almost impossible to access the cash (e.g. delay accessing linked to quicker armed response) or will render all the cash unusable. There is therefore a need for the banking industry to step up security measures at ATMs in order that the cash contents are better protected and secured.

1.2 RATIONALE OF THE STUDY

1.2.1 Reported extent of the crime
Since 2007 media reports from all over South Africa have indicated a dramatic increase in the occurrence of ATM bombings. This had, seemingly, become the newest crime trend amongst, in particular, organised crime groups (operating as syndicate gangs). As is the nature of crime, once
this trend had started, more and more perpetrators began taking up this new trend, and by the end of 2007/2008 financial year a total of 460 reported cases of ATM bombings had occurred countrywide in that year alone (SAPS, 2008: 20).

This ‘new crime’ trend which arguably began in 2005 when only twelve such incidents countrywide were reported to the police, started to dramatically escalate to 54 in 2006 and by 2007 the number of ATM bombing incidents had reached a total of 386 (SAPS, 2008: 20). These figures indicate an increase of 607%\(^1\) from 2006 to 2007 alone.

Furthermore, between the period April 2007 and March 2009, the total number of ATM bombings in South Africa was 819, with the highest number of incidents occurring in the Gauteng Province. An analysis of an incident report provided by the South African Banking Risk Information Centre (SABRIC)\(^2\) which contained ATM bombing incidents that took place in Gauteng between January 2006 and July 2009 indicated that a total of 527 ATM attacks with the use of explosives were reported in Gauteng only between this period.\(^3\)

Figure 1.1\(^4\) is a graph indicating the number of ATM bombing incidents per month for the period April 2007 to March 2009 across South Africa (SAPS, 2009: 24). It will be noticed that if one were to add up these (per month) totals, it gives a different number to total reported figures in other SAPS documents regarding these crime figures. For example, in accordance with Figure 1.1 the period April 2007 to March 2008 gives a total of 430 incidents, yet other reported totals (from SAPS) indicate that there were 460 such incidents for the same period.

---

1 Please note that in the text most percentages have been rounded off either up or down.
2 SABRIC was established in 2001 to combat crime in the banking industry. Its primary business is to detect, prevent and reduce organised crime in the banking industry. In addition, SABRIC also provides crime risk information and consequence management to the banking industry and C-I-T companies.
3 See Annexure A for details per location.
4 The original graph indicated both CIT robberies and ATM bombings.
This discrepancy is likely due to the fact that ATM bombings is not listed as a specific crime code category such as bank robberies or cash-in-transit robberies and may in fact be reported under other crime categories (e.g. merely as a robbery).

According to a SAPS crime situation report for 2006/07 financial year:

Most of the times ATM blasts, of which one was reported almost every day since the beginning of 2007, are also reported as if either business or bank robberies were involved. Almost all of these blasts actually constitute malicious damage to property and theft of money cases (if the explosion succeeds in opening the ATM safe). If somebody is injured because of the explosion (an eventuality which occurred in very few cases up to now), a charge of attempted murder will be added. If a victim dies as a result of this, a murder charge will be added – but this has not yet occurred (SAPS, 2007, 15-16).

As a direct consequence of the fact that the police do not specifically register a case of ATM bombing, the statistics as provided by SAPS and those provided separately by SABRIC do not
correspond. The researcher prefers to make use of those statistics provided by SABRIC as they are seemingly more reliable in that SABRIC does record incidents as ‘ATM attacks’ (as well as being the body directly serving the South African banking industry to record and analyse any crime incidents that directly target this industry).

Going back to the incident report provided by SABRIC, when the incidents that occurred between April 2007 and March 2009 were extracted from that report, it indicated that a total of 409 ATM attacks using explosives occurred in Gauteng for that period. Therefore if, according to SAPS the total number of incidents that occurred between April 2007 and March 2009 are 819 (nationwide) then it can be deduced that 50% of ATM attacks using commercial explosives took place in Gauteng alone.

Needless to say, despite the discrepancies (small enough not to be statistically significant) between the statistical information of ATM bombings of the SAPS and SABRIC, it is still clear that such an increase in any type of crime, particularly one of such a violent nature deserves further research.

1.2.2 Charges ATM bombers can face
The following are the charges that someone arrested for an ATM bombing can face (Geldenhuys, 2009: 38):

- Possession of unlicensed firearm (Firearms Control Act 60 of 2000): According to the Act (60 of 200), “no person may possess a firearm unless he or she holds a licence, permit, or authorisation issued in terms of this act for that firearm”.\(^5\) Offenders of ATM bombings are always armed.\(^6\) In all cases involving arrests, perpetrators were found to have unlicensed firearms in their possession (Sewpersad, 2010a; Sewpersad, 2010b).

- Charges in terms of section 22(2) of the Explosives Act 15 of 2003 (see details below): perpetrators of ATM bombings use and are in the possession of commercial explosives illegally;

\(^6\) See Chapter 5
• Attempted murder: perpetrators may be charged with this if a civilian or official is injured during the perpetration of an ATM bombing and someone is injured;

• Murder: perpetrators may be charged with this if a civilian or official is injured during the perpetration of an ATM bombing and someone dies as a result;

• Malicious damage to property: this charge is due to damage caused by the explosives used during the perpetration of the crime;

• Armed robbery: ATM bombers carry out their crimes, fully armed and are in essence committing robbery; and

• Theft of vehicles: Stolen or hijacked vehicles (pre-perpetration of crime) are often used during these crimes or the vehicles are stolen/hijacked at the scene of crime and used during the getaway.

In addition, if they were to threaten and seriously assault a security guard or staff and customers (at a convenience store or in the vicinity of an ATM site) in the process of bombing an ATM they could also be charged with Assault and Assault GBH.7

**The Explosives Act 15 of 2003**

When a suspect is arrested for having been involved in an ATM bombing, there are a number of charges he may face (see charges listed above). Inclusive of these are charges in terms of the Explosives Act 15 of 2003.

One of the main charges in terms of the abovementioned Act is that in terms of section 22(2) of this Act. Accordingly, S22(2) states that “Any person who intentionally delivers, places, discharges, detonates or initiates explosives with intent to cause death or serious bodily injury to any other person or to damage or destroy any place, facility or system is guilty of an offence.”

---

7 GBH = Grievous Bodily Harm.
Below is s22 of the Act:

**CHAPTER 5: ENDANGERING LIFE OR PROPERTY (s 22)**

**22 Endangering life or property**

(1) For the purposes of this section, 'explosion' includes a fire caused by explosives.

(2) Any person who intentionally delivers, places, discharges, detonates or initiates explosives with intent to cause death or serious bodily injury to any other person or to damage or destroy any place, facility or system is guilty of an offence.

(3) Any person who intentionally or negligently causes an explosion which endangers life or property is guilty of an offence.

(4) Any person who in any manner-

   (a) threatens that he or she or any other person intends to cause an explosion or to place explosives in such a manner or at such a place that life or property is or might be endangered is guilty of an offence; or

   (b) communicates false information, knowing it to be false, regarding any explosion or alleged explosion or explosives is guilty of an offence.

---

**1.2.3 Cost to the banking industry and/or businesses**

To date, ATM bombings have cost banks millions of rands, not only to repair or replace an ATM but also in the loss of actual cash contents. According to media reports,\(^8\) the cost per blown-up (bombed) ATM to repair or replace, may be anything from R150 000 upwards. In incidents where an ATM is attached to or next to a building and the explosion causes structural damage to the building there will also be the costs incurred to the building owner both in terms of repairs and loss of business (e.g. where such ATM is sited in a small convenience store or at a petrol garage/station).

Maree (2008, 11-12) divides these costs into immediate costs, medium-term and long-term costs. In terms of immediate costs, it will include cash losses (where the safe was blasted open and cash

---

\(^8\) Due to the sensitive nature of such information, banks are reluctant to publicly release such (and other) information with regard to bank robberies, C-I-T heists and ATM bombings. Hence the only recourse to such information has been media reports estimating the extent of (money) losses per ATM bombings and general costs of repair etc.
was damaged and/or stolen); losses due to “structural damage including possible damages to surrounding building; and loss of business if the ATM was placed in or near business premises.”

Medium-term costs, according to Maree (2008: 13), include the “replacement costs of the machine and rebuilding of damaged structures, as well as increased insurance premiums”. The category of long term costs includes loss of time (off work) to victims and eyewitnesses who may have to testify in court, which will result in loss of productivity. Such ‘work-related’ losses also imply ‘off-work’ time if customers, staff and guards in the vicinity at the time of the blast are injured (medical treatment and hospitalisation costs or time loss costs due to sick leave put in) or off work due to stress incurred at the time of the specific incident. Such loss includes potential loss of productivity and customers’ staying away due to fear of a repeat of such action. Business or loss of customers not frequenting the store/s in close proximity to the bombed ATM also occurs.

1.2.4 Danger to society

The explosives used in ATM bomb attacks have been identified as being ‘commercial explosives’ that are largely used in mines for underground blasting. The impact of such an explosion to a person near to or in the close proximity of either the ATM or building housing the ATM could cost them an arm, limb or even their lives. While the use of such explosive causes a danger to civilians, they also put the lives of the perpetrators who use them, in danger. There have been reported cases of perpetrators who have been injured whilst carrying out this crime. In one particular case an alleged ATM bomber approached the bombed ATM to retrieve cash, but some of the explosives had not detonated and exploded ripping off both his arms (Posthumus & Rondganger, 2008: 4).

In addition to the danger of the explosives, perpetrators of ATM bombings are often heavily armed and ready to open fire on anyone who gets in their way or any response teams, for example the SAPS or private security that might arrive on the scene while the crime is still in progress. As a result of the ruthlessness of these criminals, numerous security personnel, employees and customers at petrol stations have been held up and beaten, police officers lost their lives and even perpetrators themselves have been killed in gun battles with police. Furthermore, vehicles used to flee the scene are often hijacked from civilians.
1.2.5 Inconvenience to bank clients

 Whilst banks are trying to provide ATMs to those in rural areas, these are the ATMs which perpetrators first blew up when ATM bombings started. In such areas, when an ATM is destroyed by a bomb attack, people often have to travel long distances to access another ATM. For some it might mean having to take a taxi, sometimes two taxis, in order to get to an ATM.

 According to the Financial Services Charter, banks must ensure that there are “branches and service centres with a transactibility function, where customers can withdraw and deposit cash or view bank statements, within 10km of 80% of people earning a monthly income of less than R2 500” (Standard Bank, 2008: 90). This means that banks need to provide ATMs within a 10km radius of people in the country’s lower income bracket and they needed to increase their national banking network coverage by 10%, from 70% to 80% by 2008 (Standard Bank, 2008: 90). However, with regard to Standard Bank who have been most affected by ATM bombings, “out of the 29 centres that have been rolled out since 2004, 8 have been upgraded, 11 continue to operate and 10 have been closed” (Standard Bank, 2008: 90). These ten closures have been principally as a result of ATM bombings (Standard Bank, 2008: 90).

1.3 RESEARCH AIMS

 According to Mouton and Marais (1990: 193), the researcher should state the aims of the project by stating whether the project is exploratory, descriptive, explanatory, analytical or predictive. The aim of this research is to determine the nature and extent of the theft of cash contents by means of the bombing of Automated Teller Machines (ATMs) in the Gauteng Province of South Africa. The researcher wanted to examine and evaluate the security measures that are currently in place at ATM sites with the specific focus on crimes associated with the bombing of ATMs. Moreover, to investigate and analyse the modus operandi of perpetrators of ATM bombings, inter alia looking at such issues as explosives used, time of bombing, location, damage done, and for the development of a perpetrator profile. The researcher aimed to identify limitations in

---

9 See Chapter 5.
10 Most bombings of ATMs, in the period since they first started in 2005, have occurred in the Gauteng Province.
preventative measures currently in place at ATMs in order to formulate practical recommendations.

1.4 KEY THEORETICAL/OPERATIONAL\textsuperscript{11} CONCEPTS

1.4.1 Automated Teller Machine (ATM)
This is a computerized telecommunications device that provides the customers of a financial institution with access to financial transactions in a public space without the need for a human clerk or bank teller. Such transactions by means of inserting a personal ‘bank card’ into the machine and the customer/client accessing his/her own bank account by means of a personal identification number (PIN) which is inputted into the machine before the transaction can continue (Wikipedia, Nd).

1.4.2 ATM attack/bombing
“The unlawful, intentional causing of damage to an automated teller machine or any part thereof, with the intent to obtain cash, through any means whatsoever, with specific inclusion of the use of explosives” (Maree, 2008:2).

1.4.3 ATM safe
Part of the ATM machine that houses the cash. In effect a ‘strongbox’ or safe inside an ATM.

1.4.4 ATM throat
The part of the ATM through which cash is dispensed.

1.4.5 Commercial explosives
Refers to explosives used in the mining industry or for other underground or for example roadwork, dam or other large earthwork construction blasting needs, which can only be used by those authorised to (i.e. certified and trained as a blaster with a ‘Blasters Certificate’).

\textsuperscript{11} Some of the concepts discussed are operational definitions and were put together from an amalgamation of the researcher’s observations, conversations, interviews as well as from expert statements in case docket.
1.4.6 Detonator
Used to cause, initiate, ‘set off” or ignite the explosion/bomb blast.

1.4.7 Igniter cord
Igniter cord is a plastic protected continuous cord of pyrotechnic (fire causing) composition, supported in an inert medium, which burns at a specified rate with an intense and vigorous external flame. Its role is to provide the energy to initiate (set off) capped explosive fuse assemblies by means of the vigorous external flame.

1.4.8 Connector capped fuse
Is used to ensure reliable transfer of the flame from the igniter cord to the fuse. It provides a time delay determined by the burning rate and length of the fuse.

1.4.9 Integrated security system (risk control measures)
The above is a composite phrase which relates to a number of linked concepts, namely: A security aid which would be the piece of equipment or manpower used to improve or add to the overall security system made up of a number of security aids for example CCTV, control room, guards patrolling. When all these are implemented in conjunction with each other a security measure is in place. The way they all operate and are co-ordinated, are based on a clear written security policy which includes procedures and operational guidelines. When the security measures become operational a full security system is now in place which incorporates a number of security principles for example protection layers, concentric circles, hardening of target, siting of lights etc. (underlining for emphasis).

1.4.10 Security Risk Management Model
Rogers (2005: 18), building on the work of other practitioners but customising a basic risk management model to the security environment, developed what he termed a Security (Crime)

---

12 This definition has been developed by Prof. A. Minnaar for lectures given to students for the module: Industrial Security (SEP281H) in the Diploma: Security Management offered by UNISA.
13 In this context the term ‘security’ is applied not to the ‘State’ security field but more to the physical and industrial security environment of access control, loss prevention and protection of residential and business premises.
Risk Management Model.\textsuperscript{14} The Rogers’ developed Security Risk Management Model has nine basic steps that need to be followed in its application.

Step 1: Factors causing crime
Step 2: Security policy and mandate
Step 3: Orientation phase
Step 4: Risk analysis exercise
Step 5: Security survey
Step 6: Security risk control measures
Step 7: Return-on-investment exercise
Step 8: Security risk management report
Step 9: Implementation and evaluation of approved security measures (see Rogers, 2005 for more detail).

1.5 VALUE OF THE RESEARCH

This research was the study of its kind to be conducted in South Africa and more specifically in Gauteng. Banks and other institutions may be guided by the findings of this research to improve any shortcomings and weaknesses of current ATMs, the security measures to safeguard them and initiatives that might be revealed from the research analysis. To the discipline of security science, this project creates opportunities for more research to be conducted in the field of banking security, since it is the first study of its kind. Chapter 3 identifies of various other banking security problems that can be researched.

\textsuperscript{14} This model forms the basis of the risk assessment and risk analysis in the security management undergraduate security modules taught to security management students at the University of South Africa (UNISA) undertaking the Diploma in Security Management and the BTech in Security Risk Management degree studies.
2.1 INTRODUCTION

De Vos et al. (2003: 79), the main aims of quantitative research is to “measure the social world objectively, to test hypotheses and to predict and control human behaviour. In comparison to this, De Vos et al. (2003: 79) explains that the qualitative researcher is concerned with understanding; naturalistic observation; and the subjective exploration of reality from the viewpoint of an insider as opposed to the outsider perspective that is dominant in the quantitative paradigm.

This study made use of qualitative research methodology. In doing so, the researcher attempted to gather information in order to gain an in-depth understanding of the nature and extent of ATM bombings in Gauteng. Qualitative research methodology made it possible for the researcher to collect information from a variety of sources.

Given the nature of the crime, it was difficult for the researcher to access information from certain specific sources. As a result of this shortcoming and the exploratory nature of the research, the information was gathered largely through an in-depth analysis of media reports. Newspaper articles (from both printed and online sources) which reported on ATM bombing incidents in Gauteng were used as well as from other provinces. Docket analysis of SAPS ATM bombing dockets\textsuperscript{15} as well as those internal investigation dockets\textsuperscript{16} from the private company, ATM Solutions were used. Unstructured one-on-one interviews with commanding officers from the SAPS Serious and Organised Crime Section (SOCS) were conducted, specifically those dealing with ATM bombings, cash-in-transit (C-I-T) heists and bank robberies, as well as with security investigators at ATM Solutions. Given the fact that the topic of ATM security (or banking security) is of a sensitive and confidential nature, information regarding ATM security measures was gathered only through an ATM site audit. This included physical security

\textsuperscript{15} From the list of CAS docket numbers for Gauteng ATM bombings supplied to the researcher by SABRIC, A total of 214 dockets were randomly selected. Of these only 100 were analysed on a proforma sheet for in-depth information as the remainder had no information besides the initial report on the ATM bombing.

\textsuperscript{16} A total of sixty-two ATM Solutions dockets were analysed.
measures) and from what was said by bank custodians to the media.

2.2 THE RESEARCH DESIGN

The researcher chose to utilise qualitative research methodology. The qualitative research design used was that of a case study as it allowed for the exploration of a single case (in the context of this research – ATM bombings) over a period of time (Creswell, 1998: 61, cited in De Vos, Strydom, Fouché and Delport, 2002: 275). Babbie and Mouton (2007: 281) indicate “studies of events roles and relationships” as a type of case study, explaining that the focus in this type of case study is on a specific event such as a particular type of crime.

The case study strategy allowed for the exploration and description of ATM bombings to occur through in-depth data collection methods involving multiple sources of information that are rich in context (De Vos et al, 2002: 275).

2.3 POPULATION AND SAMPLING PROCEDURES

The target population for this study was SAPS detectives and information officers, and security investigators at the security department of ATM Solutions.

While other participants were identified for example banks security consultants, the sensitivity of information regarding ATM security as well as the nature of ATM bombings made it increasingly difficult to gather information from such sources (as per paragraph 2.5).

The researcher used the snowball sampling method since this research involves the identification of hard-to-reach individuals and the snowball sampling method allowed for available respondents to provide names of other respondents. For example, upon receiving permission to work with SAPS SOCS, the researcher was introduced to members of the special task team dealing with ATM bombings, who in turn introduced the researcher to explosives experts of the SAPS explosives unit.

ATM Solutions was identified as a private organisation, dealing in the distribution of ATM
machines including certain bank branded ATMs as ABSA and Standard Bank. Due to the effects of ATM bombings on the company, they established their own internal investigation unit to assist with the investigation of ATM bombings and other ATM related crimes.

After a meeting with Mr Schalk Burger who is the Head: Security Services and Mr Riaan du Preez a Safety and Security Specialist, permission was granted to work with the company’s Security Department. Investigators at the company were identified and interviewed through Mr du Preez and Mr Burger.

With regard to media reports, a total of 187 newspaper and online news articles were collected and analysed. The researcher collected all articles that could be found that was related in any way to ATM bombings.

2.3.1 Risk categorisation
With regard to ATM site audits, sites were selected in terms of high risk, medium risk and low risk factors.

For the purposes of this research the following categorisation applies:

- High risk sites were identified as those in isolated areas in townships or rural areas. These ATMs are usually portable type (but not limited to), stand alone machines situated outside a shop. High risk ATMs may also include built-in type machines at the corner of streets. This is due to the fact that the corner of streets makes for easy access and getaway.

- Medium risk sites were identified as those portable/built M in types in shopping complexes in the suburbs and areas known to be busy.

- Low risk ATMs were identified as those attached to banks, in shopping malls and garages. The reason for this is that ATMs at banks will usually be surrounded but more security measures. Those in garages mean there are always people around and are usually situated inside a garage store and ATMs in shopping malls are usually inside and often attached to a bank. In-store ATMs also fall under this category.
2.3.2 Criteria for risk ratings according to ‘Hot Spot Model’

The criteria for risk ratings used by all contributors to the Hot Spot Model are as follows:

- **Low risk** - Situational, environmental and social risk factors are considered in the criteria as salient.

- **Medium risk** - The above-mentioned factors are extended with criteria that focus on repeat victimisation and reported suspicious activities, related to vehicles and persons.

- **High-risk** - Criteria include all of the above stated criteria, as well as specific information related to the high probability that a crime will occur within the stated period and area identified within the Hot Spot Model. The listing of a specific shopping centre means that all businesses including C-I-T companies are at high risk, because of possible crime displacement.

Banks, shops, post offices and garages situated in the same street or town are at equal risk in relation to the Hot Spot Model being utilized (SACSC, 2008: 4).

2.3.3 Sampling of SAPS case dockets

Docket numbers that is SAPS CAS numbers were provided in the form of an incident report from SABRIC. Case dockets obtained from the SAPS were initially selected on the basis of police stations to which they were reported having more than nine such reported incidents of ATM bombings based on SABRIC’s incident report. However, due to the fact that the crime of ATM bombings is regarded as serious organised crime, all dockets were sent to the SAPS SOCS unit in Germiston. As a result of this and other issues the researcher was forced to work with the dockets that were available at the SAPS SOCS office. This amounted to a total of 100 dockets as opposed to the initially selected 214 dockets from seventeen different police stations across Gauteng. Additionally, the researcher was told that all other dockets were sent back to the respective police stations where they were to be filed. Most of these dockets were filed at SOCS as undetected, with the exception of one (1) court docket that the researcher managed to get hold of. If the researcher were to attempt to locate each of the dockets in the initial list, which may or
may not have been sent back to the stations the researcher was informed that she would have had to reapply for permission from SAPS head office to visit each of the identified stations in addition to arranging personal permission from each of the station commissioners involved. Given the fact that there was no clear record of the exact location of each docket and that it took months to obtain permission initially, it was not feasible for the researcher to take such a route.

2.4 DATA COLLECTION METHODS

During the data collection process, the researcher made use of different qualitative data collection methods. These included one-on-one unstructured interviews, document study as an information collection technique, which was inclusive of docket analysis by means of a pro forma data/information sheet, and ATM site audit as an observation strategy.

2.4.1 One-on-one unstructured interviews

When conducting interviews, the researcher aimed at gaining as much information as possible from the interviewees regarding the situation of ATM bombings from their investigation experience and knowledge of the crime. The researcher chose to conduct unstructured interviews. Interviewees were prompted by merely being asked to share their views of the nature and extent of ATM bombings in Gauteng. Thereafter, the researcher posed additional probing or follow-up questions to those interviewees where information was lacking in detail or clarity. According to Rubin and Rubin (1995: 145 cited in de Vos et al, 2002: 299), “the interviewer probes to complete or clarify the answer or to request further examples or evidence.” The exploratory nature of this research made the use of unstructured interviews essential in order to obtain as much information as possible.

Where interviewees failed to speak about certain areas of interest of the researcher such as a syndicates size; degree of dangerousness or explosives, the researcher asked specific directed questions pertaining to those topics. However, it was not often that the researcher needed to do this, as interviewees were generally enthusiastic and spoke about almost all issues in the area of ATM bombings. In fact some interviews went on for just over two (2) hours.
Those that were interviewed included the following:
Two Commanding officers of SAPS SOCS involved with the investigation of ATM bombings and three security investigators at private company ATM Solutions. The selection of commanding officers only was due to the unavailability detectives for interviews.

2.4.2 Document study as an information collection technique
One of the sources the researcher used was “mass media” as referred to by De Vos et al (2002: 324). These took the form of newspaper articles and online news media which reported incidents of ATM bombings and other information pertaining to the topic. These include arrests of suspects and proposed measures to curb this specific crime. According to De Vos et al (2002: 322), although documents aimed at mass media, such as newspapers, magazines or newsletters are written for the purpose of informing the public, if “studied and analysed for the purposes of scientific research, the method of document study as a data collection method becomes operative.”

Another source of document study referred to by De Vos & Strydom (2002: 323-324) and utilised by the researcher is that of “official documents”. For the purposes of this study, the official documents referred to by De Vos & Strydom, took the form of official case dockets on ATM bombings from the SAPS and internal investigation dockets from the investigations undertaken of ATM bombings carried out by ATM Solutions. De Vos & Strydom (2002: 324) speak about the issues regarding accessibility of such documents, owing to legislation and confidentiality of such information. As such, the researcher obtained written permission from SAPS head office and ATM Solutions Executive Committee in order to be allowed access to and use such information.

Only those dockets available at SOCS were perused and information collected by means of a standard proforma sheet as per Annexure A.

Investigation case dockets from ATM Solutions were also perused in very much the same way as the available SAPS case dockets. However, given that ATM Solutions had only started their own internal investigations (in collaboration with the SAPS) since 2009 all incidents investigated by
their Security Department took place only in 2009 and there was no information available in such a form relating to ATM bombing incidents prior to 2009. A total of 62 dockets from ATM Solutions were perused and analysed.

2.4.2.1 Clustering and coding of media reports
All media reports were divided into different categories of information, according to the ATM bombings it was reporting about. As such they were divided into the following categories:

- Articles reporting on a specific ATM bombing incident/s;
- Articles related to arrests, convictions and killings (through attempted arrest) of ATM bombers;
- General reports on ATM bombing (statistics etc.).

Thereafter articles were entered into a table in the form of a proforma sheet with the headings as per Annexure A. These proforma sheets reflect the objectives of the research.

2.4.3 Analysis of closed circuit television (CCTV) footage as a form of data collection
The researcher found it difficult to classify CCTV footage as a type of document study as the footage provided was confidential and formed part of evidence collected as per the investigations. However, such CCTV video footage that was accessed from internet sites can be classified as “mass media” referred to above (paragraph 2.4.2).

Other video footage, not available to the public, used in this research is referred to as an ‘official document’. Such video footage formed part of the evidence collected during investigation by ATM Solutions, who kindly provided them to the researcher.

The CCTV footage viewed on internet sources as well as those provided by ATM Solutions amounted to fifteen (15) such videos. The researcher viewed footage and made detailed notes of activities of perpetrators in the duration of the crime i.e. in the course of the crime or during the crime.

17 These were not put into a separate data base, rather, they were incorporated into the other data bases depending on the information it reported.
2.4.4 ATM site audit as a form of observation

Simple observation was undertaken by the researcher based on a survey audit security measures proforma sheet. Bless and Higson-Smith (2000: 103) explain that simple observation involves the recording of events as observed by an outsider and although it seems straightforward, it must be pursued in a systematic manner in order to obtain usable data. Accordingly, the researcher made use of an audit checklist on current security measures of a sample of 15 different bank brand ATMs in Gauteng, based on degree of risk, (as per categories discussed above with results of such site audit discussed in Chapter 4). Accordingly five ATM sites of each risk category and randomly inclusive of the four major banks (ABSA, Standard Bank, Nedbank and First National Bank) were chosen. In addition it included all different types of ATMs. The exact location of the ATM sites will not be mentioned here.

2.5 PROBLEMS ENCOUNTERED DURING RESEARCH

2.5.1 Sensitivity of information

ATM bombings impact on the banking industry, which made it difficult to collect information from a number of specific sources. Information regarding ATM security measures and/or ATM design for example is confidential banking information. Should such information be made available for public access, it could pose a serious threat to the banking industry by effectively providing a “manual” for criminal minds. As a direct consequence of this, it became difficult for the researcher to interview or obtain permission to speak to ATM security consultants and/or others working closely with cases of ATM bombings at banks. They were not able and somewhat unwilling to give out detailed information regarding ATM security measures or information regarding ATM safes, which play a major role in the securing of cash at an ATM.

Explosives experts were also reluctant about providing detailed information regarding the types of explosives used in such a crime. While explosives experts were not specified in permission letter, an initial meeting with members of SOCS included explosives experts who agreed to assist. However, after numerous efforts to arrange an interview with SAPS explosives’ experts, the researcher was not contacted to arrange a date and time as continuously promised. It is the

---

18 See Chapter 4
belief of the researcher that despite being granted approval by SAPS head office and the initial arrangement, explosives experts were wary of providing such information. As a result the researcher had to base information on explosives on internet searches, media reports and in expert statements attached to SAPS case dockets.

During interviews with commanding officers from SAPS SOCS, interviewees resorted to providing certain information ‘off the record’, and were seemingly enthusiastic to divulge “certain information once the tape recorder had been turned off”. This was an indication of the sensitivity level attached to the information provided.

2.5.2 Availability of candidates
The issue regarding sensitivity and confidentiality of certain information had a massive impact on availability of candidates for one-on-one interviews.

In general, the researcher was turned down by a number of detectives due to their heavy workload i.e. having to be at court, and manpower shortages. By the time the researcher had been granted the permission required for the fieldwork research to occur, the specialised task team initially established to tackle ATM bombings in Gauteng, had been dismantled and other units were being put together.

The researcher experienced similar issues when attempting to conduct interviews with security investigators at ATM Solutions. As a result, the researcher came to a point where an interview was conducted with two people at the same time. Given time constraints and other scheduled research activities, the researcher was unable to make additional time available to revisit those candidates who were unavailable when interviews were due to take place.

Due to interviewees’ workloads, the researcher was continuously disturbed during interviews at ATM Solutions, by ringing phones and people walking in and out of the office. This made it increasingly difficult to keep the interview conversation focused.
2.5.3  Time constraints

The application for permission to access information on ATM bombings in the form of SAPS case dockets and interviews with detectives took a number of months to finalise. This put strain on the researcher’s time limit to complete the research. Permission to view case dockets alone was dependent on receiving an incident report\textsuperscript{19} from the South African Banking Risk Information Centre (SABRIC). This in turn was only granted upon receiving permission from SAPS to access SAPS dockets. The SABRIC list of case docket numbers was crucial to identifying where the case dockets were. The SAPS did not have a separate ATM bombings list of case docket numbers, since it is not listed on the SAPS CAS system as a separate crime category.

2.5.4  Issues with regard to docket analysis

2.5.4.1  Accessibility of dockets

Upon receiving the SABRIC incident report from SABRIC, the researcher made a selection of 17 police stations from Gauteng which contributed a total of 217 reported cases. This selection was based on choosing stations where a minimum of nine ATM bombing incidents were reported at a specific station. The selection also included all areas in Gauteng. The researcher, after having received a letter from SAPS Strategic Management granting permission to look at dockets, learned that all dockets pertaining to ATM bombings were located at SOCS in Germiston, Gauteng. Certain dockets that were filed as “undetected” had made their way back to the stations. There was no record of those that had been sent back to the stations to be filed. Those that were still with SOCS, as well as uncertainty pertaining to whether they were in fact at the station or part of a court docket, only those dockets that were available at SOCS, which amounted to 100 dockets were used.\textsuperscript{20} In addition, all of these dockets had at the time of the research been closed, due to insufficient evidence and filed as ‘undetected’.

Court dockets of ongoing cases were difficult to access as detectives were always busy with them or they were in court. As a result, the researcher was only able to peruse one such docket, where the alleged suspect confessed to involvement in eleven ATM bombings across Gauteng.

\textsuperscript{19} Such an incident report consisted of a list of ATM bombing incidents occurring in Gauteng and was inclusive of SAPS CAS numbers. As per Annexure C (annexure does not include CAS numbers)

\textsuperscript{20} This number excludes court dockets and duplicate dockets (in cases of missing dockets)
The court docket consisted of case dockets pertaining to five of the incidents, which brought the number of dockets analysed to 106 with the majority being cases that were undetected.

2.5.4.2 Language barriers
In the duration of docket analysis, the researcher found that a large number of dockets included expert statements that were in Afrikaans. The translation of such statements delayed the process of the docket analysis and made it difficult for the researcher to understand as she was unable to adequately translate them. A smaller percentage of dockets included other statements and/or investigation diary notes that were in Afrikaans, which resulted in translation issues.

2.5.4.3 Illegible handwriting
Whilst the majority of dockets were easily readable the researcher experienced difficulty with the handwriting in some of the statements. Some investigation diary notes were completely unreadable. The researcher was forced to eliminate some of the information contained in unreadable documents from the data collection process.

2.5.5 Issues regarding ATM site audits
Conducting ATM site audits was necessary to determine ATM security measures and make recommendations for improving such measures. The only security measures available to “see” at an ATM are those of a physical security measures nature. During the perusal of dockets, the researcher came to learn of an ATM alarm that is installed in ATMs and are triggered when someone interferes with the ATM. Such alarms are not visible at the ATM and as a result were not included in the site audit checklist. In addition, security measures regarding safes could not be established.

2.5.6 Challenges in transcribing interviews
In the absence of an electronic transcriber the researcher spent numerous hours transcribing interviews. The period of time taken to transcribe was lengthened due to ongoing background noise. The taped interview was difficult to hear clearly above the background noise in the interview conducted with one of the commanding officers at SAPS SOCS offices. During the interview, cleaning was taking place in the form of vacuuming and the sound of the vacuum
cleaner is dominant on the tapes. The walls of the office in which the interview was held were thin as it was made from rhino board. The loud voices of people in other offices, made it difficult to hear what was being said by the interviewer and interviewee.

2.6 DATA ANALYSIS

The data and other research information that was collected was collated, ordered, analysed and interpreted. The data analysis began with the organisation of the collected data. This entailed making an inventory of what the researcher had found and to see how complete the data was. The interview data was then transcribed and clustered in categories and themes. Data from media reports, docket analysis and CCTV footage, was clustered into themes and categories according to those categories used in the proforma sheets for docket analysis and media reports.\(^\text{21}\) Where required, simple arithmetic was used to count common information (for example the total number of SAPS dockets where the incident involved an FNB ATM machine). Simple arithmetic was also used to calculate certain percentages. For example if 43 of the 100 dockets analysed involved FNB ATMs, then the percentage was calculated as follows: \(\frac{13}{100} \times 100 = 12\%\).

Data pertaining to the modus operandi information was dealt with separately from other data. Such information was read and re-read and grouped (clustered) according to different themes and categories of information such as the use of a crowbar to widen an ATM throat and manner in which entrance was gained. This information was thematically coded and analysed.

Analysis of media reports proved to be a lengthy process in that information is provided largely in the form of interviews conducted by reporters. Most newspaper articles did not provide all the information that was required. The abovementioned proforma sheets of categorised information now take the form of databases of collated research information which are in the researchers’ possession. Each database was thematically analysed to form the findings discussed.\(^\text{22}\)

\(^{21}\) See Annexure A

\(^{22}\) Given that the findings were drawn from the information in each database compiled, they will be referenced as such throughout this dissertation. It would be impractical to reference each and every media report and/or docket that contained the information being discussed in a finding.
2.7 VALIDITY, RELIABILITY AND ACCURACY OF COLLECTED INFORMATION

2.7.1 Ensuring validity
To ensure validity the transcribed interviews were cross checked with handwritten notes. Anonymity and confidentiality of respondents was upheld where requested. The same questions were asked to all the interviewees. Where information was supplied by an interviewee the information which differed was noted. The researcher avoided being biased and avoided asking leading questions during the interviews. Interviewees freely provided the information themselves, without any prompting or leading. Where information provided by interviewees was ambiguous, the researcher probed for clarity.

In order to ensure validity of media reports, the researcher compared media reported information to that included in case dockets. In addition, seemingly fictitious information in the media reports were posed as questions to investigators for clarity of such information.

Information provided in interviews was also compared to information in case dockets.

2.8 ETHICAL CONSIDERATIONS

The researcher obtained written consent from the SAPS and SABRIC to conduct the research (See Annexure F). The participation of interviewees in the study was on a voluntary basis, and the researcher confirmed with each interviewee what information could and could not be used in the research report. All the interviewees and other involved people were informed about the reason for the study and what it aims to achieve. In the process, all the information gathered was handled confidentially and the guaranteeing of the anonymity of interviewees who requested it. The UNISA Code of Research Ethics was adhered to at all times in order to stick to quality, confidentiality and anonymity.

During the perusing of SAPS SOCS dockets, personal information regarding witnesses, complainants, victims and banks were not used in any way. A confidentiality agreement was also signed directly with ATM Solutions.
2.9 CONCLUSION

The information pertaining to ATM bombings is a sensitive topic in the banking industry as well as in policing. The seriousness of the crime in terms of the threat posed, the mere fact that it involves large amounts of money and the use of commercial explosives makes it a topic that experts in the field are reluctant to discuss in detail. However, from the information that is available to the public as well as certain other information provided in official documents, the researcher was able to analyse the data and find similarities and dissimilarities, draw on certain themes identified and make conclusions based on such information.
Chapter 3
AN OVERVIEW OF BANK SECURITY THREATS

3.1 INTRODUCTION

While the focus of this research is on ATM bombings, there exists a number of other crime risks that the banking industry faces. ATMs in particular are vulnerable to a number of other crime threats which are both violent and non-violent in nature. There is a lack of literature relevant to bank security concerns as well as that which is specific to ATM security concerns.23

Owing to the lack of literature on banking security, this chapter addresses only the most prominent bank security threats. While the researcher could not find any books written in recent times that discuss issues pertaining to bank security, the information used in this chapter was drawn from earlier writings. These date back to the early 1980s and based on American bank security issues at the time and a few other sources.24 The small amount of relevant information located by the researcher has been put together in this chapter to provide a brief, but comprehensive overview on bank security threats. The focus is on ATM crime threats and methods of protection. Information regarding such issues in the banking industry in South Africa as methods of protection is limited and difficult to come across, due to their sensitive nature. As discussed in Chapter 2 many people associated with the banking industry are reluctant to provide detailed information regarding bank security. Barnes (2008: 2) points out that South African commercial banks do not, for obvious reasons, generally release details of the amount of cash taken during an armed robbery or the security measures implemented at their branches.

3.1.1 Reasons pertaining to non-disclosure of information regarding banking security

Because certain violent crimes affect the bank security,25 the South African banking industry26 is often reluctant to publicise improvements and upgrades in security measures. They fear that if

23 It should be noted here that the security concerns spoken about here are those which relate to the ATM physical site crime risks and exclude those related to information security and cyber crimes as those extend beyond the scope of this research.
24 These consist mostly of internet sources, including bank websites and information brochures.
25 Cash-in-transit heists, bank robberies and ATM bombings.
26 This includes banks, SABRIC, private ATM providers as well other institutions involved in banking security.
criminals have knowledge of what security measures are in place at an ATM, they will find a means of overcoming or bypassing them during the planning of their crimes, hence making the success of their crimes more probable.

The following are some reasons why a bank will not disclose sensitive information regarding security measures:

- If everyone knew what security measures were in place at banks then anyone would be able to find ways to bypass them.
- If people were aware of all the procedures in place, then they would know when, where and how to gain access to the bank’s money.
- It would make it simple for criminals to target banks, ATMs and cash-in-transit vehicles and successfully gain access to cash (Kole, 2010: 84).

The abovementioned reasons involving non-disclosure of information is understandable if one takes into consideration the financial, infrastructural and reputational loss that the banking industry is confronted with when crimes of a violent nature, that also pose risks to their clientele, occur on a daily basis. In addition, while crimes of a non-violent nature do not pose a risk of threat of violence to society, they still cause great financial, reputational (and in some cases infrastructural) loss to the banking industry and their clients.

### 3.2 BANK SECURITY THREATS

In this section only the most prominent threats facing the banking industry will be discussed. While the number of bank security threats may extend far beyond what is discussed here, those issues fall outside the scope of this research. The focus will be on violent threats at both branches and ATM sites (which will include C-I-T) and other (non-violent) ATM crime risks that pose an ongoing concern to banking institutions and their clientele.
3.2.1 Armed robbery

The discussion on violent threats will be focused on armed robbery. Armed robbery includes its sub-categories of bank robbery, cash-in-transit (C-I-T) heists and ATM attacks\(^\text{27}\) with the use of explosives. There are apparent similarities in the *modus operandi* between the perpetrators of all three crimes. This can be attributed to the fact that in most cases it is the same perpetrators that are involved in all three crimes. According to Maree (2008: 3) it has been confirmed that in South Africa the bank robbers who robbed banks are now also involved in C-I-T robberies and ATM bombings. In these bank-related crimes, the criminals are also involved in armed robberies targeting for example casinos and jewellery stores (Maree, 2008: 3).

A national crime situation report dealing with the national serious crime figures and ratios for the 2006/2007 financial year indicated the following with regard to C-I-T robberies and bank robberies. It also indicates certain similarities in such violent crimes with regard to the size of gangs and the amount of cash stolen:

*In less than 10% of C-I-T and bank robberies there are more than eight or even more than six perpetrators involved. Groups of between two to five perpetrators were involved in 73% of the C-I-T robberies and 78% of the bank robberies.*

*In 71, 7% of bank robberies and 70, 2% of C-I-T robberies respectively the amounts of money robbed were less than R200 000-00. In only 6% of bank robberies and 10% of C-I-T robberies did the amounts robbed exceed R1 000 000-00 (SAPS: 2007: 21).*

Maree (2008: 3) explains that in committing armed robbery against different targets the adaptive skills of criminals come to the fore. The perpetrator/s will, therefore, use the same *modus operandi* irrespective of the target, but will adapt their *modus operandi* according to the target. For example, entrance can be gained by taking a guard posted at a selected target hostage. He is taken into a bank or jewellery store during the robbery, while at a casino he is held hostage outside to create the impression that all is in order, without attracting attention (Maree, 2008: 3).

\(^\text{27}\) ATM attacks can also be seen as burglary.
3.2.2 Bank robbery

This type of crime includes the robbery at a bank branch. By definition, armed (bank) robbery includes the unlawful, intentional and violent removal and appropriation, or attempted removal and appropriation, of movable property (e.g. cash) whilst under the control of a bank by means of violence, or a threat of violence, where the victim has to believe that the perpetrator will, or is capable of making use of the indicated violence (Maree, 2008: 2).

According to official statistics, bank robbery in South Africa has increased by 11.6% between 2006/2007 and the 2007/2008 financial years as depicted in Figure 2.1.

In actual numbers this percentage is an increase from 129 in the 2006/2007 financial year to 144 in the 2007/2008 financial year. The figure of 129, as reported for the 2006/2007 financial year, increased from only 59 in the previous financial year (SAPS, 2008). However, from the 2007/2008 financial year to 2008/2009, bank robberies decreased by 29.2%, i.e. from 144 to 102.

Figure 3.1: Bank robberies: 2003/04-2008/09

Anderson (1981: 2) illustrates the gravity of bank robbery by pointing out that in the United States of America (USA) the Bank Protection Act in 1968, which was enacted by the US
Congress, was triggered more by the crime of bank robbery than any other bank-related crime. This was largely due to the rapid rise in bank robberies in the USA at the time. Being a crime of a violent nature that is directed at people (frequenting the selected target institution) it is therefore usually of much greater concern than the numerous bank-related crimes directed at property alone (Anderson: 1981:2). In present day bank robberies are not the only bank-related crime which is of a violent nature that poses an actual or potential risk of injury to people.

Barnes (2008: 3) is of the opinion that the foremost factors that contribute to an increase in bank robberies are that “there are more bank branches with extended business hours; banks still remain a very lucrative robbery target; and bank robberies are usually fast, low risk crimes”.

Branches are inclined to have standardised designs with foreseeable and fairly predictable standard layouts and operating procedures and bank guards are unarmed. The reason for this is that it could trigger a gun fight and customers and employees could be injured or killed. Employees are instructed to be compliant and the majority of robbers evade arrest, particularly at the scene of the crime (Barnes, 2008: 4).

3.2.3 Cash-in-transit attacks/robbery
Here the researcher refers to the robbery of C-I-T security during the transportation of cash from one point to another, and usually includes the use of violence or the threat thereof. It may also include the direct robbery of cash in carry cases for transport of C-I-T personnel during the loading of the cash of an ATM or delivering of cash to a bank branch. C-I-T robbery pertains to the “unlawful, intentional and violent removal and appropriation of movable assets in transit while the assets are under the control of a security company. This may include incidents inside or outside a bank and/or other premises, depending on the circumstances. This may further include removal and appropriation of movable assets under the threat of violence. The main consideration is that the movable assets must be under the control of the security company/guard” (Maree, 2008: 2).

The Global ATM Security Alliance (GASA) distinguishes between two types of C-I-T attacks; “Inside Premises” attacks and “Cross Pavement” attacks (ATMIA, 2005: 26). Inside premises
attacks take place when “the cash carrier is replenishing cash within the premises where the ATM is located” (ATMIA, 2005: 26). A gang on average enters the ATM area prior to arrival of the C-I-T company personnel and “lays an ambush” (ATMIA, 2005: 26). Weapons and extreme violence may be used with the cash carrier being forced to handover the cash.

During cross pavement attacks diverse modus operandi are employed, the most common of which is to attack the cash carrier, in order to snatch the cassettes, after the cash cassettes have been removed from the armoured vehicle for delivery to the ATM (ATMIA, 2005: 26). As in the case of ‘inside premises attacks’ weapons, intimidatory threats and extreme violence may be used.

The national crime situation report for the 2006/2007 financial year indicated the following with regard to the use of weaponry and violence during C-I-T attacks:

Case analysis of C-I-T and bank robbery incidents reported during 2006 by SABRIC and the CIAC [SAPS Crime Information Analysis Centre] revealed inter alia the following: In the majority of C-I-T cases (55, 5%) the security officers were either held at gunpoint or overpowered by armed perpetrators, while in 8, 0% the perpetrators opened fire on the security officers and in another 7, 2% the security officers were actually shot and seriously injured. By far the majority of the above 70,7% of cases involved instances in which the security officers were busy collecting money from businesses or carrying the cash to/from the armoured vehicles (i.e. so-called cross-pavement robberies)(SAPS, 2007: 20).

On identifying key concerns and considerations associated with the physical ATM site, Winters (1986: 12) spoke of ‘service personnel safety’ as one of these concerns. Whilst not clearly stated, one can presume that this refers to the safety of the cash-in-transit (C-I-T) personnel and may also include bank custodians called out to retrieve cash from an ATM that had been damaged.28

The job of cash-in-transit personnel usually entails the loading of cash into an ATM, including

28 This is often the case when an ATM is bombed. A bank custodian is one of the people called out to a scene to retrieve the cash from the blown up ATM.
transportation from cash hold facility to ATM site or transporting cash from a cash-holding facility to a bank branch (ANON, nd). Given their job description, these people often have access to or are in possession of a large amount of cash. According to Winters (1986: 12), depending on the policy of the financial institution, their service calls can occur at rather late hours and therefore “every effort must be made to ensure that security measures are taken to protect them and give them the edge in dealing with a potential security threat”.

Prior to the increase in ATM attacks, the robbery/attack of C-I-T security became a major cause for concern to the banking industry and law enforcement. Accordingly, SAPS statistics illustrate that C-I-T robberies increased steadily from 192 in the 2003/2004 financial year to 220 in 2004/2005 (SAPS, 2009). By the 2006/2007 financial year, the number of reported C-I-T robberies reached 467 (SAPS, 2009). During the 2007/2008 and 2008/2009 financial years, the number of incidents decreased by only 9, from 395 to 386 reported incidents (SAPS, 2009).

The following graph (Figure 3.2) indicates the occurrences of C-I-T robberies in South Africa for each financial year from 2003/2004 to 2008/2009. As indicated in the graph below, between the 2003/2004 and 2006/2007 financial years an upward trend is prevalent, with the greatest increase of 163 occurrences occurring between 2005/2006 and 2006/2007. However, after its peak in 2006/2007, the number of C-I-T attacks began to decrease and continued to do so until the release of the 2008/2009 crime statistics. The number of incidents decreased by -15.4% in 2007/2008, and at the same time ATM attacks were increasing considerably which is suggestive of syndicates changing their crime (or adapting their modus operandi29) due to the increased police and business focus on C-I-T robberies.

---

29 As discussed in paragraph 4.1 above
3.2.4 ATM attacks

An ATM attack is defined as the “unlawful and intentional causing of damage to an automatic teller machine or any part thereof, with the intent to obtain cash, through any means whatsoever, with specific inclusion of the use of explosives” (Maree, 2008: 2). An ATM attack may also be referred to as an ATM burglary. Winters (1986: 12), identifies the “threat of burglary” as one of the key concerns and considerations associated with the physical ATM site. The threat of burglary can be seen as attempts by criminals to access cash by burglarising or breaking into the machine. He explains that as the criminal element in society becomes more aware of the amount of cash contained in some ATMs, and as the number of remote stand-alone machines grows, the more vulnerable banking institutions will become to having their ATMs or cash dispensers burglarised.

The bombing of an ATM using commercial explosives can be considered a burglary of an ATM as the perpetrator intentionally and unlawfully breaks into the ATM structure using an instrument or explosives in an attempt to gain access to the safe housed by the ATM structure.
and thereafter commit a crime, i.e. the theft of the cash. The Global ATM Security Alliance (GASA) defines an ATM burglary as “the use of force, usually involving technology equipment such as angle grinders, blow torches, and explosives to break into the inside of an ATM on site in order to steal the cash stored in the machine” (ATMIA, 2005: 28).

The issues surrounding the crime of ATM bombings will be discussed in greater detail in chapters four and five and this discussion will stem from the actual research findings of this study. When ATM bombings first started ATM security measures were inadequate to deal with such attacks. As a consequence such security inadequacies resulted in the increasing success of ATM bombing gangs in accessing the ATM safe. While improved policing methods and success in arrests have by 2009 led to a decrease in ATM bombings, given the nature of the criminal activity of organised crime syndicates, this number is likely to increase again unless the banking industry can find a way to prevent criminals from accessing the safe, even if explosives are used. Anderson (1981: 92) explains that security and protection of ATMs against physical attack and fraud receives very little attention in the planning phase of the design ATM and/or siting of the ATM. As a result, when ATMs are physically attacked, the bank is faced not only with the cost of repairing or replacing the damaged ATM, but also with the cost of improving security measures that are in line with the method of the attack. This will either delay or prevent such attacks and thereby reduce their incidence. Anderson (1981: 92) points out that “many banks simply rely on the minimum [author’s own emphasis] standards without recognising that these minimum standards are ‘bare bones’ and pertain to limited physical protection against external attack”.

Another burglary issue pertaining to ATMs in South Africa is what is commonly referred to as “grindings”. In such a scenario, the perpetrator uses an angle grinder to cut open the ATM structure and also to open the ATM safe. This method is most commonly used on in-store ATMs. Another burglary issue pertaining to ATMs in South Africa is what is commonly referred to as “grindings”. In such a scenario, the perpetrator uses an angle grinder to cut open the ATM structure and also to open the ATM safe. This method is most commonly used on in-store ATMs.31

In overseas countries, specifically those in the United Kingdom, criminals use other methods to attack ATMs such as ram raids and gas attacks.

30 See Chapter 1 (page number?)
31 Information provided during informal meeting with ATM Solutions security personnel, Schalk Burger and Riaan du Preez, 1 October 2009.
3.2.4.1 Ram raids

Ram raids often take place in the early hours of the morning in areas where the police response times might be slower than normal (ATMIA, 2005: 29). One can differentiate between ram raid methods at externally sited ATMs and internally sited inside a building/mall ATMs.

At externally sited ATMs’ ram raids consist of “highly organised activity often involving the use of three vehicles and industrial equipment whereby the ATM surround is chiselled out and an industrial wire is placed around the machine. A transit van is reversed towards the ATM; wire is fed through the back and front (windscreens removed) and attached to a tow bar on a 4x4. The 4x4 pulls away and drags the whole ATM into the rear of the van” (ATMIA, 2005: 29).

For internally sited ATMs, the free-standing ATM is “lassoed, the rope is then tied to a vehicle which pulls away and removes the ATM away from [floor or wall] anchoring and the ATM is stolen whole” (ATMIA, 2005: 29). The cash is later removed from the cassettes away from the robbed premises.

While this is not a daily occurrence in the UK, a Cash Machine Crime Report for the 12 month period to June 2008 indicated at least 15 incidences of ram raids occurred in the UK for that period, while 10 ram raids occurred in the 12-month period to June 2007, indicating an upward trend (APACS & BBA, 2008: 2).

The following photograph depicts the scene at an ATM after a ram raid:
3.2 More common occurrence as reported in the UK, that falls under the category of attacks on ATMs, is that of the removal of an ATM from its premises. It is unclear as to whether the methods used to remove the ATM is similar to ram raids, but the abovementioned report indicated that 60 incidents where ATMs where removed from its premises occurred in the 12-month period to June 2007 and 85 in the 12-month period to June 2008, demonstrating a 42% increase (APACS & BBA, 2008: 2).

3.2.4.2 Gas attacks

During a gas attack on an ATM, criminals inject gas through apertures in the ATM (e.g. acetylene gas or Calor gas) and use a pyrotechnic fuse to ignite it. The fuse is usually electronic (Chrismas, Nd). The explosion destroys the outer shell which blows off the ATM, thereby allowing access to the cash. This is a similar method to the use of commercial explosives. While in most European countries gas attacks on ATMs appear to be isolated incidents, 280 out of 398

---

32 From IBP. Nd. ATM Security Threats: Attack methods, crime trends and counter measures.
attacks on ATMs in Italy in 2004 were with the use of gas and in 2005 there were 270 such incidents in Italy (Christmas, Nd).

The following is a picture depicting the damage caused by a gas attack on an ATM in Austria:

**Image 3.2: Damage caused to an ATM by a gas attack**

3.2.5 Client robbery

‘Client robbery’ refers to the unlawful, intentional use of violent methods or threat of violence to obtain cash from a client after he/she has drawn cash from an ATM or from inside a bank. In such a case the perpetrator will watch his/her victim whilst the victim draws cash and wait for an opportune moment to rob the victim and will not hesitate to use any form of violence (Kole: 2010: 88).

Winters (1986: 12) refers to customer safety as one of his key concerns associated to the ATM site. He emphasises the bank security departments’ role in taking precautions to “assure customers that transacting business at a remote ATM is safe and that they may do so with a sense of personal security.” However, in the 21st century this approach has changed. While customer

---

33 From IBP. Nd. ATM Security Threats: Attack methods, crime trends and counter measures.
safety is still of paramount importance to banks, instead of assuring clients that they are safe, banks have taken to providing clients with advise on precautionary measures that should be observed when transacting at an ATM.

Anderson (1981: 15) identifies a number of concerns faced by the bank security personnel with regard to safety and security around ATMs. One of these is the victimisation of customers using ATMs “by criminals who assault and rob them”. Today we refer to this as “muggings/client robbery”. This may also take the form of “forced withdrawals” and are categorised as “cardholder related” type of ATM crimes by the Global ATM Security Alliance (GASA) (GASA, nd). The researcher categorises these under client robberies as they fit the elements of client robberies.

The following could also fall into the broader category of client robbery as sub-categories of client robbery:

3.2.5.1 Mugging
An (ATM) mugging simply refers to an incident where a “client is physically attacked whilst in the process of conducting a transaction at an ATM machine” (ATM Solutions, Nd).

3.2.5.2 ‘Forced withdrawal’
A forced withdrawal on the other hand, refers to an incident which occurs when a cardholder (ATM user) is forced or intimidated into making a cash withdrawal from his/her account, whereupon the cash is taken by the criminal (SPARK ATM, Nd). “Research has shown that this most commonly occurs at isolated street facing ATMs” (SPARK ATM, Nd).

Given that such crimes exist and could happen to anyone at anytime, instead of giving clients a false sense of security banks provide their clients with measures to prevent them from becoming victims of such crimes. For example, the following information, which was retrieved from the Standard Bank website, informs the bank’s clients of preventative measures that should be taken at an ATM:
ATM security tips

Only use ATMs in well-lit, high-traffic areas. If the lights aren't working, don't use that machine. Stay alert. Look out for suspicious individuals or circumstances. If you feel uncomfortable, trust your instincts and leave the area.

Have your ATM card for your transaction ready and in your hands. Opening your wallet or purse can be time consuming and also provides a potential thief with easier access to your valuables.

Never tell anyone your personal identification number (PIN) and be sure to shield the keypad with your hand when entering your PIN. To further reduce the risk of fraud, memorise your PIN and never write it down.

Be wary of strangers who offer to help you - even if you are experiencing difficulty with your transaction. Don't allow others to distract you while you're banking.

Make sure the card you get back from the ATM after your transaction is yours.
Don't count or expose your money after your transaction. As soon as you receive your money and bank receipt, put them away and leave the ATM area (Standard Bank, Nd).

In addition to such tips provided on various bank websites, notices with similar information often appear on or near ATMs and at bank branches. Annexure B is an example of a poster illustrating security tips and guidelines, used by ATM provider, ATM Solutions.

3.2.5.3 ‘Non-violent threats’ (theft) at or from ATMs

Non-violent ATM crimes involving the client (card-holder crimes) are those of “card swapping”, “card jamming” and “skimming”.\(^\text{35}\)

\(^{34}\) The number of non-violent threats faced by the banking industry are not limited to the contents of this discussion.\(^{35}\) Although non-violent, these may also be included under client robberies.
**Card swapping**
Card swapping involves a scenario “where a customer’s ATM card is swapped for another card without their knowledge whilst undertaking an ATM transaction” (ATM Solutions, Nd). In such a situation the thief offers his assistance to customers and then swaps the cards. These criminals play on the trust of unsuspecting customers (SPARK ATM, Nd).

**Card jamming**
Card jamming is “where an ATM machine card reader is deliberately tampered with so that a customer’s card will be held in the card reader and cannot be removed from the machine by the customer” (ATM Solutions, Nd). In such a case the criminal who jammed the card reader, will remove the card once the customer has departed (ATM Solutions, Nd).

**Card skimming**
Card Skimming is the copying of the encoded information on the magnetic stripe of a legitimate card, making use of a card reader, for fraudulent purposes and utilising the data to encode counterfeit or lost or stolen cards (SABRIC, 2008: 44). Card skimming devices include handheld skimming devices as well as ATM skimming devices. However, the focus here is on ATM skimming.36

During a crime of ATM skimming, the skimming device is placed on the ATM in such a way that disguises its presence but allows it to capture the information on the magnetic strip of the card and the input of the customer’s PIN (Enisa, 2009: 14). The customer inserts their card into the ATM that has been modified with a skimming device, performs a normal transaction, and retains the card. The customer leaves the ATM unaware that their card has been compromised. The captured information is used to produce counterfeit cards for subsequent fraudulent cash withdrawals (Enisa, 2009: 14). The customer will only become aware of the fact when unauthorised cash withdrawals/transactions are made from their bank account. Because the skimming devices are very sophisticated, and often difficult to detect, multiple cards are regularly compromised (Enisa, 2009: 14).

36 See Minnaar, 2008 for more detail on cybercrime practices regarding card skimming.
Several different methods are used by criminals to do this, and the PIN is obtained either by the usage of a small spy camera, or by a PIN pad overlay (false PIN pad). Increasingly blue tooth wireless technology is used to transmit card and PIN details to a laptop at a remote location. This information can then easily be sent anywhere in the world to allow the fast production of counterfeit cards (Enisa, 2009: 14).

Criminals can create a magnetic strip reader that fits directly and neatly over the magnetic strip reader on the ATM, and the person making a withdrawal is often none the wiser. This skimming device, when placed on the ATM machine is virtually undetectable (Enisa, 2009: 14). It looks like a normal part of the ATM.

**Image 3.4 & 3.5: Skimming devices**

Fake ATM machines

Criminals have been known to place fake ATM machines in and around shopping centres and other public locations in the United Kingdom. These look like real ATM machines, and some have even been known to dispense cash. All cards used at these machines are copied, and the PIN information is obtained from the PIN pad. As these machines are not connected to a network, the criminals can place them anywhere there is a power source (Enisa, 2009: 15).
3.2.6 Threat of vandalism

The threat of vandalism referred to by Winters (1986: 12) is not clearly explained in terms of the type of activity regarded as vandalism. However, these days vandalisms are seen as deliberate attempts to damage an ATM machine and/or card reader slot which is jammed preventing the customer’s card from being inserted (ATM Solutions, nd). Vandalism may also occur when an ATM bombing attempt is foiled. For example, as will be described in greater detail in Chapter 5, when a perpetrator attempts to bomb an ATM using explosives, he will use some type of tool to make apertures through parts of the ATM in order to insert the explosives. Where the perpetrator is disturbed and flees before completing his crime, and all that he has managed to do is make incisions in the structure, this too can be considered vandalism.37

3.3 METHODS OF PROTECTION

Now that what needs to be protected and what the threats are, have been identified, and that the vulnerability to risk has been assessed, measures that can be implemented in order to protect the assets need to be addressed.

A discussion on how banking institutions can utilise security measures to protect their assets will follow.

3.3.1 Human element

The human element of security includes guards, who may be armed or unarmed. They may be accompanied by dogs or have metal detectors. The level of security is related to the threat assessment. The higher the probability and impact, the higher the level of security needed.

37 ATM vandalism has also been noted in terms of as a protest whether political, social or economic against economic exploitation, i.e. as a target or symbol of capitalism or resentment at banking control over money or even for their perceived manipulation of financial markets (as alleged in the recent economic crisis (sub-prime fiasco) in the USA).
3.3.1.1 Guarding aids

i. Firearms
Armed guards are not generally used at branches of banks, since banking institutions aim to protect their clients and staff first and foremost. Armed guards could trigger a gun fight with armed bank robbers and customers and employees could be injured or killed. They could be caught in the cross fire if there happened to be an armed robbery at a bank branch or in its near vicinity. If this were to happen it could be seen as a reputational risk for banking institutions. You will, however, find armed C-I-T security officials at banks.

ii. Dogs
Once again whether or not a guard has a dog will depend on the probability of an incident (robbery) occurring. It may also be in accordance to the risk assessment of such any specific site.

iii. Metal detectors
Metal detectors use an electromagnetic field and register any changes due to the movement of metal in the field. Therefore if a guard has a metal detector and runs it over your person before you enter the bank, he will be able to tell if you are armed and you will then not be allowed to enter the bank.

3.3.2 Armed reaction
Banking institutions make use of armed reaction security companies who will respond to a panic alarm in the case of an armed robbery or to any disturbance after hours. In the case of burglary after hours, they will pick up a signal via the banks alarm system.

3.3.3 Staff (procedures)
In a banking institution, staff members may be trained in certain security procedures. For example, they should comply with the perpetrators demands in the case of an armed robbery, and press the panic button if possible. They will also be trained to follow certain lock-up procedures and evacuation procedures.
3.3.4 A central command centre
In the banking industry there exists a central command centre that a number of different banks use. This is where all signals regarding disturbances are sent.

3.3.5 Physical security equipment
There are several types of physical security equipment that can be used by banks to support the security measures above:

3.3.5.1 CCTV surveillance
Closed-circuit television is one of the most advanced and widely used security technologies available today. In banking institutions the use of CCTV surveillance cameras are widespread and usually in conjunction with other security technologies. This is referred to as system integration. It is believed that they do not deter armed robbers because they simply do not believe that they will be apprehended. We can assume that surveillance videos can assist in the identification of the perpetrators and the building up of an image database of perpetrators for future use in court and linking to multiple bank robberies.

3.3.5.2 Alarm systems
All banks use alarm systems and although they are effective in providing protection against after-hours burglaries, they do not reduce the incidence of armed robbery during banking hours, since they are not activated during banking hours (Barnes, 2008: 4). What is of particular significance in an alarm system as a protection method are such alarm features as fixed buttons and mobile panic buttons accessible to counter staff or in a supervisor’s or manager’s office.

Robbers are not generally deterred by such alarms because they expect the crime to proceed quickly and they would be able to escape before the alarm is activated or before the response team arrives at the scene (Barnes, 2008: 4).

3.3.5.3 Time delay locks or doors
Time delay means that the lock will not open for a specified time period following the entry of the correct access code. The delay in the door being opened will delay the robbery in process.
This raises the risk for robbers by forcing them to still be on the premises waiting for safes to be opened and thereby exposing them to possible apprehension by responding persons, police, private security or both.

3.3.5.4 Safes
Safes used at banks work according to a classification system. Depending on what needs to be protected, the safe classification will be more intricate.

3.3.5.5 Turnstiles
This is a form of a gate that will allow only one person to pass at a time and can also be used to enforce one-way traffic and to allow access to authorised people only.

3.3.5.6 Interlocking doors
Interlocking doors are usually installed at the entrance to a branch of a bank in the form of an entrance cubicle, two doors on either side. The first door can only be opened when the second door is closed and a person can only exit the cubicle once the first door is closed completely behind them. This will also allow entry of only one person at a time into a bank. Such cubicle entrance can also be remotely ‘locked’ and thereby ‘trapping’ a person in the cubicle. The glass sides and doors of these bank entrance cubicles are also made from bullet proof glass.

3.3.5.7 Bulletproof glass
This is widely utilised at bank branches, usually at teller sites in order to protect the tellers behind which tellers can work and still communicate; do business and dispense money to customers.

3.3.5.8 Vehicle interlocking systems
Used on C-I-T vehicles, the vehicle interlocking system controls the operation of the exterior and safe doors (OTT, Nd). As such, the vault cannot be opened if the side exterior door is open (OTT, Nd).
3.3.6 Policies and procedures

Every institution has its own security policies and procedures or operating guidelines. These procedures generally form part of a comprehensive security plan, which security officials need to implement, manage and monitor while also seeing to it that employees adhere to them.

3.4 CONCLUSION

This chapter provided a discussion on the various types of crime risks that the banking industry is faced with, specifically with regard to ATMs. In addition it looked at the use of various methods that are used by banking institutions in order to protect their assets from certain crime risks. It is important results that custodians utilise security measures that are specific to the crime risk and based on individual risk profiles.

It is evident that aside from the bombing of ATMs, ATM sites are vulnerable to numerous other crime risks in the many forms discussed above. As such, ATMs need to be protected against any possible ‘attack’ in a way that addresses the ATMs specific needs in accordance with its crime risk profile. In the chapters that follow, numerous issues regarding security measures at the physical ATM site which emanate from ATM site audits will be discussed. While these issues are focused specifically on the bombing of ATMs, some of them constitute security weaknesses to most of the ATM crime risks as discussed above. The need to improved security measures at ATM sites cannot be overemphasised.
Chapter 4
ATM SITE AUDIT AND AN ANALYSIS BASED ON LOCATION OF ATM BOMBING

4.1 INTRODUCTION

It is essential, in order to make an informed decision regarding the enhancement of security measures, that the responsible individuals follow a systematic process in order to determine the security concerns and steps that should be taken in order to tackle the problem. This can be achieved by following and applying the security risk management process. The security risk management process begins with a preliminary meeting with the client (Rogers and Schoeman, 2009). The client, the in-house security manager or external security consultant may initiate this meeting (Rogers and Schoeman, 2009: 54). Regrettably, most of the time, this meeting is frequently initiated only after having experienced a critical financial crime-related loss, for example through an upsurge in ATM bombings (Rogers and Schoeman, 2009: 54).

4.2 ATM SITE AUDIT

In line with the UNISA developed Security Risk Management Model a site audit of ATMs was applied in order to analyse a number of criteria regarding security at ATMs.38

This chapter provides an analysis of information gathered during site audits of various ATMs in Gauteng. The ATM sites chosen include ATMs that were previously involved in ATM attacks and subsequently repaired or replaced. As discussed in Chapter 2, the sample included ATMs of the four major South African banks; i.e. ABSA, Standard Bank, First National Bank and Nedbank. It included the following different types of ATM sites:

38 See Table 4.1 below
Stand-alone ATMs

These include container type ATMs that are not attached to a fixed structure such as a building as well ATMs that are stand-alone but are housed in a modest building designed specifically for that structure.

Image 4.1: Stand-alone portable type ATM

ATMs at a petrol station

Such ATMs are those located at petrol stations and may be housed inside the convenience store at the petrol station or it may be a stand-alone type ATM. This will be located on the property of the petrol station, i.e. outside the convenience store at the petrol station. These also include 24-hour petrol stations and petrol stations that are not open on a 24-hour basis but usually open till late at night.

Built-in type ATMs

These types of ATMs are those that are built into a wall. Such built-in type ATMs may be found at just about any location. Examples of places where these ATMs are found most often are inside

---

39 To avoid repetition of stand-alone ATM types, only ATMs inside the convenience store were used in the sample. However, the dangers of an ATM attack at an ATM situated outside at a petrol station are also discussed in the following analysis.
shopping malls, attached to banks where the bank is located on the street in a central business
district or in a mall and small shopping centres.

Image 4.2: Built-in type ATM

Image 4.3: Built-in type ATM inside shopping mall, attached to bank
**In-store ATMs**

Whilst ATMs located inside a convenience store at a petrol station may also be regarded as an in-store ATM, the risks in a case of an ATM bombing at an in-store ATM at a petrol station and at any other type of store differ dramatically. For the purposes of this research, in-store ATMs are defined as those located inside stores such as your round-the-corner small supermarket.

**Image 4.4: In-store type ATM**

Each of the abovementioned types of ATMs were selected according to the four different bank brands and risk categorisation. The selection included ATM sites that may be categorised as low, medium and high risk sites. For example a stand-alone ABSA ATM in a suburb e.g. Constantia Kloof, as well as a stand-alone ABSA ATM in a township, for example Soweto, were both included in the site audit. As such the site audit sample included five low risk; five medium risk; and five high risk sites and the bank brands of each ATM (although inclusive of all four major banks) were random.

In addition to an analysis of the site audits, in this chapter we will first look at some limitations relating to the information gathered during site audits. There is a brief discussion on the Security Risk Management Model, from which the rationalisation of performing site audits has emanated,
and it will also provide an analysis of ATM attacks based on location, in accordance with the incident report provided by SABRIC, SAPS dockets and media reports.

4.3 LIMITATIONS EMANATING FROM SITE AUDITS

Whilst conducting site audits the researcher was limited to the knowledge of physical security measures, as well as to only what can be observed at an ATM site. It is the belief of the researcher that a site audit should have been conducted with the assistance of professionals who have extensive knowledge of the security measures in place at ATMs. Technicians and installers who have knowledge of possible electronic security measures and devices inside ATM housing should be consulted. This, however, was not possible due to the banking industry’s reluctance to provide detailed information pertaining to such security measures. For obvious reasons, such as those discussed in Chapter 3, it is not in the best interest of the banking industry as a whole to make such information accessible to the public. This was pointed out by SABRIC, as well as ATM Solutions who made it clear that information pertaining to ATM security design and security measures could not be provided. Spokespeople of banks also refused to provide such information. For example in an article published in the Pretoria News in 2007 when ATM attacks were on a dramatic upward spiral with almost constant week-ok-week increases, a Standard Bank spokesperson indicated that the bank had taken steps to secure ATMs identified as high risk but he declined to elaborate on these security measures, let alone the nature and extent of them (Hosken, 2007a: 2).

Information regarding the strength or resistance of the different safes used in ATMs to withstand the power of explosives, would have been enormously valuable to this research. Other information, such as that of which of the ATM sites audited were installed with alarms and whether any of the ATMs contained such security measure as dye-bombs would have also added value. Whether any other security devices were installed inside the ATM (that which is not visible from the outside), would have rendered the research findings more comprehensive. As will be seen in the analysis discussed in this chapter, these limitations impacted to a certain extent on the findings derived from the available information gathered during the site audits.

---

40 Such devices are expected to stain money when tampered with, rendering the cash unusable.
It is worth noting that the analysis of case dockets, both from SAPS and ATM Solutions as well as media report information, provided no information relating to ATM security measures with the exception of a few statements found in the SAPS dockets that made mention of an ‘ATM alarm’ that went off during an attack. In only two newspaper articles, an ABSA spokesman mentioned that:

1. That safes in ABSA ATMs ‘could not be penetrated’; and (SAPA, 2007a)

2. ABSA ATMs contained dye bombs\(^\text{41}\) that stained the money rendering them unusable (Molosankwe and Eliseev, 2007; Eliseev, 2007: 2)

This was perhaps a tactic to deter perpetrators as more bombings of ABSA ATMs occurred after these statements were made. As will be discussed below, ABSA ATMs were one of the most targeted bank brands.

4.4 THE SECURITY RISK MANAGEMENT MODEL

It is mandatory in order to make a comprehensive decision on how to overcome a specific crime problem, that one follows a security risk management process when collecting and analysing risk information.

The diagram (Figure 4.1) below indicates the various components that make up the Security Risk Management Model,\(^\text{42}\) which graphically illustrates the security risk management process. According to Rogers (2008: 151), “the various components of the model/approach are linked to each other and overlap”. He further explains that its implementation takes on a cyclical approach and that the various components do not exist separately in “watertight compartments” (Rogers, 2008: 151-152). He elaborates as follows, “the components cannot be viewed in isolation, but

\(^{41}\) These are placed in the money cassettes in ATMs and go off if the machine is bombed, tampered with or the cash is forcibly removed

\(^{42}\) As developed by lecturers at UNISA – see Footnote 10 above.
should be approached as comprising of sub-components of an integrated whole” (Rogers, 2008: 152), as they are linked and inter-dependent upon each other.

Figure 4.1: Security Risk Management Model/process

![Security Risk Management Model/process diagram](image_url)

1. The problem of security (crime) risks
2. The security policy and mandate
3. The orientation phase
4. The risk analysis exercise
5. The comprehensive security survey
6. Return-on investment
7. Security risk control measures
8. The crime risk management report
9. Implementation, evaluation and maintenance of security measures

(Rogers, 2005; Adapted by Olckers, 2007, cited in Rogers, 2008: 152)

A change in any one of the components that make up the Security Risk Management Model will have an influence on the other components (Rogers and Schoeman, 2009: 45). For example, “if the risk of ATM bombings increases, this directly influences the security measures, which have to be improved in order to manage this specific risk. The security measures will cost money, so policy changes on the part of banks may result” (Rogers and Schoeman, 2009: 45). Rogers (2008: 152) illustrates eleven premises on which the Security Risk Management Model is based. However, the third premise mentioned is of relevance here as it explains the researcher’s rationale for carrying out ATM site audits and its relevance to this study. Accordingly, the third premise states the following:
“As a point of departure an orientation visit to the client’s site is undertaken to gather preliminary information on both crime risks and security weaknesses (implementation of a dedicated preliminary security survey). Specific research needs with regard to the next two phases are also established during this phase” (Rogers, 2008: 152).

This premise is an extension of the third step in the Security Risk Management Model, namely the orientation phase or “on-site orientation”. On-site orientation necessitates a physical site visit, in this study the ATM site audit “during which vulnerable assets, security risks and security weaknesses are identified” (Rogers and Schoeman, 2009: 55). In practice, the orientation phase concludes with the planning for the risk analysis and comprehensive security survey exercises (Rogers and Schoeman, 2009: 54). The findings from the site audits will be used to compile a security survey checklist\(^{43}\) in order to assist bank security consultants and managers in compiling a survey sheet for auditing ATM security. This will contribute to a comprehensive security survey exercise, as discussed in premise 4 and 5 as well as the Security Risk Management Model above (Rogers, 2008: 152).

### 4.5 ANALYSIS OF INCIDENT REPORT PER LOCATION

It has already been pointed out that the highest number of ATM attacks with the use of explosives occurred during 2007 and 2008 and this number decreased by early 2009. However, ATM bombings have not stopped altogether, nor have they decreased to numbers that date back to 2006.\(^{44}\) Gauteng as a region has by far been the hardest hit. During this research, it was discovered that while ATM bombings are the work of organised crime syndicates, a number of different syndicates exist which operate not just in different areas of Gauteng, but also in different provinces. An Interviewee of SAPS SOCS stated during an interview that syndicates operating in Gauteng will, for example, also drive down to KwaZulu-Natal (KZN) to commit the same type of crime (SAPS 2: 2010). This was also ascertained from the analysis of media reports pertaining to arrests, convictions and killings of ATM bombers.

---

\(^{43}\) See Chapter 6

\(^{44}\) See Chapter 1 for figures
For example, convicted offender Lebohang Nicholas Ranyali, who media reports stated came from Welkom, was linked to at least six bombings in the Durban area and many more in Johannesburg. He was arrested on the N3 highway near Pietermaritzburg while allegedly trying to flee to Durban after bombing (the day previous to his arrest) two ATMs, one of which was in Vereeniging and one in Soweto (Maravanyika, 2007: 2 & 4; Kirk, 2007: 4).

Another incident in which the accused Fukani Zwane of Kwa-Mashu in KwaZulu-Natal was shot and killed after opening fire on police in an attempt to flee during attempts to arrest him, Snr Supt Jay Naicker (SAPS Spokesman) told the media that investigations led them to believe that “he worked with guys from Gauteng, and further explained that they [perpetrators from Gauteng] would come to him for help when they wanted to move into the province” (Le Grange, 2008: 6).

These are only a few examples of cases where investigations led police to discover that the syndicates did not confine their attacks to a single province. Information contained in media reports relating to ATM bombers link to other provinces and all areas in Gauteng were confirmed by interviews with members of the SAPS SOCS unit.

Below is an analysis, drawn from Annexure A, of which areas in Gauteng are most affected by ATM bombings. According to the SABRIC incident report for January 2006-July 2009, ATM bombings were reported at 100 of the 127 police stations in Gauteng during the abovementioned period. The table includes only these 100 police stations.

The province was then divided into the policing areas of East Rand, West Rand, Greater Johannesburg (including Johannesburg North and South and Soweto), Pretoria and Vaal Rand (Southern Gauteng). Each of the reported incidents were put into the relevant policing areas and analysed accordingly.

---

45 Annexure C indicates the number of reported incidents per police station in Gauteng. These were further organised in descending order, beginning with the areas that had the most number of ATM bombings reported between January 2006 and July 2009. This information is based on SABRIC’s incident report on ATM bombings for the said period.
According to the table in Annexure A, the highest number of ATM bombing incidents, eighteen, was reported at the Atteridgeville Police Station (Pretoria); followed closely by Springs (17) (East Rand), Tembisa (16) (East Rand), Soshanguve (15) (Pretoria) and Kagiso (15) (West Rand) for the given period. The police stations which were identified in the above table were categorised into the above-mentioned areas. The total number of incidents reported was 527. Using a simple calculation, the percentage of incidents per area was calculated. Figure 4.2 below indicates the percentage of incidents reported per area for the aforesaid period in accordance SABRIC’s incident report.

**Figure 4.2: Percentage of ATM bombing incidents per policing area in Gauteng (SABRIC)**

The two areas with the highest number of ATM bombing occurrences include the East Rand, 28% of all incidents and Greater Johannesburg, 26%. Following closely is Pretoria with 21% of incidents occurring here. While an analysis of SABRIC’s incident report gives a clear indication of the areas most affected, interviews with commanding officers of SAPS SOCS gave the same

---

46 See Annexure E for map indicating division of areas.
results. Although they could not give exact numbers, both indicated that most bombings occurred in Johannesburg, Pretoria and the East Rand.

In addition, the analysis of SAPS dockets indicated similar findings. The Figure (4.2) below illustrates the areas where most ATM bombings occurred in accordance with the docket analysis. These results can be said to represent the true situation as dockets were not purposefully selected to represent all areas in Gauteng.47

**Figure 4.3: Percentage of ATM bombing incidents per policing area in Gauteng (SAPS)**

![Pie chart showing percentage of incidents per area](image)

(According to SAPS case dockets)

The East Rand was the most affected with a total of 34 (= 34% as 100 dockets were used in sample) incidents during the abovementioned period. Second is Johannesburg with a total of 29% of incidents during the aforesaid period.

---

47 See Chapter 2
This simple observation of the incident report and dockets was confirmed by members of SAPS who were interviewed. Both SAPS SOCS commanding officers stated during interviews that Pretoria, East Rand and Johannesburg were most affected.

When comparing the analysis of SABRIC’s incident report and the dockets, however, one will notice (as indicated in Figure 4.3 below) that there is a minor discrepancy.

**Figure 4.4: Comparison between SABRIC and SAPS percentages of ATM bombing incidents per policing area in Gauteng**

The analysis of SAPS dockets illustrates a greater number of bombings having occurred on the West Rand than in the Pretoria area; while SABRIC’s report indicated that more bombings
occurred in Pretoria than the West Rand. SABRIC’s incident report constitutes a more reliable source as it essentially is a list of ALL incidents for the aforementioned period. It can therefore be correctly assumed that the reason for the discrepancy is merely that dockets that were still available at the SAPS SOCS, consisted of more dockets from the West Rand than Pretoria.48

4.5.1 Towns/suburbs most affected
For each of the above areas the towns or suburbs that were most affected were identified. Tables 4.1 to 4.5 below demonstrate the towns most affected in each area.

a) East Rand
Table 4.1: Towns/suburbs most affected on the East Rand

<table>
<thead>
<tr>
<th>Town/Suburb</th>
<th>Number of incidents between January 2006 and July 2009</th>
</tr>
</thead>
<tbody>
<tr>
<td>Springs</td>
<td>17</td>
</tr>
<tr>
<td>Tembisa</td>
<td>16</td>
</tr>
<tr>
<td>Katlehong</td>
<td>13</td>
</tr>
<tr>
<td>Brakpan</td>
<td>12</td>
</tr>
</tbody>
</table>

The above four towns (Springs, Tembisa, Katlehong and Brakpan) on the East Rand of Gauteng were most affected by ATM bombnings. The other towns or suburbs identified from the incident report had between one and seven reported ATM bombnings, with six towns or suburbs having recorded a number of incidents that are between five (5) and seven (7) (i.e. greater that (>5 and less than (<7).

48 According to investigators, dockets that have been filed undetected and no leads to the investigation are found, the docket is returned to the station after a period of time.
b) Greater Johannesburg

Table 4.2: Towns/suburbs most affected in the Greater Johannesburg

<table>
<thead>
<tr>
<th>Town/City</th>
<th>Number of incidents between January 2006 and July 2009</th>
</tr>
</thead>
<tbody>
<tr>
<td>Soweto, Mondeor</td>
<td>13</td>
</tr>
<tr>
<td>Soweto, Moroka</td>
<td>13</td>
</tr>
<tr>
<td>Eldorado Park, Johannesburg S</td>
<td>12</td>
</tr>
<tr>
<td>Soweto, Dobsonville</td>
<td>11</td>
</tr>
<tr>
<td>Soweto, Jabulani</td>
<td>10</td>
</tr>
</tbody>
</table>

In the Greater Johannesburg Metropolitan area, Soweto had the highest number of ATM bombings, 47 in total. The only other town or suburb in the Greater Johannesburg area with a number of reported incidents above ten was Eldorado Park. All the other towns/suburbs experienced between one and eight ATM bombing incidents, with three places having experienced between six and eight incidents.

c) Pretoria

Table 4.3: Towns/suburbs most affected in the Greater Pretoria region

<table>
<thead>
<tr>
<th>Town/Suburb</th>
<th>Number of incidents between January 2006 and July 2009</th>
</tr>
</thead>
<tbody>
<tr>
<td>Atteridgeville</td>
<td>18</td>
</tr>
<tr>
<td>Soshanguve</td>
<td>15</td>
</tr>
<tr>
<td>Temba</td>
<td>9</td>
</tr>
</tbody>
</table>

In Atteridgeville the highest number of ATM bombings were recorded during the said period, for the whole of Gauteng. Although, it is only one more than the second highest number of incidents recorded. Other places in Pretoria, suffered between 1 and 8 incidents and 5 places recorded a number of incidents that were between 5 and 9 (>5 and <9).
d) Vaal Rand (Southern Gauteng)

Table 4.4: Towns/suburbs most affected in Vaal Rand

<table>
<thead>
<tr>
<th>Town/Suburb</th>
<th>Number of incidents between January 2006 and July 2009</th>
</tr>
</thead>
<tbody>
<tr>
<td>Orange Farms</td>
<td>8</td>
</tr>
<tr>
<td>Ennerdale</td>
<td>6</td>
</tr>
</tbody>
</table>

As seen in table 4.4, the number of incidents reported in the Vaal Rand was generally low. Other Vaal towns encountered between one and five incidents only.

e) West Rand

Table 4.5: Towns/suburbs most affected in the West Rand

<table>
<thead>
<tr>
<th>Town/Suburb</th>
<th>Number of incidents between January 2006 and July 2009</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kagiso</td>
<td>15</td>
</tr>
<tr>
<td>Roodepoort</td>
<td>12</td>
</tr>
<tr>
<td>Randfontein</td>
<td>10</td>
</tr>
</tbody>
</table>

In table 4.5 are the areas on the West Rand that were most affected by ATM bombings. Of the remaining towns, four had reported incidents between five and ten (>5 and <10) with 9 incidents having occurred in Krugersdorp.

4.5.2 Type of areas most affected

In each of the above high risk areas i.e. towns or suburbs, certain specific types of locations are more at risk than others. Initially, ATM bombings took place outside the towns in less populated areas, such as rural areas (Geldenhuys: 2009: 39). However, as incidents of ATM bombings increased, perpetrators moved into towns, into areas that are more populated and even those which are more affluent. (Geldenhuys: 2009: 39).
As the number of ATM bombings increased, the number of attacks that took place in areas where they did not previously take place increased. Shopping centres in suburbs too became regular targets of ATM bombings. In accordance with the SAPS docket analysis: 43% of ATM bombing incidents took place at ATMs next to shops, mostly supermarkets, at the corner of streets and in central business districts (CBDs): 27% took place at petrol stations and the remaining 30% took place at shopping centres and complex’s in townships, towns and suburbs. Due to the fact that the exact location of an ATM bombing is not always stipulated in media reports, it was difficult to ascertain where most bombings occurred from media reports.

4.6 ATM SITE AUDIT

4.6.1 The importance of ATM site security and security risk control measures

The increasing utilisation and awareness of ATM sites throughout the country and the world is of equal benefit to customers and service providers (banks) but also rather risky (Winters, 1986: 11). As withdrawal limits have increased and as credit access has become more widespread, a consequent increase in incidents of ATM crime has occurred. Generally the public face further potential increases in crime incidents with the increase in the deployment of ATMs throughout the country and especially in previously unserviced areas.49 The banking industry has not only introduced ATMs for their clients’ convenience but also for its cost effectiveness and cost benefits (Winters, 1986: 11). When customers become cautious of, or believe they are unsafe at ATMs sites, the banking industry experiences difficulty in guiding them to increased levels of usage (Winters, 1986: 11). Aside from ensuring the safety of customers at ATMs, there is also the need to ensure the safety of people who install and service the equipment, as well as those that replenish cash contents. They could be bank or financial institution employees or third party contractors, including C-I-T companies (Winters, 1986: 12). Therefore, the need and the importance of securing ATMs goes beyond the mere protection of assets (i.e. cash). Appropriate and meticulous ATM site audits through comprehensive risk analysis and security survey can play a valuable role in the enhancement of security at ATMs by examining remote sites. As we as those in high crime areas or those considered as high risk ATMs, and ascertaining that certain

49 An ‘unserviced’ or ‘unbanked area’ refers to an area where there is an absence of banking and financial services in terms of branches and infrastructure like ATMs.
sufficient measures are taken to protect the institutions assets. According to Winters (1986: 13) these assets include:

- The customer/client;
- The institution’s employees;
- The institution’s cash;
- The institution’s equipment; and
- The institution’s image.

In order to ensure effective protection of such assets, it is essential that appropriate security risk control (SRC) measures are implemented and regularly evaluated. In order to make an informed decision regarding the most cost-effective means of protecting assets, a thorough security survey must be completes (as per the Security Risk Management Model).

According to Rogers & Schoeman (2009: 76), the following events or activities must have taken place before SRC measures can be identified:

- The organisation (in this case the banking industry) concerned must have encountered a crime risk problem (ATM bombings) that warrants investing money in security risk control measures.

- Top management must have supplied the security department with a mandate (permission) to manage crime risks.

- The specific site (physical ATM sites, perhaps mostly high risk sites and high risk areas for the specific problem as identified above) where the crime problem is must have been visited and certain functions performed (on-site orientation).

- Specific crime risks endangering specific assets must have been identified and measured (risk analysis). It is these crime risks that require security risk control measures.
Weaknesses in the current security system must also have been identified. It is these weaknesses that must be rectified (security survey)

Only after the above events and activities have taken place can effective risk control measures be identified.

While this research aims only to provide a suitable recommendation with regard to security survey, it is necessary to note the importance and objectives of adequate SRC measures. While the primary objective of implementing improved security is to address a security problem, the following detailed list of objectives has been identified Rogers & Schoeman (2009: 98-105):

- **Deterrence of criminal conduct**: essentially, the primary aim of a security measure is to manipulate an offenders’ behaviour. It should satisfy a potential criminal that the probability of remaining undetected and unpunished is small. This would deter the person from committing the crime.

- **Deflection**: “Deflection occurs when a criminal attempts to commit a crime but fails due to the existence of security measures. This means that the security system has successfully prevented the crime (risk) from being committed and financial loss to the organisation from being suffered” (Rogers & Schoeman, 2009: 100)

- **Detection**: The total security system must be designed in a way that crimes are identified as soon as an attempt is made to commit a crime. Technological aids such as real-time surveillance and the use of alarms assist in achieving this objective.

- **Delay**: Once criminals or intruders have been detected, security measures in place will cause them to be delayed in their pursuit to reach the asset concerned. This delay is achieved by “placing various physical and/or procedural barriers between the criminal and the asset being protected” (Rogers & Schoeman, 2009: 102). Barriers used to achieve this objective may take the form of walls, fences, burglar bars, doors, safes, security officials etc.
• **Reaction:** Once criminal conduct has been detected, a security/other law enforcement official must react. The security system in place draws the attention of the security official on duty or control room operators the moment an attempt is made to commit a crime (the person reacting will be based on the system in place).

• **Detention:** “Where the security policy provides for it, criminals should be detained (arrested). All legal requirements and company policies must always be complied with” (Rogers and Schoeman, 2009: 104).

• **Rectifying identified security weaknesses:** “The evaluation of crime risk control measures and the rectification of any weaknesses in the security system are an important objective of the crime risk control process. The evaluation of the security system must take place on a regular basis and not only after a loss has been experienced” (Rogers and Schoeman, 2009: 105).

• **Recovering losses:** When a person has been identified as responsible for financial losses caused by criminal conduct, the security measures will have to provide for the recovery, where possible, of the damage suffered.

Security risk control measures must contribute to the achieving of security objectives. These objectives are ultimately aimed at the effective short-term prevention of financial losses caused by criminal conduct (Rogers and Schoeman, 2009: 105).

### 4.6.2 The on-site orientation phase

The on-site orientation is a laconic preliminary exploratory investigation on site to identify vulnerable assets, security risks confronting the organisation, and the state of security measures at the premises (Rogers and Schoeman, 2009: 56). The objective of the on-site orientation is to determine whether a security survey is desirable and is technically and economically feasible (Broeder, 1984:49), and to quickly identify vulnerable assets, security risks and security weaknesses (Rogers and Schoeman, 2009: 56).
According to Rogers and Schoeman (2009: 62), the following must be addressed as part of an on-site orientation:

- core business processes that may be vulnerable to security risk;
- assets that may be vulnerable to security (crime) risks;
- security risks that may endanger assets; and
- security weaknesses and excessive security measures.

The activities conducted as part of the orientation security have a direct impact on the accuracy of the risk analysis exercise and comprehensive security survey.

During the physical inspection of the site, one needs to pay attention to the immediate environment by walking around the premises and inspecting the perimeter fence, alarms, CCTV cameras, security control rooms, locks and burglar guards. Nearby features such as types of neighbouring premises, public areas (public roads), public transport systems (railway lines and bus or taxi ranks), open spaces (veld in the vicinity of the premises) and residential areas should also be noted (Rogers and Schoeman, 2009: 62).

In addition to making notes on observations during ATM site audits, as part of on-site orientation, the researcher compiled a survey sheet to assist with the process.

Table 4.1 below is the ATM site audit checklist that was utilised by the researcher during the ATM site audit.
Table 4.6: ATM site audit survey checklist

<table>
<thead>
<tr>
<th>CONTROL ISSUE</th>
<th>Y/N</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>A. ATM TYPE</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Stand-alone/portable type</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. In-store ATM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Built-in type</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>B. LOCATION</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Petrol station</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Shopping centre</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Bank</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Shopping mall (inside)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Corner of street</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Other</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>C. OPERATIONAL HOURS</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. 24 hours</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Limited hours</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>D. LIGHTING</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Sufficient lighting</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Insufficient lighting</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>E. CCTV CAMERAS</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Y (If Y, are they operational)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. N</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>F. SECURITY GUARD</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Y/N</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. If Y, does he have a panic button?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. If Y(to 1), is he armed</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>4. ATM ALARM</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Y/N</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
2. Silent/sounded

5. PHYSICAL BARRIERS
   1. Is property where ATM situated fenced (if applicable)
   2. Is ATM protected by steel/roller doors? (if not 24hr)

6. CUSTOMER AWARENESS INFO
   1. Clearly visible (Y/N)

7. INTERCOM (Y/N)

8. ALARM/PANIC BUTTON (Y/N)

9. FOR IN-STORE ATMs
   1. Smoke alarm/detector (Y/N)
   2. Alarm system (Y/N)

10. OTHER SECURITY DEVICES AVAILABLE (If Y – what are they)

4.6.3 Findings from ATM site audits
With special permission not being granted by the banks to do so, the findings of the ATM audits, will not include the bank brand of the ATM sites that were observed as well as the exact location of the ATM. As discussed previously\textsuperscript{50} detailed information regarding ATM design and security measures are often not made available publically.

During site audits, it became more and more apparent to the researcher, that despite the low, medium and high risk profiles of the ATM, most ATMs have similar measures of security or lack thereof.

\textsuperscript{50} See chapter 2
4.6.3.1 Lighting

Of the 15 ATM sites, nine ATMs were situated outdoors and six (6) in-doors. The six in-door ATMs include in-store ATMs, ATMs inside a petrol station convenience store and one in a casino. Of the nine outdoor ATMs, only four ATM sites had sufficient lighting and the remainder displayed insufficient lighting.

Insufficient lighting at an ATM site will make it difficult for police/security guards to see anyone at the ATM clearly.

4.6.3.2 CCTV surveillance

Most ATMs do not have CCTV surveillance cameras. All ATM sites that were categorised as high risk did not have CCTV cameras. In some cases the researcher was unable to establish whether cameras that did exist were operational.51

Additionally, in only a handful of the dockets analysed was there CCTV footage available as evidence. A majority of the cases did not have CCTV footage due to cameras not being operational (for various reasons, out-of-service or control room operations not being 24/7 recording etc.) or, as in most cases, the site not having CCTV cameras installed. Mostly ATMs at petrol stations had CCTV cameras and from the site audits, only ATMs at petrol stations and the one in a casino had CCTV cameras at the ATM.

4.6.3.3 Customer awareness

Most ATM sites did not have customer awareness information displayed at the machine. The only ATMs with clear customer awareness information were those inside malls and those attached to a bank. Customer awareness information is important so that customers are fully aware of the possible risks that they face while using an ATM. In addition, it plays an important role in informing customers of the things that they need to be aware of and the manner in which they need to conduct themselves when using an ATM facility.

51 In research regarding security measures at petrol stations by Kole (2010) it was found in numerous cases that CCTV cameras on site protecting petrol stations (and by proxy ATMs also on site) were either not functioning, inadequate, not recording any incidents or were not monitored 24/7. In addition those that were in place a number suffered from the poor quality of the recorded images.
All of the four major South African bank brands have websites which provide tips on how customers can prevent becoming victims of crime as well as information regarding ATM crimes that they should be wary of. However, not all bank clients use internet facilities provided. Therefore, customer awareness information at an ATM sit is crucial so that customers can protect themselves.

### 4.6.3.4 Panic/Alarm Buttons

None of the ATMs audited had a panic/silent alarm button that could be used by customers who are in danger. Winters (1986: 22) includes this as control issue that needs to be addressed during site audits. Such a device, especially a silent alarm will not only give nervous customers a sense of security, but will also assist in possible detection of suspect. However, security guards stationed at ATM sites do have panic buttons. In addition, cashiers at petrol stations do have panic buttons at the counter, which can assist in alerting authorities if they are given a chance to use it.

### 4.6.3.5 ATM Alarm

The researcher was unable to establish which of the ATMs that were visited for the site audit had an ATM alarm (inside). However, from the analysis of case dockets it was established that some ATMs do have such alarms.

When asked about the ATM alarm during an interview, an interviewee of SAPS SOCS, indicated that it was not a silent alarm, but rather one which is heard (SAPS 2, 2010). It is, however, connected to a central control room where a signal is picked up when the alarm is sounded. It also gives the security guard, at a shopping centre for example, who is not in the vicinity of the ATM a chance to react if he/she has not been located by the perpetrators. However, it has been established that not all ATMs are fitted with such alarms. (In fact few and largely those that have been bombed and repaired are fitted with these additional security measures)
4.6.3.6 Additional security measures/devices
There was no evidence of additional security measures at any of the ATM sites visited. This makes the job of the ATM bomber very easy, as there are insufficient measures in place to detect criminal activity and delay access to cash, in order for authorities to react.

4.6.3.7 Presence of security guard
The presence of an armed security guard after hours also seemed to be an issue. While some ATM sites had security guards who were armed and had panic buttons others did not even have a guard. Shopping centres that did have armed security guards only patrolled the area around the ATMs at certain times. This makes it possible for perpetrators to plan accordingly, thereby only attacking once the security guard had completed his/her patrol. By the time the security guard hears the explosion and calls for help, the perpetrators would already have accessed the safe and made off with the cash. However, in almost all the cases where an armed security guard was present at the scene, he/she was subdued and robbed of his/her cell phone, panic button and firearm. Therefore, while the presence of an armed security guard is a good deterrent, their presence is in vain when perpetrators do attack and their lives are put at risk.

4.6.3.8 ATM intercom
Most ATMs also do not have an intercom, which should be available for customers who have been victims of a crime to speak to someone directly or to report suspicious activity while still at the site. Those that do are there to assist customers who experience problems while using an ATM.

4.6.3.9 Alarm systems (in-store ATMs)
All the stores at which ATMs were looked at had an alarm system. However, it was found that in all cases of in-store ATM bombings, the perpetrators were able to disarm the alarm system, therefore making them undetectable. Almost all the cases investigated internally at ATM Solutions involved in-store ATMs. They all reported that the alarm system was disarmed before

---

52 Some of the video footage indicated that the bombing and theft of cash out of an ATM occurred in under 60 seconds.
53 This finding occurred from the analysis of case dockets and not from ATM site audits.
54 Such a communication system can be installed similarly to what system has been installed for instance at parking cash machines. Such a system can also easily be linked to a shopping centre security control room.
the ATM was targeted. In cases where in-store ATMs were targeted, perpetrators would either enter the shop through the roof, but cutting a hole in it, at the exact place where the alarm box is located or by cutting the pad locks of the security gate and removing glass door for example. They would, therefore break in through the main entrance door and make their way towards the alarm and disarm it.\textsuperscript{55} It was suggested by interviewees that employees of the stores could be providing information to criminals regarding such things as alarm systems, lock-up procedures etc. (Interview, ATM Solutions 1).

\subsection*{4.6.3.10 Physical barriers}
For those ATMs that were on a property that was protected by a physical barrier (i.e. a fence), the fence did not appear to be an electric fence. It could not have been fitted with sensors that set off an alarm as those ATMs were bombed and in gaining access the perpetrators merely cut a hole through the fence and then subsequently made their getaway through the hole in the fence. Only two of the ATMs audited were protected by roller/steel doors after hours.

\subsection*{4.7 CONCLUSION}

While there have been no reasons cited as to why for example, the East Rand, Johannesburg and Pretoria are most affected by ATM bombings or why certain towns in these regions are more affected, it is important to note. High risk ATM sites in the areas most affected or those targeted on more than one occasion and can be used as a point of departure. For example, knowing which areas criminals prefer means that one can now deduce that an ATM in Springs (East Rand) that is placed at the corner of two streets outside a bank is a higher risk site than one in a similar location in say, Ennerdale (Vaal). Therefore, knowing which areas are more prone to ATM bombings can assist as a determinate factor regarding the risk profile of a particular ATM site.

Although findings with regard to the information gathered from the site audits are limited, it seems that ATMs in so-called “high risk” areas, such as those stand alone type ATMs in townships are poorly secured from the outset. ATMs that are medium and low risk also have

\textsuperscript{55} See chapter 5 also.
limited risk control measures. This means that such ATMs do not just face the risk of ATM bombings, but also other ATM crimes as outlined in Chapter 2.

Without any knowledge of whether or not any measures have been taken to curb ATM bombings, one must wonder whether in fact, ATMs in suburbs and supposedly medium and low risk areas are better secured than those in high risk areas.

The security of an ATM unit and the safety of both customers and service personnel are principal to any successful ATM program (Winters, 1986: 21). In addition, proper lighting, use of alarms, CCTV equipment, training programs for service personnel, security awareness for any guarding personnel posted at sites where ATMs are sited for example petrol stations and shopping malls, customer education and cooperation between the banking industry and law enforcement are basic to effective and successful ATM security practices.

The information that was gathered and the findings that were made will be used to draw up a survey sheet for a detailed security survey checklist (see Chapter 6). This will be of assistance to the banking industry in implementing the correct risk control measures at the right ATMs, as well as with the ongoing evaluation and improvement of security risk control measures.
Chapter 5

THE MODUS OPERANDI OF ATM BOMBING SYNDICATES

5.1 INTRODUCTION

*Modus operandi* is a Latin term which means behaviour, comportment or operational procedure (Horgan, 1979: 57 cited in Van der Westhuizen, 1995: 32). A more comprehensive description is that *modus operandi* are the habits and techniques of criminals which have become stereotyped and are the routine mode of conduct in which individualised techniques are employed (Van Heerdan, 1985: 10 cited in Van der Westhuizen, 1995: 32).

Although the primary rational for the study of the modus operandi of criminals lies in the possibility of revealing the identity of the perpetrator (Van der Westhuizen, 1995: 33), understanding how a criminal plans and carries out his criminal activity makes it possible for professionals to be able to plan protective measure accordingly. Therefore, if we can understand the manner in which ATM bombers execute their crimes, how they bypass certain security measures which make it possible for them obtain the cash contents of ATMs, then recommendations can be made to counteract such crimes.

Although the *modus operandi* of different ATM bombing gangs/syndicates is more or less the same, the actual type of target differs. What this means is basically that the chosen target of perpetrators of ATM bombings is ATMs, but, they might need to use different means to get to a specific chosen ATM due the fact that ATMs are located at different types of places. The following are some places where one can find an ATM:

- Inside a store: this type of ATM is inside a store that is not open 24 hours.

- At a petrol station: this type of ATM is situated at a petrol station, but may be located either inside a petrol station convenience store or outside at the petrol station.
• ATMs on a property that is protected by some type of physical barrier, for example fence or wall. The property may be that of a small shopping complex.
• ATMs inside a shopping mall.

Here we can also include ATMs that are protected by some means for example steel doors or roller doors or card accessed glass doors similar to cubicle entrances for banks). These ATMs are often not operational 24 hours and sealed off after hours or off-peak times due to the risk they carry.

As explained in Chapter 3, the perpetrators use the same modus operandi, but will adapt according to the target ATM site location. Therefore, perpetrators of ATM bombings will use the same methods of transport, the same weapons and tools, but will adapt it to the different type of target. For example, while they will merely walk up to an ATM on the corner of a street, place explosives in the machine and blow it up. For an in-store ATM they will have to break into the store first in order to get to the ATM.

The importance of the modus operandi of ATM bombers for this research is to understand how ATM bombers operate and use that information to make recommendations regarding the enhancement of security measures at ATMs. If we can understand how they go about bombing an ATM, then we can find ways to block them, thereby deterring such criminals.

According to Marais and Van Rooyen (1990: 68), modus operandi systems and reports should contain information regarding the characteristics of conduct in the planning stage of a crime, characteristics of conduct during commission of the crime and modus operandi after the commission of the offence.

In the remainder of the chapter, the modus operandi of ATM bombing syndicates will be explained in terms of the above. Unless otherwise stated the information contained in this chapter was drawn from a clustering and amalgamation of all the information drawn from the following sources: an analysis of the selected SAPS case dockets; case dockets from ATM
Solutions internal investigations; media reports; individual interviews and video footage. All the themes explained were drawn from these sources and clustered accordingly.

### 5.2 MODUS OPERANDI OF ATM BOMBING GANG/SYNDICATES

The SAPS confirmed that ATM bombings throughout the country are the work of highly organised crime syndicates. In South Africa, it has been confirmed that the same crime syndicates that rob banks, also rob casinos, jewellery stores, C-I-T vehicles and bomb ATMs. However, it must be borne in mind that not every single gang is organised and experienced. There are some gangs that are opportunistic, copycat gangs, who saw the upsurge in ATM bombings as an opportunity for them to make a ‘quick buck’. These types of gangs often fail at attempts to gain access to cash in the ATM safe. Also, they appear to have no or inadequate knowledge on how to use explosives and often injure themselves in their attempts to bomb ATMs (Geldenhuys, 2009: 38).

### 5.3 PLANNING THE ATTACK

While detailed information regarding the manner in which an ATM bombing is planned, may come from the criminal, there is much that can be learned about the planning of an attack from the perpetrators modus operandi during the attack.\(^5^6\)

While the bombing of ATMs initially started off with the aforementioned so-called copy cat criminals or opportunists, it soon turned into a highly organised criminal activity.

A criminal chooses certain days and times to commit his crime. Perpetrators of ATM attacks weigh the risks and benefits of days and times to commit their crime before attacking. Such

---

\(^5^6\) Since 2005 there have only been single prosecutions of ATM bombers. Accordingly no convicted ATM bombers could be tracked in prison as they were convicted on the broad crime category of theft/robbery (depending on the actual circumstances) and could therefore not be identified for an ATM bombing conviction so no perpetrator one-on-one interviews could be conducted to establish a perpetrator modus operandi. Accordingly modus operandi information is largely based on the analysis of reported cases in the media, the actual SAPS reported cases in the dockets, from the interviews conducted with investigators – all this information corroborated from the video recordings viewed by the researcher.
organised crime syndicates plan their crimes carefully, paying attention to every detail from the time and day of the attack to the escape route.

It starts with one person, who will decide on his team and brief them as to his idea. One arrested suspect stated in his confession that he was called and told that there was a job for him. He was given a time and place and asked to meet there. Of the people that were there, he knew almost everyone. He later discovered that the one person he did not know was responsible for planting the explosives into the ATM.

When asked about the amount of planning that goes into the bombing of an ATM, all interviewees agreed that it was a crucial part of the commission of the crime. The following was found from the interviews:

ATM bombing syndicates put much planning into their crimes. In planning their attack the group chooses a location and for a period of time prior to the attack they will stake out the location and conduct pre-surveillance on the target. They will take this time to work out their escape routes; vehicles they will use during the job; what time they will carry out the attack and select a specific suitable day taking all factors such as busy times, traffic volumes, and other security measures present or not present. This will be based on observations that are carried out in the time spent on pre-surveillance of the chosen target. The gang will spend a long time merely watching a target; checking to see when it is replenished; what time security guard patrols come past; what time the police patrol the area, etc. Once they are satisfied that they will not be disturbed at a certain time and that on a specific day there will be a large amount of cash in the machine, they will set their day and time.

As in the case of C-I-T robberies, the day that the attack will be carried out will be the day of or a day after the ATM has been loaded to ensure a large amount of money.

---

57 All those who were interviewed spoke of similar details regarding planning.
5.3.1 Popular days and times for ATM bombings
Evidence that specific days are planned ahead can be confirmed from the analysis of media reports and case dockets. The researcher found that from the total of the 100 SAPS dockets the most common day that an ATM bombing occurred was on a Thursday, with 21 incidents out of the hundred (100) analysed occurring on this day. The second most common day was that of Tuesday, with 18 incidents occurring on this day. Media reports and ATM Solutions dockets produced similar results. Most incidents from the analysis of media reports took place on a Thursday, while ATM Solutions dockets reflected 54% of cases occurred on a Thursday.
The days on which the lowest number of ATM bombings occurred were Fridays and Sundays.

While there is no specific time that is chosen, the most common period for which ATM bombings occur is between midnight and 5:00 am.

5.3.2 Expert members, other helpers and gang member’s role in the team
Syndicate gangs may recruit someone for example a security guard, especially in isolated areas where there is no one else but a single security on duty to inform them once the police/security patrol vehicle has done its rounds. It has also been suggested that cash-in-transit personnel who load the ATMs may work with these groups, informing them when the ATM is “full”. Alternatively, this forms part of their pre-surveillance.

Prior to the job, each member of the group will be informed by the leader or organiser of the operation of their function in the team. While there will be one or two members in charge of loading explosives into the ATM, others may be designated as drivers, in charge of holding guards hostage during the attack or patrolling the premises, armed and ready should they be confronted by the authorities (police) or a private security company armed response team.

This modus operandi was evident from statements obtained from security guards and eyewitnesses as reflected in both the SAPS dockets and the ATM Solutions investigation case reports, as well as statements made to the media by eyewitnesses.
An example of a case in which their duties were clearly defined is one where six to eight suspects arrived at a petrol station in Mooinooi armed with R5 rifles and 9mm pistols driving a white double cab LDV, with their faces covered with balaclavas. They entered the shop site where they held the petrol attendants and cashiers at gunpoint. Four suspects came into the garage while others were on observation outside having secured the perimeter as ‘point men’. One of the suspects then came in with a crowbar and the explosives where he tried to force open the throat of the ATM’s machine safe to place explosives. Failing to do so they all fled the scene, the driver of the vehicle was still in it and the engine was still running ready for a quick getaway (SAPA, 2008q).

While this was not discernible from case dockets, the media often made statements regarding the involvement of not just security guards and C-I-T personnel but also members of the police. Media reports on arrests of police personnel confirm that gangs ensure that expert members from the SAPS and other paramilitary structures are included as part of the syndicates.

In June 2008 the station commissioner at the Nyanga Police Station, Snr Supt Duma Ntsezo, turned himself in after commercial explosives, ammunition and 18m fuse as well as a rifle grenade, bulletproof vests and battle jackets were found at his home in the Eastern Cape (Rank and Nombembe: 2008). Also in 2008, three North West police constables were arrested in connection with ATM bombings (SAPA, 2008e). Other police officials connected to ATM bombing cases also included a West Rand dog handler, who handled sniffer dogs that are trained to identify explosives. He was positively linked to three ATM bombings on the West Rand (Molosankwe: 2008).

5.3.3 Purchasing of explosives

Part of the planning carried out by these syndicates is the purchasing of explosives. They need to ensure that they have the correct amount of explosives, enough to blow open the safe and not do too wide damage to surrounding areas and in the process harm or kill themselves as well as someone who knows how to use the explosives. In the case mentioned above, the one person that the suspect arrested offender did not personally know when the gang first came together, was the person who had placed and detonated the explosives. This suggests that the recruitment of people
who have knowledge regarding the handling of explosives is often outside common criminal circles and from an industry of mining where expertise in blasting can be obtained. The fact that they tend to use the correct amount of explosives and injuries, although reported, seldom occur, means that they either have someone who teaches them how to use the explosives and the amount to use or they make direct use of an explosives expert. As will be elaborated below, in most cases of ATM bombing, bombers are successful and not the other way around as often stated in media reports quoted by bank spokespeople. Explosives used are believed to come from the mines and/or construction sites. Corrupt mine workers steal explosives from the mines and sell it to criminals on the street. For example, in August 2008, an Impala Platinum mine worker (a Mozambican national) was arrested for having been believed to be selling explosives to syndicates. He was believed to be supplying bombing syndicates across the country with explosives and was linked to syndicates as far away as KwaZulu-Natal and the Eastern Cape (Hosken, 2008b). An employee of Consort Mine, Mduduzi Maseko was also arrested for involvement in failed ATM bombings and was said to have provided explosives to three other suspects (Labuschagne, 2008).

Although unable to describe each of them in detail, the following commercial explosives and explosive devices were most often found at crime scene:

V6 explogel (Sasol)
Khubela explosives
PMP1-S cone packs
Trojan
Powergel, and
African Explosives Ltd (AEL);

5.3.4 Size of gangs

While many media reports, reported that gangs of between fifteen to thirty men are responsible for the bombing of ATMs, this is not entirely accurate (Sewpersad, 2010b). The size of the gang often depends on the selected target. If the targeted is considered to be an easy target, where there are no guards and limited chances of being noticed, the gangs tend to be smaller in
numbers. Smaller gangs will also often choose targets in remote areas, while larger gangs will take on any target, including petrol stations.

In almost all of the one hundred dockets analysed, the exact size of the group was not clear and approximate numbers were given based on witnesses’ accounts of the crime. Even where an exact number was given, it was based on what someone saw. Additional members of the gang may have been out of sight during the occurrence of the crime, i.e. further away on perimeter or across the street as on observation to see if there are any response teams arriving or police patrols driving past. In other words unobserved members may well have been present but on the lookout on the perimeter of the premises, where they could not be seen by others (eyewitnesses and victims). In one case, a witness who looked out of his bedroom window when he heard the sound of the explosion mentioned seeing a car at the corner of the street in his statement. This car and its occupants may have been involved in the crime as it was just parked at the corner and drove off shortly after the explosion. No other witnesses mentioned seeing that particular car in their statements (SAPS Docket No. 29).

Out of the one hundred SAPS dockets analysed, forty-nine such dockets indicated that the number of suspects were unknown. This was attributed to the fact that there were no witnesses to the crime and no CCTV cameras at the crime scene. This further implies that in almost 50% of the cases there was no one who saw what happened or no CCTV surveillance footage that can assist in the investigation of the crime.

From the remainder of the cases analysed, where numbers indicating the size of the group involved, only twenty cases indicated a number that was inclusive of “+/−” (plus/minus). All the other cases suggested uncertainty regarding the size of the group by the inclusion of “+/−” before the number. These numbers ranged from +/-two (2) to +/-fifteen (15) black males having been seen at the crime scene and/or involved in the commission of the crime. The majority of the cases reported approximately three black males having been seen at the scene, with four black males being reported as the second most often number of participants. Ten cases indicated that +/-three suspects were seen and eight indicated that four suspects were seen. The number of suspects in a group, ranging between one and fifteen (excluding three and four) appeared in
between one and four of the cases examined. Larger groups of suspects were often involved in cases that involved an ATM/s at shopping complexes, malls or petrol stations. One case alleged the involvement of fifteen males which took place at a shopping complex. Two cases indicated the involvement of a gang of twelve men, which took place at malls as did a case involving nine suspects. Those cases involving larger groups that took place at petrol stations consisted of two cases of nine and ten suspects respectively.

An analysis of media reports, on the size of gangs, indicated that the average sizes of gangs are often between four and eight men. The most common size of gangs indicated in media reports were five.

Regardless of the size of the group all witnesses stated that the groups consisted only of black males. This was confirmed during interviews as well as from CCTV footage. However, what cannot be assumed is that these black males consist only of South African black males. It is believed and confirmed by investigators who were interviewed that some foreign nationals have also been recruited in ATM bombing syndicate gangs.

5.3.5 Weapons

Other than the direct danger, caused by the use of explosives by non-professionals in a way that it is not permitted to be used, perpetrators themselves have continuously been reported to be dangerously armed. The selection and use of weapons is an important aspect in the planning phase of ATM bombings.

Although the analysis of dockets show only a small number of perpetrators having carried firearms during the commission of the crime, it is believed that in a number of cases gangs were heavily armed. The firearms are not always visible and those members that carry the heavy armament are those on the lookout posts on the perimeter and not readily visible to eyewitnesses or to CCTV camera surveillance. These suspected heavily armed members appear not to hesitate to make use of their firearms if confronted by authorities. There have been numerous reports of gun battles between perpetrators of ATM bombings and the police. In many of these reports both suspects and police have either lost their lives or been injured as a result of being shot. Such gun
battles not only take place at the scene of the crime, but also at the residents of offenders when attempts have been made to arrest them.

The analysis of SAPS case dockets indicated that in cases where firearms of suspects where used or their carrying of firearms were seen by witnesses, it is always mentioned that the suspects “were armed”. However, in cases where suspects did not use firearms or witnesses did not see it, no mention at all is made about firearms in dockets. Therefore, it is deduced that where no mention is made about firearms in a docket, one cannot say that the suspects were armed or that they were not. It could have been either way, and the absence of evidence pointed either way leaves it as an unknown.

Of the 100 police dockets analysed, 64 dockets did not mention the use or presence of firearms of any kind in the crime. The remaining 36 indicated that the suspects were armed, with the type of weapons being unknown in eight of the 36 cases. In the remainder of the cases, thirteen cases mentioned the suspects having carried or used automatic rifles (usually AK47 rifles). In thirteen cases mention was made of either just handguns or 9mm pistols being used or carried. In five cases, it was said that suspects were armed with both rifles and pistols.

Dockets analysed from ATM Solutions produced similar results with 29% (18/62) reflecting the use of firearms. Both AK47 rifles and 9mm pistols were mentioned in those cases as well as the use of R5 rifles and in one case a grenade.

Other military type weapon such as R3/R5s may belong to members of the South African National Defence Force (SANDF), while AK47 rifles are most likely to be from arms caches in neighbouring states and smuggled in from previous areas of conflict such as Mozambique and Angola and then bought in townships on the black market (see Minnaar, 1994 & 1998). Members of both the SAPS and the SANDF were arrested in connection with ATM bombings but there were no reports of prosecutions resulting from these arrests. In an interview with a commanding officer at SAPS SOCS, he told a story of how a firearm he was supposed to have booked in as evidence himself, but trusted the task to a colleague, was found to have been used some months later in the commission of another crime. It was soon discovered that that very same colleague
who he has entrusted to book in the weapon, had rented it to a criminal as he had done with many other weapons booked in as evidence (SAPS 1, 2010).

5.3.6 Dress code
Little evidence was found that suggested a specific dress code of ATM bombing syndicates. However, in all the cases where there were witnesses, they indicated that all the suspects wore balaclavas. In addition, the CCTV footage provided that was analysed showed all suspects, in all of the video footage wearing balaclavas.58

5.3.7 Bank brand ATM59
Since some banks seem to be targeted more than others, it can be suggested that perhaps perpetrators prefer certain bank brand ATMs and as such, during the planning of the attack, they also decide on which bank brand ATM to target.

The information supplied in this paragraph are mere research findings and may not reflect that a certain bank lacks security measures. There may be a number of reasons why certain banks are targeted more than others. In this section the researcher will provide reasons why this may be the case. These reasons provided are purely deductions made from the research findings.

While the problem of ATM bombings have affected the banking industry at large, some banks may have been affected more than others with regard to the number of their ATMs that have been chosen as targets and bombed. The costs of replacing or repairing an ATM, as discussed in Chapter 1, costs the banking industry million’s a year. The more ATMs of a particular bank that are blown up, the more it is going to cost that particular bank to repair or replace the ATMs. In an attempt to establish the bank most affected, the researcher recorded the bank brand ATM that was bombed in each case studied. This is inclusive of the 100 dockets analysed from SOCS and the 62 investigation dockets from ATM Solutions. To avoid duplication the researcher

58 This has been a major contributing factor to the low level of ATM bomber convictions since video footage cannot decisively identify perpetrators that are disguised with balaclavas. Arrests have most often occurred when police have been able to respond quickly enough to interrupt the crime-in-progress or acting on prior information been able to ambush or surprise the attackers as they commit the attack, or alternatively arrest perpetrators after the fact based on informer supplied crime information.
59 The information supplied in this section is a mere research finding and may not reflect a certain bank/s lack of security measures.
eliminated the dockets of ATM Solutions that reflected the same case which a docket from SOCS reflected. In addition, the researcher did not make use of the numbers from the media reports in combination with the numbers in the two sets of dockets as the same case may then be counted twice. Therefore, the number of ATMs blown up as reflected in the analysis of media reports will be dealt with separately. The researcher will not eliminate this source altogether as media reports do not cover every single bombing in Gauteng and may include many cases that were not covered in the docket analysis.

In the majority of the media reports analysed it was reported that Standard Bank ATMs were targeted the most. However, the number of ABSA ATMs bombed, reflected in media reports, are not far behind the number of reported Standard Bank ATMs targeted. FNB and Nedbank consisted of a smaller percentage in media reports. Capitec and merchant-filled (not a bank brand) machines were the least affected.

At the time of research (2009), as mentioned in Chapter 1, ATM Solutions provided and serviced ATMs for only ABSA and Standard Bank part of the major South African banks. Other than that they provided merchant-filled machines that are not branded. For this reason, the findings regarding bank brands could be false as the dockets do not provide a representative sample.

An analysis of ATM Solutions dockets indicated that ABSA ATMs were most affected. Accordingly only 23% of the ATMs from the 62 dockets analysed were that of Standard Bank, 78% were that of ABSA and 1.5% were non-branded merchant-filled machines.

On the other hand, SAPS SOCS 100 dockets produced different results. According to the analysis of SOCS dockets, 41 of the 100 case dockets analysed indicated Standard Bank ATMS; 32 were ABSA ATMs; 14 FNB; four Nedbank ATMs and only one Capitec ATM. In addition, six dockets did not reflect the brand of the bombed ATM. This could mean that they were merchant ATMs or the investigating officer failed to include that detail in the docket.

---

60 It should be borne in mind that not all media reports mention the bank brand of the ATM bombed, whereas most (SAPS) and all ATM Solution dockets do so.
61 Some cases involved more than one ATM which were not necessarily of the same bank but placed next to each other.
The diagram below shows the split graphically:

**Figure 5.1: Percentage of incidents per bank brand as per SAPS dockets**

Overall it would seem that Standard Bank ATMs were targeted most often. This may be for a number of reasons. For example, it might just so happen that ATMs in the areas most affected have more Standard Bank ATMs installed there or perpetrators may find that Standard Bank ATMs are most often easily penetrated or that they generally have more cash. The mere fact that Standard Bank and ABSA are South Africa’s two biggest banks could be the main reason why they are targeted the most.

### 5.4 THE ATTACK

#### 5.4.1 Tools used

The two most important and most frequently mentioned ‘tools’ used during the commission of an ATM bombing are a crowbar or similar steel object and commercial explosives. Every single docket analysed and the media reports mentioned that commercial explosives were used to bomb the ATM. What is most worrying is that generally commercial explosives are used only in mines and for underground blasting at construction sites. Commercial explosives are government

---

62 Modus operandi information was derived from the analysis of witnesses account of events, CCTV footage and other information pertaining to it in case dockets.
authorised and only those who are authorised to do so and in the possession of special permits may use them.

Expert statements were the only form of information regarding the types of commercial explosives used to bomb ATMs. As mentioned in chapter 2 the majority of the statements were written in Afrikaans which made it difficult for the researcher to understand. However, the researcher was able to identify the types of explosives, detonating cords and fuses that were mentioned in certain cases. Very few cases provided evidence of the actual explosives that were used. However, from the damage caused to bombed ATMs, experts were able to deduce that commercial explosives were in fact used. In most cases that provided information regarding the explosives’ equipment, remnants of safety fuses and detonating cords were found at the scene.

5.4.2 Vehicles used

ATM bombing syndicates always use motor vehicles as a mode of transport to and from the scene. Depending on the size of the gang, they will arrive in anything between one and seven\textsuperscript{63} motor vehicles. The vehicles used during the commission of the crime may be stolen or hijacked or may even be the perpetrators’ own vehicle. It was difficult to ascertain exact ownership since some of the vehicles used did not have registration plates while others that had plates, were false. The latter was most often the case from the information gathered from both sets of dockets examined. In one case a maroon BMW was used during an ATM bombing. A witness took down the registration number of the car and upon investigation, it was found that the registration number was linked to a person who drives a maroon Mercedes Benz (SAPS Docket No. 11). This points to the fact that in their planning the perpetrators simply duplicate the registration of a car similar to the one intended to be used during the perpetration the crime.

In another case, a gang of ATM bombers had planned an attack on an ATM at a shopping centre. Two young students, driving in the vicinity of the mall were stopped by the perpetrators who got into the car then ordered them to drive their vehicle to the premises of the shopping complex. The complex was closed off and the perpetrators cut open the gate which was locked. When the victims drove into the complex, one of the ATM bomber gang members stayed with them and

\textsuperscript{63} Seven vehicles were the highest number of vehicles used in an attack as indicated from all the information analysed.
the others got to work. They later dropped off the students somewhere else and took their car. The car was later found abandoned. When approached the student to whom the car belonged said that he did not report the incident as he feared for his life (SAPS Docket No. 67).

5.4.3 **Arrival at the scene and gaining entrance**

As stated above, syndicates will adapt their *modus operandi* to the chosen target. The following is a discussion of the manner in which ATM bombing syndicates gain access to different premises in order to get to the ATM.

5.4.3.1 **Gaining access to the premises where the ATM is located**

In cases where an ATM is situated in a fenced off area, the perpetrators would need to gain access to the premises. If it is merely fenced off with no access control, perpetrators cut open a hole in the fence and enter and escape through that opening. In situations where there is an access control system with guards at the entrance, the perpetrators will subdued the guards (see sub-heading 5.3.4 below) and get to the ATM. In one case two suspects, on foot, approached a security guard at the entrance, held him at gunpoint then forced him to call the other security guard and held both of them at gunpoint. The suspects then called a third suspect who was carrying a shopping bag with crowbar, bolt cutter and explosives inside. This third suspect then cut through the locks to gain entry to the premises where they were then able to bomb the ATM (SAPS Docket No. 71).

5.4.3.2 **Gaining access to an in-store ATM**

As discussed above, ATM bombings usually take place at night at any time between midnight and 5am. Most stores that house an ATM tend to be closed during this time. An exception to this is the 24/7 convenience stores at petrol stations, but these have been a more recent phenomena with more of this type only being opened in the last two years. In order to gain access to such closed stores after operating hours the perpetrators will break in. They do this in one of two ways. The first method used to gain access and the one that is most used by ATM bombing syndicates, is gaining access through the entrance doors of the shop by breaking the burglar gates and doors and then breaking the window or glass door and entering the shop. They use different ways to get through the first burglar door. The most common means is using an angle grinder,
bolt cutter or other such object to cut the pad locks off the burglar-proofed door. They may also forcefully cut through the burglar bars. Once they have passed the burglar-proofed door, they will either break the glass door, or force it open and gain entrance to the shop. In 73% of the cases involving in-store ATMs (from ATM Solutions’ dockets), the perpetrators gained access to the shop using these methods. In one case, the perpetrators used explosives to blow open the door.

The other method used to gain access to in-store ATMs is through the roof. They will do this by cutting a hole through the roof. Once inside, they immediately cut off (disconnect) the alarm system. From the dockets analysed from ATM Solutions, of those cases that involved in-store ATMs, 27% involved gaining access through the roof. In all cases where access was gained through the roof, the alarm wires were cut before the ATM was bombed. In order for them to know exactly where to enter so that they are closest to the alarm system box, they must have been in the store before, or have someone who works at the store feeding them information.

Only four cases of the SAPS dockets involved in-store ATMs. Three of those four cases involved perpetrators entering through the roof of the premises and disarming the alarm system.

5.4.3.3 ATMs at petrol stations
When a gang enters a petrol station with the intention to blow up the ATM which is situated either inside the convenience store or outside, they do not always immediately attack staff and approach the ATM. They will approach the petrol station and pretend to be potential customers, either wanting petrol or purchasing something from the store. Once they have staff and customers (if any) believing they are customers, they will catch them off guard and hold them at gunpoint and restrain them (as discussed below in sub-heading 3.4) (Sewpersad, 2010a; Sewpersad, 2010b). In almost all64 cases involving ATMs at petrol stations, perpetrators first pretended to be customers. In one incident at a petrol station, suspects arrived in two cars, but parked far from the petrol pumps. One suspect got out of the vehicle and walked to the window and purchased something. While this was going on others held up the attendants, who were

---

64 Cases from SAPS dockets, ATM Solutions and media reports that included detailed information on ATM bombing cases.
sitting in a small room and other members of the gang then proceeded to blow up the ATM which was situated outside. The staff members in the store were still unaware of what was going on outside until they heard the explosion and as a result did not have time to react. Before they knew it the suspects had collected the cash and drove off. In video footage viewed of a number of ATM bombings at petrol stations the average time to secure the scene, place the bomb, blow up the ATM, take the money and make a getaway was 4-6 minutes. This points to the planning, experience and slickness of the operation by gang syndicates. The response, if any, from police or security officers being at best only after five minutes and usually at least ten minutes later and by then the bombers had already left the scene. In one of the videos perused the police had responded after 4 minutes 25 seconds but then only because a SAPS patrol happened to be in the vicinity.

5.4.4 Security guards, police and civilians

In almost all the cases where a security guard was present at the scene during an ATM bombing, the security guard was held hostage by certain members of the gang, while others blew up the ATM. In the cases where the security guard was not subdued by the perpetrators, it was due to the fact that he was hiding or not noticed by the (Sewpersad, 2010a; Sewpersad, 2010b).

In most cases the security guard was held at gun point, tied up and robbed of his firearm (if armed); panic button (if he had one), two-way radio and his cell phone. In addition, the perpetrators order them to lie face down on the ground and to look down. In some cases they were hit with the gun. If a guard room is available on the premises where the ATM is located, those in charge of taking care of the guards will keep them inside the room. If there is no guard room they will keep the security guard/s at a separate location away from the ATM site (Sewpersad, 2010a; Sewpersad, 2010b).

In some cases, the perpetrator will return the guards’ cell phone just before they leave the scene. The only reason they take away their cell phones is to ensure that they are unable to make any calls.

---

65 All security guards in the cases analysed were male.
If during an attempt to bomb an ATM, police arrive at the scene, those that are on the lookout will warn the other gang members and they will attempt to flee. While attempting to flee, they will open fire at any police official or security officer that is standing in their way. As a result of this, many law enforcement personnel and suspects have lost their lives or have been injured. In one case, a gang stormed an Engen garage in Villieria, Pretoria, held up staff and bombed the ATM. Police arrived at the scene after an alarm had been raised only to find themselves ambushed by the gang members. The resultant gun battle led to a police officer being shot in the neck. He died at the scene due to severe blood loss and neck damage (Otto, 2009).

In cases where the target is at a petrol station, the perpetrators will subdue the staff and customers (if any) at the petrol station in almost the same way they do the security guards. Everyone is asked to lie face down on the floor of the store and they are robbed of their cell phones (Sewpersad, 2010a; Sewpersad, 2010b).

5.4.5 Working on the ATM

Those members of the gang that are expected to blow up the ATM almost always know exactly what to do and how to do it correctly. As previously mentioned, one of the tools used during the bombing of an ATM is a crowbar or similar object. In 34% of the dockets (from both SOCS and ATM Solutions), mention was made of a crowbar or piece of steel rod found at the scene. All video footage analysed showed ATM bombers making use of a crowbar or similar object.

While at the ATM, the perpetrator will first try to enlarge the ATM cash dispenser. He does this using a crowbar or similar iron tool. All the case dockets, including those of ATM Solutions with information regarding where explosives were inserted into the ATM mentioned that it was inserted via the throat of the ATM. However, a few mentioned that in some cases they also break the screen of the ATM, thereby creating a hole in the front of the ATM thereby getting at the inside of the ‘throat’.

Once they have enlarged the throat of the ATM and/or broken the screen, the perpetrator has now created an opening/s through which to insert the explosives into the ATM proper, i.e. not
merely just blowing off the housing cover.\textsuperscript{66} Explosives are inserted directly into the safe via the cash dispenser and the fuse lit. They use an appropriate length of fuse that gives them a certain time delay to move away from the ATM before it sets off the explosion. Some even drive off and return after they hear the explosion. Once the explosives have been detonated they return to collect the cash from the ATM or there will be others at hand with bags waiting to load the cash and flee.

\textbf{5.4.6 Collecting the cash and frequency of success in accessing the safe}

Once the ATM safe is exposed those waiting to collect the cash fill up their bags and run off to the vehicle/s waiting. Perpetrators immediately flee the scene after collecting the cash. Those that collect the cash from the machine, signal the rest of the gang once they are done and everyone rounds up, jump into the waiting getaway vehicles and drive off. (As mentioned above the whole operation is often completed within 4-6 minutes and in one case on the video footage perused three minutes).\textsuperscript{67}

\textbf{5.4.6.1 Cash accessed/taken and cash recovered at the scene}

In almost all media articles reporting incidents of ATM bombings, experts\textsuperscript{68} in the field are quoted as having said that despite the increasing number of ATM bombings taking place across the country, it is very seldom that perpetrators get away with the cash from the ATM. They add that in most cases, perpetrators fail to gain access to the safe, thereby leaving empty handed. Notwithstanding these statements which are continuously printed, 73\% of 100 media reports analysed reported cash being stolen during the crime.\textsuperscript{69} (See below for SAPS and ATM Solutions’ docket information on this aspect of ATM bombings).

Perpetrators do sometimes fail to blow open the safe where the cash is housed. However, this is mostly due to “inexperience” on the part of the perpetrator/s, insufficient explosives having been

\textsuperscript{66} Apparently some of the first bombings and copycat attacks merely placed the explosives in such a way that just the covers of the ATM were blown off. This necessitated the placig of a second charge to blow open the ATM safe in order to get at the cash. These ‘failures’ led to the method of inserting right into the dispenser ‘throat’ of the machine (Interviews with SAPS and ATM Solutions investigators).

\textsuperscript{67} Footage provided by ATM Solutions.

\textsuperscript{68} These may include bank custodians and spokespeople.

\textsuperscript{69} No two media reports analysed were about the same incident, if it was about the same, the information contained in the two reports were combined as one case.
used or maybe even bad-luck. This is because incorrectly placed explosive charge, failure to ignite fully or too little explosive charge used on the part of the perpetrator (Sewpersad, 2010a; Sewpersad, 2010b). Inexperience usually indicates a new gang, perpetrating the crime of an ATM bombing for the first or second time or copycat criminals trying their luck bombing an ATM after hearing or reading about it in the media. One arrested suspect indicated in his confession that after being recruited into a gang, their first attempt at bombing an ATM was unsuccessful as was their second, and they did not gain access to the cash in the perpetration of their first two ATM attacks. However, on their third attempt, they were successful and each received a share of R3 400. The remainder of his confession indicated successes in all other ATM bombings they committed (with the exception of the first two), where the reason behind the unsuccessful attempt was having being disturbed and as a result leaving immediately. Furthermore, after a small share of R3 400 in their first successful ATM bombing, the suspects’ share subsequently increased every time – bearing in mind that there were eight members of this gang and the splitting of the cash was not equal being dependant on the role each member of the gang played in the bombing and/or his position in the specific gang’s hierarchy (Sewpersad, 2010a; Sewpersad, 2010b).

From the one hundred dockets analysed, in only 34 cases were the perpetrators unsuccessful in gaining access to the cash while in 57 cases they were successful. The remaining nine dockets did not clearly state whether or not the cash was accessed. In addition to this, during interviews, all interviewees indicated that cash was stolen in most cases (SAPS 1, 2010; SAPS 2, 2010; ATM Solutions 1, 2009; ATM Solutions 2, 2009).

While in the majority of cases it is unknown what amount of cash was stolen, the cases where it is known indicate anything between R9 000 and R300 000 was stolen. This range is only from 100 cases. In one of the cases, the ATM safe was empty and no cash was lying around the scene other than that which was destroyed in the explosion.

---

70 Banks routinely decline, for inter alia banking and client confidentiality and security sensitivity reasons, to publicly release exact amounts of cash stolen.
When an ATM safe is blown open in an explosion, the perpetrators cannot always take all the cash and seldom do. As a result there is cash that is lying around the scene, which includes both damaged and undamaged notes as well as remaining inside the ATM. Sometimes the cash left behind amounts to more than what was stolen. Of the one hundred dockets analysed twenty-five included the amount of cash recovered from the scene. These amounts ranged from R140 to R281 000. From the cases where both the amount of money stolen as well as the amount recovered is known, which amounted to only seven cases, in most cases (6/7), the amount stolen is more than the amount recovered at the scene. In only one of the cases where both the recovered and stolen amounts were known, was the amount stolen far less than that which was taken (i.e. R90 000 stolen and R195 000 recovered at the scene). Of the six cases where the amount of money recovered and stolen are both known, the stolen amount exceeds the recovered amount, an average of the six amounts to R132 361.67. More money is stolen than that which is recovered at the scene. In one particular case, as little as R140 was recovered while R178 630 was stolen by the perpetrators (SAPS Docket no. 53). Furthermore, out of the 62 internal investigation dockets of ATM Solutions, 47 cases reported that cash had been stolen from the ATM. That is in 76% of those cases, cash had been stolen.

5.4.7 Deaths and/or injuries resulting from ATM bombings

In any situation that involves the use of deadly weapons and that of explosives, whether it is at work as a miner or construction worker, a soldier fighting in the army, a police officer or a professional ATM bomber, there is a risk of death or injury. Many suspects, police officers, civilians and security personnel have been injured or lost their lives as a result of this crime.

While an analysis of dockets did not reveal any deaths resulting from the cases studied, numerous media reports reported on both deaths and injuries. Such deaths and injuries may have been a result of a gun battle between police and suspects at the scene or during a police raid of a suspects’ place of residence, or as a result of the explosives used in the commission of the crime. While the researcher made no findings of police being injured as a result of explosives, numerous suspects were injured in the commission of the crime as a result of explosives, e.g. SAPA, 2007d (Sewpersad, 2010b). In one case, a suspect blew off both his arms and later died in hospital. Interviews confirmed death and injury of suspects as a result of explosives (SAPS 1, 2010; SAPS 2, 2010). One interviewee mentioned that it is easy to tell when a person has been
injured as a result of an explosion (SAPS 2, 2010). He further stated that in such a situation, the injured suspects’ gang member would usually leave and drive the injured suspect to a hospital where they would drop him off at the emergency/trauma section (SAPS 2, 2010).

From all the SOCS dockets, in only one case was a person reported injured and in two other cases, traces of blood was found at the scene. However, the perpetrator could have been hurt in a number of different ways other than by explosives. For example, he could have been hurt from breaking the screen or a tool or he could have been hurt by a sharp piece of the ATM after the explosion while removing the cash.

Although few dockets reflected injuries, there were other cases where shots were fired by perpetrators, either as warning shots to police or to chase away security guards on duty.

### 5.5 POST-ATM BOMBINGS ACTIONS

Very little is known about what goes on after an ATM has been successfully bombed. However from interviews and a suspect’s confessions, the following can be presumed:

Prior to the commission of the crime the gang will make arrangements as to where they will meet afterwards. This location may or may not be a house of one of the gang members. When asked whether gang members trust each other with such a plan, as it seems possible that the person/s with all the cash can run off with the money, investigators mentioned that while there is much distrust amongst gang members, they also fear that if they were to do that, they will be tracked down and killed by the other members.

In fact, the amount of distrust is such that when they arrive at the scene and all the money is laid out to be divided, all gang members are required to remove all their clothing. They do this to ensure that no one has stolen any of the stolen cash.
5.6 SUGGESTED PROFILE OF AN ATM BOMBER

Owing to the lack of information of convicted ATM bombers,\(^\text{71}\) the researcher cannot make valid and reliable comments on the profile of ATM bombers. In order to do this one would need to look at the biographical information of a representative sample of convicted ATM bombers in South Africa.

However, from media reports and witness accounts of suspects, the following can be suggested about the profile of ATM bombers (Sewpersad, 2010b):

**Gender:** Male

**Race:** Black but not only of South African nationality

**Age:** between 23 and 45

**Education and employment:**
It was pointed out during interviews that some criminals are actually educated and are in the possession of post-matric qualifications. In addition, most have legitimate day jobs, although many are unemployed and crime is their only form of employment. (SAPS 2, 2010; Sewpersad, 2010b)

For example, Lebohang Nicholas Ranyali (23) from Welkom in the Free State who was arrested in 2007, is a former engineering student an electrician (Nare and Sishi, 2007). This particular offender was believed to be the mastermind behind ATM bombings across the country (Nare and Sishi, 2007). Soweto resident Mzwakhe Gule (44), a married father of three who was also arrested and the first to be convicted for ATM bombings, owned a taxi business that transported children to school (Peters, 2008).

\(^{71}\) Due to the lack of evidence available few ATM bombing cases have been successfully prosecuted. As a result there is a low number of convicted ATM bombers available to be interviewed and the conviction record only states robbery which makes it difficult to identify and then interview of such criminals in prison (convicted specifically for ATM bombings).
5.7 CONCLUSION

What was learnt from the modus operandi of the ATM bombing syndicates is that they are highly organised and plan their crimes meticulously. In addition, they are usually heavily armed. All members of the gang, with the exception of the designated ‘bomber’ are usually armed with pistols/revolvers (handguns) and rifles (AK47s preferred but a sprinkling of R3s/R5s mentioned in dockets) and they can be extremely dangerous if threatened. All of these gang members make use of vehicles to get to the scene and to make their getaway. Explosives used are commercial explosives, with the source being largely the mines but can also be sourced from construction sites where blasting operations occur. Explosives appear most often to be obtained on the black market supplied by miners or workers on mines. A large proportion of cases perused indicate that sums of cash were obtained from the bombing and such successful bombings of ATMs appear to be lucrative as reasonably large sums of money are made off with.

Information regarding the modus operandi of ATM bombers, knowledge of the nature and extent of ATM bombings, crime scene characteristics and preventative measures, give power to role-players. In the concluding chapter recommendations regarding preventative and deterrent security measures and procedures will be outlined in support of the profile and modus operandi findings.
CHAPTER 6
SUMMARY OF FINDINGS, RECOMMENDATIONS AND CONCLUSION

6.1 INTRODUCTION

The value of this research is that it demonstrates the extent and seriousness of the crime of ATM bombings in South Africa and the need for existing ATM security measures to be upgraded. It provides a comprehensive overview of the lack of sufficient security measures currently in place at ATMs to protect against the use of explosives. Detailed information is provided regarding the extent of the ATM bombings and the modus operandi of ATM bombers and ATM bombing syndicates. The information based on the modus operandi of ATM bombers can be used by the banking industry and SAPS to include both preventative measures and police methods in order to reduce and curtail such ATM bombings. Detailed security surveys, especially at high risk sites, can assist bank security personnel in reaching conclusions based on the current state of security at ATMs, so that they can find cost effective methods of improving security at ATMs. Improved and more integrated and detailed security measures around ATM sites will provide a deterrent and preventative effect on the actual occurrence of ATM bombings. Security hardening of sites overall, in a more holistic integrated manner should be implemented.

Crime information with regard to the modus operandi of ATM bombing gangs and information regarding lack of sufficient security measure must be used in conjunction with one and other in order that the information is utilised to its maximum extent. As such, questions such as: Are the safes currently used strong enough to withstand the force of commercial explosives? Will it cost more to replace an ATM damaged by explosives or to install an alarm sensor in the ATM throat at high risk sites? Need to be asked.

ATM security measures must be fully evaluated in the form of detailed security surveys at high risk sites in order for cost-effective and effective security measures to be installed so as to successfully protect ATMs. The long term benefits of installing technological devices that will not only deter ATM bombers but also assist in tracing criminals and increasing convictions, must be thoroughly evaluated.
6.2 SUMMARY OF RESEARCH FINDINGS

6.2.1 Summary of findings related to ATM site security\textsuperscript{72}

- Overall, there exists a lack of sufficient security measures in place at ATM site that will assist in deterring, detecting or delaying criminal activity.

- High risk ATM sites, which should be secured the most, are those which are most lacking in proper security measures.

- Most ATMs do not have CCTV surveillance cameras; CCTV surveillance cameras are not sufficiently made use of at both medium and high risk sites.

- Physical barriers protecting properties where ATMs are located, are insufficient and do not provide adequate delay or detection of suspicious activity; they are poorly maintained and easily bypassed or penetrated; and

- The alarm systems in stores that have ATMs are of little value since the perpetrators are aware of where they are and how they can be disconnected. Furthermore, if in-store alarms are activated during closed hours criminals tend to implement their attacks while stores are open to circumvent active alarms. Hence the need for alarms inside the actual ATM for example a sensor alarm in throat\textsuperscript{73} of ATM and when this is tampered with – ATM bombers use a crowbar or other similar implement to widen the throat so as to insert the explosives into the ATM.

- There is insufficient use of security guards at ATM sites, especially at shopping centres; Security guards at ATM sites are easily subdued and at time improperly used (for guarding/protective purposes or as a deterrent);

- Not all ATMs have their own alarms systems installed inside them.

- The East Rand, Greater Johannesburg and Pretoria were most affected by ATM bombings;

\textsuperscript{72} Chapter 4
\textsuperscript{73} See chapter 1 for definition.
• The ten most affected towns in Gauteng include Springs, Tembisa, Kattlehong, Brakpan, Soweto, Eldorado Park, Atteridgeville, Soshanguve, Kagiso and Roodepoort;

• Most ATM bombings take place at ATMs at the corner of streets and in central business districts and shopping centres and complexes in townships, towns and suburbs;

• Lighting at ATM sites, especially high risk sites are inadequate;

• Customer awareness information is not sufficiently displayed at most ATM sites;

• No ATMs have panic buttons;

• ATMs mostly appear to be insufficiently protected against the threat of an ATM bombing and thorough security surveys need to be done in order to establish fully the current state of security at ATMs to deter ATM bombers.

6.2.2 Summary of findings related to modus operandi

• ATM bombing syndicates carefully plan their attacks;

• Commercial explosives from the mines are used in these attacks;

• Mine workers are mostly responsible for the illegal sale of explosives;

• V6 explogel (from Sasol), Khubela explosives, PMP1-S cone packs, Trojan, Pength, and African Explosives Ltd (AEL) are the main types of (commercial) explosives used;

• The use of deadly weapons appear to be mandatory in ATM bombings;

• Standard Bank is the most common target of ATM bombings; and

• Most ATM bombings are successful, i.e. perpetrators succeed in accessing the cash.

74 Chapter 5
6.3 RECOMMENDATIONS

The recommendations made here will be based on all of the findings. The findings on areas most affected, modus operandi as well as the findings of the ATM site security audit are combined in order to be able to provide a comprehensive security survey sheet.

This security survey sheet and the notes on how a security survey should be approached was compiled by the researcher on the basis of the Security Risk Management Model and as such provides a security risk management approach to securing ATMs.

The survey sheet consists of a checklist of security measures not only on the physical ATM, but also at ATM sites and properties where ATMs are located as emanating from the research findings. The main reason or the main objective for conducting such a security survey is to improve the level of protection at ATMs against the threat of being bombed. By identifying as many security weaknesses as possible with the aid of a survey sheet and by rectifying them, the level of protection could be drastically improved. The survey sheet is recommended for use by bank security consultants or security risk management specialists. That is, the person who conducts the survey should have knowledge of and the ability to identify security weaknesses. He/she should also have the know-how on how comprehensive risk analysis should be conducted.

Detailed risk analysis and security surveying\(^7\) of ATMs according to their risk profile, will allow security consultants working for the different banks in South Africa to analyse the costs spent on improving security measures as well as to make the return-on-investment calculations (i.e. future costs’ and loss prevention savings) (see Rogers, 2008 for detail on aspects of the UNISA developed Security Risk Management Model).

The security survey is aimed at the following:

---

\(^7\) Detailed risk analysis would appropriately emanate from and be based on the findings of the initial security survey.
- to examine the current state of security measures at ATMs with a view to identifying security weaknesses; and

- to ensure that the minimum security measures required by the banking industry, legislation and by insurance companies are in place, in order that the security risk of ATM bombings may be managed cost-effectively.

### 6.3.1 Recommended security survey sheet

<table>
<thead>
<tr>
<th>Security measures</th>
<th>Yes</th>
<th>No</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. ATM alarm</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1 Is the ATM fitted with an ATM alarm?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.2 Does the alarm produce a superior force reaction?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.3 Does the alarm go off if the ATM cash dispenser is being tampered with?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Total &quot;yes&quot; answers:</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Total &quot;no&quot; answers:</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Security weakness factor:</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>2. Safes and cash</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.1 Are there set times and days for cash replenishment?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.2 Are employees of C-I-T companies regularly screened?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.3 Does the safe weigh at least 340kg/750lbs.?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.4 Are safes securely anchored inside the ATM structure?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.5 Type of safe used:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TL-15</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.6</td>
<td>Is safe door at least 1.5 inches in thickness?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----</td>
<td>--------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.7</td>
<td>Does the lock, if a combination lock is used, meet the standards of SABS?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.8</td>
<td>Is the cash in the safe equipped with special devices such as dye/tear gas packs?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Total "yes" answers:**

**Total "no" answers:**

**Security weakness factor:**

### 3. CCTV surveillance cameras

<table>
<thead>
<tr>
<th>3.1</th>
<th>Are CCTV cameras installed on the outside at the entrance of the store?</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.2</td>
<td>Are cameras installed at the ATM?</td>
</tr>
<tr>
<td>3.3</td>
<td>Is real time surveillance used?</td>
</tr>
<tr>
<td>3.4</td>
<td>Are the cameras operational?</td>
</tr>
<tr>
<td>3.5</td>
<td>Are they linked to a 24 hour centre?</td>
</tr>
</tbody>
</table>

**Total "yes" answers:**

**Total "no" answers:**

**Security weakness factor:**

### 4. Guards

<table>
<thead>
<tr>
<th>4.1</th>
<th>Are armed guards present at ATM sites after hours?</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2</td>
<td>How many guards are present?</td>
</tr>
<tr>
<td>4.3</td>
<td>Do guards have panic buttons?</td>
</tr>
<tr>
<td>4.4</td>
<td>Do guards have guard dog?</td>
</tr>
<tr>
<td>4.5 Do the guards regularly undergo integrity testing?</td>
<td></td>
</tr>
<tr>
<td>-----------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Total &quot;yes&quot; answers:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Total &quot;no&quot; answers:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Security weakness factor:</strong></td>
<td></td>
</tr>
</tbody>
</table>

**For in-store ATMs**

### 5. Doors of stores housing ATMs

5.1 Do entrance doors have a security gate?

5.2 Do the gates have any rust?

5.3 Are burglar gates locked by means of a padlock?

5.4 Are locks robust enough?

5.5 Is the entrance glass door made of bullet/shatter proof glass?

5.6 Is there a sensor connected to the alarm system on the door?

**Total "yes" answers:**

**Total "no" answers:**

**Security weakness factor:**

### 6. Alarm system of stores

6.1 Does the store have an alarm system?

6.2 Is the alarm operational?

6.3 Does the alarm sound at a 24-hour centre?

6.4 Does the alarm produce a fast reaction?

6.5 Is the alarm box visible?

6.6 Do any of the staff members know where it is?

**Total "yes" answers:**
### Total "no" answers:

### Security weakness factor:

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### For ATMs located on a fenced off property

#### 7. Fencing

#### 7.1 Fence environment

- 7.1.1 Is the fence area lit at night?
- 7.1.2 Is it regularly patrolled?
- 7.1.3 Is it inspected daily for holes?
- 7.1.4 Are "No trespassing" notices erected?
- 7.1.5 Do trees overhang the fence/wall?
- 7.1.6 Is there dense vegetation nearby?

#### 7.2 Non-lethal electric fencing

- 7.2.1 Is this fencing up to SABS specifications?
- 7.2.2 Are warning notices erected?
- 7.2.3 Does the fence have an electronic alarm?
- 7.2.4 Is the alarm effective?
- 7.2.5 Does the alarm sound at a 24-hour centre?
- 7.2.6 Does the alarm produce a fast reaction?
- 7.2.7 Does the alarm produce a superior force reaction?
- 7.2.8 Are all gates crawl-proof (rail gates)?
- 7.2.9 Are all gates locked or guarded?
- 7.2.10 Are locks robust enough?

### Total "yes" answers:

### Total "no" answers:

### Security weakness factor:
8. **Lighting**

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is security lighting provided (if needed)?</td>
<td></td>
</tr>
<tr>
<td>Are patrol routes lit up?</td>
<td></td>
</tr>
<tr>
<td>Are security checkpoints well lit?</td>
<td></td>
</tr>
<tr>
<td>Are all vulnerable areas well lit?</td>
<td></td>
</tr>
<tr>
<td>Are lights protected against damage?</td>
<td></td>
</tr>
<tr>
<td>Is there a secondary (UPS) power supply?</td>
<td></td>
</tr>
<tr>
<td>Is the power supply checked and tested monthly?</td>
<td></td>
</tr>
<tr>
<td>Are portable emergency lights available?</td>
<td></td>
</tr>
</tbody>
</table>

**Total "yes" answers:**

**Total "no" answers:**

**Security weakness factor:**

Once the security survey is completed, the information must be processed and a survey report must be compiled. In addition, all weaknesses must be calculated and prioritised and vulnerability factors must be calculated.

### 6.3.2 Recommendations on the use of special security devices

The following is a list of security devices that the researcher believes will make a contribution to the deterrence of ATM bombers and for the future prevention of ATM bombings.

#### 6.3.2.1 Tear gas/Dye pack devices

A tear gas/dye pack is a bank security device that resembles a regular stack of strapped currency that emits tear gas and red smoke and dye after being removed (Anderson 1981: 176). A 1980 study in the USA investigated the result of 171 bank robberies in where tear gas/dye packs left the banks with robbers and found that more than 1 000 robbers had been apprehended and financial institutions recovered more than $5 million as a result of the tear gas/dye packs (Anderson 1981: 176). The study found that banks that use tear gas/dye packs recover three to four times the amount of stolen robber money than banks that do not use tear gas/dye packs (Anderson 1981: 176). In South Africa, a company called “Deter-a-Dye Security” has developed
a dye staining system similar to this. The South African Bureau of Standards (SABS) approved the staining system\textsuperscript{76} (liquid discharge tube). The liquid discharge tube was designed to release a liquid (dye) in various types of containers. It discharges dye and stains the cash within 1.5 seconds (Deter-a-Dye, 2010). The actual dye cannot be washed off or bleached out and is designed specifically for staining bank notes and documents. This will have a great deterrent effect. It is recommended that this type of staining system should be used in ALL ATMs. This will render cash useless and thereby put a stop to ATM bombings. It may also stop other forms of attacks on ATMs.\textsuperscript{77}

6.3.2.2 Use of pepper spray in ATMs

Another delay or deterrent tactic in the form of security technology could include pepper spray which is activated when someone attempts to manipulate or tamper with the ATM. This has been attempted by a South African bank, but not yet perfected.\textsuperscript{78} Continued testing and piloting of such a device could lead to it being effectively implemented as delaying tactic.

6.3.2.3 ATM alarm, surveillance cameras and systems integration

Some ATMs (i.e. the actual ATM and not the site) do have alarms. The researcher suggests that all ATMs should at least be fitted with alarms. The reason for this emanates from the fact that ATMs that are considered low and medium risk sites were also affected by ATM bombings. In addition, an ATM alarm may deter criminals who commit other types of ATM crimes\textsuperscript{79} (such as ATM skimming) from tampering with the ATMs.

ATM alarms should also not just be there to alert a security guard. It should rather be linked to a central control room where signals will be received. This in turn should be linked to real-time surveillance cameras. In this way, control room operators will be able to see what caused the alarm to be set off and make a decision as to whether it was a false alarm or not.

\textsuperscript{76} Provided by Deter-a-Dye Security
\textsuperscript{77} See chapter 2 for discussion on such attacks. That is, those attacks where attempts are made to access the ATM safe.
\textsuperscript{78} The effectiveness or deterrent value of pepper spray to attackers is still not clear.
\textsuperscript{79} See Chapter 3
Alarm sensors should especially be included at the ATM throat as this is the ATM bombers first point of penetration.

In addition to all ATMs having an alarm, surveillance cameras should be present at ATM sites. This is necessary to identify suspects and their modus operandi. From the analysis of dockets, it was found that a majority of the cases did not have CCTV footage, therefore the majority of the ATMs did not have CCTV cameras installed at the site.

6.3.2.4 TXRTL-60 safes

The researcher is unclear as to the types of safes and the classification used in ATMs due to sensitivity of this information. However, Anderson (1986: 111) identifies the most common safes used in financial institutions. One of the safes listed is TXRTL-60 which according to its description “is a combination-locked safe designed to offer a high degree of protection by common mechanical and electrical tools, cutting torches and high explosives. This safe shall resist entry while attacked for a networking time of 60 minutes”. If the safe can withstand the force of explosives if continuously attacked for 60 minutes and it can be securely bolted down, then this is exactly the type of safe that needs to go into high risk ATMs at least.

6.3.3 Other recommendations

6.3.3.1 Need for more research

Academic institutions, the banking industry and SAPS research should conduct more research on ATM bombings. This should entail detailed interviews with convicted ATM bombers in order to gain information regarding their modus operandi as well as to establish a complete profile on ATM bombers and syndicates.

There is also a need for academic institutions, SAPS and the mining industry to conduct research of mining security. Such research should include an in depth study of security at mines and should include recommendations on the proper securing of explosives and preventative measures to avoid explosives from being stolen from mines and sold on the streets.
6.3.3.2 The need for proper recording and classification of ATM bombings as a crime
Throughout this report, problems emanating from the fact that ATM bombings were recorded as various other crimes, were identified. It was mentioned that offenders of ATM bombings are convicted of various other crimes. It is therefore recommended that ATM bombings are recorded as such and that offenders be charged with an ATM bombing charge amongst the other charges emanating from the crime. This should be done in the same way a cash-in-transit heist, for example, is recorded. This will allow for the proper recording of ATM bombings as a crime and make it easier to identify offenders of the crime. Proper recording will mean accurate statistics. Being able to identify offenders involved in such crimes will allow researchers to interview and compile detailed modus operandi information as well as detailed information on the profile of such offenders.

6.4 CONCLUSION
This research has outlined the extent to which ATM bombings occurred in South Africa. It focused on ATM bombings in Gauteng but the findings illustrate that ATM bombers operate throughout the country and their modus operandi remains basically the same. It also illustrates the state of security measures and the need to upgrade current security measure at ATMs in an attempt to deter future ATM bombers; delay their crimes to make way for effective reaction and to improve security to better trace suspects.

The seriousness of the problem of ATM bombings and its impact on the banking security, their customers and the nation in general, cannot be overlooked. Therefore, the findings of this research should guide the banking industry in exploring a means of improving security at ATMs and understanding the manner in which these crimes are perpetrated.

Hopefully, the research findings from this research project will further stimulate interest in ATM security and ATM bombings in particular that can be used be used in formulating a comprehensive best practices model for securing ATMs in South Africa.

---

80 Especially in chapter 2 and 5.
81 Such as malicious injury to property, theft, and various charges under the explosives act.
BIBLIOGRAPHY/LIST OF REFERENCES

PUBLICATIONS/MONOGRAPHS/JOURNAL ARTICLES


Anon. 27 June 2007. *Happy 40th Birthday to the ATM*. Available at: http://www.absa.co.za/


SparkATM. Nd. *You Security brochure*. Spark ATM Solutions: Cape Town. Available at: [www.sparkatm.co.za](http://www.sparkatm.co.za)


NEWSPAPER ARTICLES


Maravanyika, B. 2007. ATM bombing breakthrough. The Saturday Star. 8 September.
Masombuka, S., Kotlolo, M. & Papayya, M. All out war on bombers. The Sowetan. 8 August.
Mooki, V. 2008. ATM crackdown. City Press. 3 August.
Moselakgomo, A. 2008. ATM bombed but thieves fail to take cash. Sowetan. 6 May.
SAPA. 2007b. Police probe theory explosives from mines used to blast ATMs. Cape Times. 29 August.


LEGISLATION

INTERVIEWS
SAPS 1, Commanding Officer SOCS, Germiston. 2010.
SAPS 2, Commanding Officer SOCS, Germiston. 2010.

SAPS SOCS DOCKETS AND DATA BASES
SAPS Docket No. 29
SAPS Docket No. 11
SAPS Docket No. 67
SAPS Docket No. 71
SAPS Docket no. 52
SAPS Docket no. 12
SAPS Docket no. 67
SAPS Docket no. 45
SAPS Docket no. 13

82Where persons have requested anonymity or confidentiality agreement signed interviews have merely been numbered and listed as per the organisation/company.
ANNEXURE A: PROFORMA SHEETS

1. Docket Analysis

<table>
<thead>
<tr>
<th>CAS NO.</th>
<th>Day</th>
<th>Time</th>
<th>Location</th>
<th>Bank Taken ATM</th>
<th>Cash Taken</th>
<th>No of Men</th>
<th>Armed?</th>
<th>Type of Weapon/s</th>
<th>Deaths/Injuries</th>
<th>Vehicles</th>
<th>More Info</th>
<th>ATM Type</th>
<th>Add Info</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2. Articles related to arrests, convictions and killings (through attempted arrest) of ATM bombers

<table>
<thead>
<tr>
<th>Name</th>
<th>Age</th>
<th>Place of residence</th>
<th>No of cases linked to</th>
<th>Circumstances of arrest</th>
<th>Evidence found</th>
<th>Civilian or law enforcement</th>
<th>Where arrest was made</th>
<th>Other info on suspect</th>
<th>Sentence</th>
<th>Add info</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
3. Articles reporting on a specific ATM bombing incident/s

<table>
<thead>
<tr>
<th>NP/WS&amp;DATE PUB*</th>
<th>DAY</th>
<th>TIME</th>
<th>LOC**</th>
<th>ATM</th>
<th>CASH TAKEN Y/N</th>
<th>MO INFO</th>
<th>WEAPONS NO. OF MEN</th>
<th>I/D***</th>
<th>Add info</th>
</tr>
</thead>
</table>

*newspaper/website and date published

**Location and/or place of site

***injuries/deaths
ANNEXURE B: EXAMPLE OF ATM SECURITY TIPS

ATM security tips and guidelines

The following hints may help you to avoid becoming a victim of ATM crime:

- Only use ATM machines in a well lit, open, high-traffic area.
- Avoid bank ATM machines adjacent to obvious hiding places.
- When you approach an ATM, scan the area first for loiterers.
- Have your card ready and leave quickly, not counting your cash in public.
- Walk, run, or drive away immediately if your instincts tell you so.
- Beware of offers for help from strangers or security guards during an ATM transaction. Press ‘cancel’ immediately, ensure the returned card is yours and leave the ATM immediately.
- Tell any suspicious person in a loud, firm voice to back-off.
- Don’t argue with a robber; if confronted, give up the cash.
- Don’t fight with or attempt to follow the robber.
- Drive or walk to a safe place and immediately call the police.
- Do not allow yourself to be distracted.
- Stay alert. Be aware of your surroundings and don’t allow yourself to be crowded at an ATM. When waiting in line, stand well behind the person using the ATM and ensure that the person queuing behind you keeps a reasonable distance from you.
- Avoid drawing cash when you are alone, especially at night or at isolated ATMs.
- Key in your personal identification number (PIN) only when prompted to do so by the screen and not when requested to do so by a stranger. Do not key in your PIN if the card appears to be stuck.
- Stand close to the ATM and shield the keypad with your body when keying in your PIN to ensure that nobody can see what your PIN is.
- Do not write your PIN on your ATM card, or on a piece of paper that you keep in your wallet or purse, as this is the first place a thief will look.
- Ensure that your PIN is not revealed to anyone. This includes bank staff, friends or family members.
- If the ATMs in a certain area are not working, it is best not to go to the nearest available ATM in the same area, especially if you detect suspicious circumstances. Sabotage of an ATM is often used to lead potential victims to a specific ATM.
- Check that the card in your possession is yours before and after a transaction.
- Avoid drawing large sums of money. Reduce your daily or monthly withdrawal limit at your bank.
- Report a stolen card immediately.
- When your transaction is complete, take your money, card and receipt immediately and put them in your pocket or purse without delay. Count your money at a later stage when it is safe to do so.
- If your card is lost or stolen or is retained at an ATM, report it immediately to your bank or via the toll-free numbers displayed on the ATM. Criminals typically transact with a card within 40 to 50 seconds after it has been stolen. Prevention is the best policy.
- Be wary of ‘helpful’ strangers who offer you mobile phone assistance to cancel your card. If you accept the help, check that the number they dial is the same as the toll free number displayed on the ATM. Report all incidents of ATM crime to the bank and the police.
- Retain transaction slips and check them against your statement. Query unauthorised debits as soon as possible. The relevant contact numbers are on your statement.

Trust your instincts. If you feel uncomfortable or if you are suspicious when drawing cash from an ATM, act on your instincts. You can always draw money later when you feel it is safe to do so.

REPORT ATM FRAUD 0800 212 767
ANNEXURE C: NUMBER OF REPORTED INCIDENTS PER POLICE STATION IN GAUTENG

<table>
<thead>
<tr>
<th>POLICE STATION</th>
<th>NUMBER OF INCIDENTS RECORDED AT STATION BETWEEN JANUARY 2006 AND JULY 2009</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actonville</td>
<td>2</td>
</tr>
<tr>
<td>Akasia</td>
<td>8</td>
</tr>
<tr>
<td>Alberton</td>
<td>4</td>
</tr>
<tr>
<td>Alexandra</td>
<td>4</td>
</tr>
<tr>
<td>Atteridgeville</td>
<td>18</td>
</tr>
<tr>
<td>Bedfordview</td>
<td>2</td>
</tr>
<tr>
<td>Benoni</td>
<td>3</td>
</tr>
<tr>
<td>Boipatong</td>
<td>1</td>
</tr>
<tr>
<td>Boksburg</td>
<td>2</td>
</tr>
<tr>
<td>Boksburg North</td>
<td>4</td>
</tr>
<tr>
<td>Boysens</td>
<td>5</td>
</tr>
<tr>
<td>Brackendowns</td>
<td>5</td>
</tr>
<tr>
<td>Brakpan</td>
<td>12</td>
</tr>
<tr>
<td>Bramley</td>
<td>2</td>
</tr>
<tr>
<td>Brixton</td>
<td>1</td>
</tr>
<tr>
<td>Bronkhorstpruit</td>
<td>1</td>
</tr>
<tr>
<td>Carletonville</td>
<td>6</td>
</tr>
<tr>
<td>Cleveland</td>
<td>3</td>
</tr>
<tr>
<td>Crystal Park</td>
<td>1</td>
</tr>
<tr>
<td>Cullinan</td>
<td>3</td>
</tr>
<tr>
<td>Daveyton</td>
<td>7</td>
</tr>
<tr>
<td>De Deur</td>
<td>5</td>
</tr>
<tr>
<td>Diepkloof</td>
<td>7</td>
</tr>
<tr>
<td>Dobsonville</td>
<td>11</td>
</tr>
<tr>
<td>Douglasdale</td>
<td>5</td>
</tr>
<tr>
<td>Place</td>
<td>Count</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>Duduza</td>
<td>3</td>
</tr>
<tr>
<td>Dunnottar</td>
<td>1</td>
</tr>
<tr>
<td>Edenpark</td>
<td>3</td>
</tr>
<tr>
<td>Eersterust</td>
<td>2</td>
</tr>
<tr>
<td>Eldorado Park</td>
<td>12</td>
</tr>
<tr>
<td>Elsburg</td>
<td>6</td>
</tr>
<tr>
<td>Ennerdale</td>
<td>6</td>
</tr>
<tr>
<td>Erasmia</td>
<td>7</td>
</tr>
<tr>
<td>Etwatwa</td>
<td>7</td>
</tr>
<tr>
<td>Evaton</td>
<td>4</td>
</tr>
<tr>
<td>Fairlands</td>
<td>1</td>
</tr>
<tr>
<td>Florida</td>
<td>8</td>
</tr>
<tr>
<td>Germiston</td>
<td>5</td>
</tr>
<tr>
<td>Hammanskraal</td>
<td>1</td>
</tr>
<tr>
<td>Heidelberg Gauteng</td>
<td>3</td>
</tr>
<tr>
<td>Hekpoort</td>
<td>1</td>
</tr>
<tr>
<td>Hercules</td>
<td>7</td>
</tr>
<tr>
<td>Honeydew</td>
<td>7</td>
</tr>
<tr>
<td>Ivory Park</td>
<td>7</td>
</tr>
<tr>
<td>Jabulani</td>
<td>10</td>
</tr>
<tr>
<td>Jeppe</td>
<td>6</td>
</tr>
<tr>
<td>Johannesburg Central</td>
<td>3</td>
</tr>
<tr>
<td>Kagiso</td>
<td>15</td>
</tr>
<tr>
<td>Katlehong</td>
<td>13</td>
</tr>
<tr>
<td>Kempton Park</td>
<td>3</td>
</tr>
<tr>
<td>Kliprivier</td>
<td>1</td>
</tr>
<tr>
<td>Kliptown</td>
<td>6</td>
</tr>
<tr>
<td>Krugersdorp</td>
<td>9</td>
</tr>
<tr>
<td>Kwa-Thema</td>
<td>5</td>
</tr>
<tr>
<td>Town</td>
<td>Count</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------</td>
</tr>
<tr>
<td>Langlaagte</td>
<td>2</td>
</tr>
<tr>
<td>Lenasia</td>
<td>6</td>
</tr>
<tr>
<td>Lenasia South</td>
<td>4</td>
</tr>
<tr>
<td>Lyttelton</td>
<td>3</td>
</tr>
<tr>
<td>Magaliesburg</td>
<td>1</td>
</tr>
<tr>
<td>Mamelodi</td>
<td>8</td>
</tr>
<tr>
<td>Mamelodi East</td>
<td>3</td>
</tr>
<tr>
<td>Meadowlands</td>
<td>4</td>
</tr>
<tr>
<td>Meyerton</td>
<td>2</td>
</tr>
<tr>
<td>Midrand</td>
<td>2</td>
</tr>
<tr>
<td>Mondeor</td>
<td>13</td>
</tr>
<tr>
<td>Moroka</td>
<td>13</td>
</tr>
<tr>
<td>Muldersdrif</td>
<td>2</td>
</tr>
<tr>
<td>Naledi</td>
<td>8</td>
</tr>
<tr>
<td>Olifantsfontein</td>
<td>2</td>
</tr>
<tr>
<td>Orange Farms</td>
<td>8</td>
</tr>
<tr>
<td>Orlando</td>
<td>7</td>
</tr>
<tr>
<td>Pretoria central</td>
<td>1</td>
</tr>
<tr>
<td>Pretoria West</td>
<td>8</td>
</tr>
<tr>
<td>Protea Glen</td>
<td>2</td>
</tr>
<tr>
<td>Rabie Ridge</td>
<td>7</td>
</tr>
<tr>
<td>Randburg</td>
<td>2</td>
</tr>
<tr>
<td>Randfontein</td>
<td>10</td>
</tr>
<tr>
<td>Rietgat</td>
<td>3</td>
</tr>
<tr>
<td>Roodepoort</td>
<td>12</td>
</tr>
<tr>
<td>Sandringham</td>
<td>1</td>
</tr>
<tr>
<td>Sebenza</td>
<td>1</td>
</tr>
<tr>
<td>Sebokeng</td>
<td>3</td>
</tr>
<tr>
<td>Sharpeville</td>
<td>2</td>
</tr>
<tr>
<td>Location</td>
<td>Count</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------</td>
</tr>
<tr>
<td>Silverton</td>
<td>1</td>
</tr>
<tr>
<td>Sinoville</td>
<td>3</td>
</tr>
<tr>
<td>Sophia Town</td>
<td>6</td>
</tr>
<tr>
<td>Soshanguve</td>
<td>15</td>
</tr>
<tr>
<td>Springs</td>
<td>17</td>
</tr>
<tr>
<td>Temba</td>
<td>9</td>
</tr>
<tr>
<td>Tembisa</td>
<td>16</td>
</tr>
<tr>
<td>Tokoza</td>
<td>7</td>
</tr>
<tr>
<td>Tsakane</td>
<td>7</td>
</tr>
<tr>
<td>Vanderbijlpark</td>
<td>3</td>
</tr>
<tr>
<td>Vereeniging</td>
<td>4</td>
</tr>
<tr>
<td>Villieria</td>
<td>1</td>
</tr>
<tr>
<td>Vosloorus</td>
<td>4</td>
</tr>
<tr>
<td>Welbekend</td>
<td>2</td>
</tr>
<tr>
<td>Westonaria</td>
<td>3</td>
</tr>
<tr>
<td>Wierdabrug</td>
<td>4</td>
</tr>
<tr>
<td>Zonkezizwe</td>
<td>1</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>527</strong></td>
</tr>
</tbody>
</table>
ANNEXURE D: TABLE INDICATED STATIONS WITH MOST NUMBER OF REPORTED CASES (IN DESCENDING ORDER)

<table>
<thead>
<tr>
<th>POLICE STATION</th>
<th>PART OF GAUTENG</th>
<th>NUMBER OF INCIDENTS RECORDED AT STATION BETWEEN JANUARY 2006 AND JULY 2009</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Atteridgeville</td>
<td>Pretoria</td>
<td>18</td>
</tr>
<tr>
<td>2. Springs</td>
<td>East Rand</td>
<td>17</td>
</tr>
<tr>
<td>3. Tembisa</td>
<td>East Rand</td>
<td>16</td>
</tr>
<tr>
<td>4. Kagiso</td>
<td>West Rand</td>
<td>15</td>
</tr>
<tr>
<td>5. Soshanguve</td>
<td>Pretoria</td>
<td>15</td>
</tr>
<tr>
<td>6. Mondeor</td>
<td>Johannesburg, Soweto</td>
<td>13</td>
</tr>
<tr>
<td>7. Moroka</td>
<td>Johannesburg, Soweto</td>
<td>13</td>
</tr>
<tr>
<td>8. Katlehong</td>
<td>East Rand</td>
<td>13</td>
</tr>
<tr>
<td>9. Roodepoort</td>
<td>West Rand</td>
<td>12</td>
</tr>
<tr>
<td>10. Eldorado Park</td>
<td>Vaal</td>
<td>12</td>
</tr>
<tr>
<td>11. Brakpan</td>
<td>East Rand</td>
<td>12</td>
</tr>
<tr>
<td>12. Dobsonville</td>
<td>Johannesburg, Soweto</td>
<td>11</td>
</tr>
<tr>
<td>13. Randfontein</td>
<td>West Rand</td>
<td>10</td>
</tr>
<tr>
<td>14. Jabulani</td>
<td>Johannesburg, Soweto</td>
<td>10</td>
</tr>
<tr>
<td>15. Krugersdorp</td>
<td>West Rand</td>
<td>9</td>
</tr>
<tr>
<td>16. Temba</td>
<td>Pretoria</td>
<td>9</td>
</tr>
<tr>
<td>17. Florida</td>
<td>West Rand</td>
<td>8</td>
</tr>
<tr>
<td>18. Orange Farms</td>
<td>Vaal</td>
<td>8</td>
</tr>
<tr>
<td>19. Akasia</td>
<td>Pretoria</td>
<td>8</td>
</tr>
<tr>
<td>20. Mamelodi</td>
<td>Pretoria</td>
<td>8</td>
</tr>
<tr>
<td>21. Pretoria West</td>
<td>Pretoria</td>
<td>8</td>
</tr>
<tr>
<td>22. Naledi</td>
<td>Johannesburg, Soweto</td>
<td>8</td>
</tr>
<tr>
<td>23. Honeydew</td>
<td>West Rand</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>Area Name</td>
<td>Location</td>
</tr>
<tr>
<td>---</td>
<td>----------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>24.</td>
<td>Erasmia</td>
<td>Pretoria</td>
</tr>
<tr>
<td>25.</td>
<td>Hercules</td>
<td>Pretoria</td>
</tr>
<tr>
<td>26.</td>
<td>Diepkloof</td>
<td>Johannesburg, Soweto</td>
</tr>
<tr>
<td>27.</td>
<td>Orlando</td>
<td>Johannesburg, Soweto</td>
</tr>
<tr>
<td>28.</td>
<td>Ivory Park</td>
<td>Johannesburg, Midrand</td>
</tr>
<tr>
<td>29.</td>
<td>Daveyton</td>
<td>East Rand</td>
</tr>
<tr>
<td>30.</td>
<td>Etwatwa</td>
<td>East Rand</td>
</tr>
<tr>
<td>31.</td>
<td>Rabie Ridge</td>
<td>East Rand</td>
</tr>
<tr>
<td>32.</td>
<td>Tokoza</td>
<td>East Rand</td>
</tr>
<tr>
<td>33.</td>
<td>Tsakane</td>
<td>East Rand</td>
</tr>
<tr>
<td>34.</td>
<td>Carletonville</td>
<td>West Rand</td>
</tr>
<tr>
<td>35.</td>
<td>Ennerdale</td>
<td>Vaal</td>
</tr>
<tr>
<td>36.</td>
<td>Kliptown</td>
<td>Johannesburg, Soweto</td>
</tr>
<tr>
<td>37.</td>
<td>Sophia Town</td>
<td>Johannesburg West</td>
</tr>
<tr>
<td>38.</td>
<td>Lenasia</td>
<td>Johannesburg South</td>
</tr>
<tr>
<td>39.</td>
<td>Jeppe</td>
<td>Johannesburg Central</td>
</tr>
<tr>
<td>40.</td>
<td>Elsburg</td>
<td>East Rand</td>
</tr>
<tr>
<td>41.</td>
<td>De Deur</td>
<td>Vaal</td>
</tr>
<tr>
<td>42.</td>
<td>Douglasdale</td>
<td>Johannesburg North</td>
</tr>
<tr>
<td>43.</td>
<td>Booyens</td>
<td>Johannesburg Central</td>
</tr>
<tr>
<td>44.</td>
<td>Germiston</td>
<td>East Rand</td>
</tr>
<tr>
<td>45.</td>
<td>Brackendowns</td>
<td>East Rand</td>
</tr>
<tr>
<td>46.</td>
<td>Kwa-Thema</td>
<td>East Rand</td>
</tr>
<tr>
<td>47.</td>
<td>Evaton</td>
<td>Vaal</td>
</tr>
<tr>
<td>48.</td>
<td>Lenasia South</td>
<td>Vaal</td>
</tr>
<tr>
<td>49.</td>
<td>Vereeniging</td>
<td>Vaal</td>
</tr>
<tr>
<td>50.</td>
<td>Wierdabrug</td>
<td>Pretoria</td>
</tr>
<tr>
<td>51.</td>
<td>Meadowlands</td>
<td>Johannesburg, Soweto</td>
</tr>
<tr>
<td>52.</td>
<td>Alexandra</td>
<td>Johannesburg North</td>
</tr>
<tr>
<td></td>
<td>City</td>
<td>Area</td>
</tr>
<tr>
<td>---</td>
<td>---------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>53.</td>
<td>Alberton</td>
<td>East Rand</td>
</tr>
<tr>
<td>54.</td>
<td>Boksburg North</td>
<td>East Rand</td>
</tr>
<tr>
<td>55.</td>
<td>Vosloorus</td>
<td>East Rand</td>
</tr>
<tr>
<td>56.</td>
<td>Westonaria</td>
<td>West Rand</td>
</tr>
<tr>
<td>57.</td>
<td>Heidelberg</td>
<td>Vaal</td>
</tr>
<tr>
<td>58.</td>
<td>Sebokeng</td>
<td>Vaal</td>
</tr>
<tr>
<td>59.</td>
<td>Vanderbijlpark</td>
<td>Vaal</td>
</tr>
<tr>
<td>60.</td>
<td>Cullinan</td>
<td>Pretoria</td>
</tr>
<tr>
<td>61.</td>
<td>Lyttelton</td>
<td>Pretoria</td>
</tr>
<tr>
<td>62.</td>
<td>Mamelodi East</td>
<td>Pretoria</td>
</tr>
<tr>
<td>63.</td>
<td>Rietgat</td>
<td>Pretoria</td>
</tr>
<tr>
<td>64.</td>
<td>Sinoville</td>
<td>Pretoria</td>
</tr>
<tr>
<td>65.</td>
<td>Johannesburg Central</td>
<td>Johannesburg</td>
</tr>
<tr>
<td>66.</td>
<td>Cleveland</td>
<td>Johannesburg</td>
</tr>
<tr>
<td>67.</td>
<td>Benoni</td>
<td>East Rand</td>
</tr>
<tr>
<td>68.</td>
<td>Kempton Park</td>
<td>East Rand</td>
</tr>
<tr>
<td>69.</td>
<td>Duduza</td>
<td>East Rand</td>
</tr>
<tr>
<td>70.</td>
<td>Edenpark</td>
<td>East Rand</td>
</tr>
<tr>
<td>71.</td>
<td>Muldersdrif</td>
<td>West Rand</td>
</tr>
<tr>
<td>72.</td>
<td>Meyerton</td>
<td>Vaal</td>
</tr>
<tr>
<td>73.</td>
<td>Sharpeville</td>
<td>Vaal</td>
</tr>
<tr>
<td>74.</td>
<td>Eersterust</td>
<td>Pretoria</td>
</tr>
<tr>
<td>75.</td>
<td>Welbekend</td>
<td>Pretoria</td>
</tr>
<tr>
<td>76.</td>
<td>Protea Glen</td>
<td>Johannesburg, Soweto</td>
</tr>
<tr>
<td>77.</td>
<td>Olifantsfontein</td>
<td>Johannesburg, Midrand</td>
</tr>
<tr>
<td>78.</td>
<td>Randburg</td>
<td>Johannesburg North</td>
</tr>
<tr>
<td>79.</td>
<td>Langlaagte</td>
<td>Johannesburg</td>
</tr>
<tr>
<td>80.</td>
<td>Midrand</td>
<td>Johannesburg</td>
</tr>
<tr>
<td>81.</td>
<td>Bramley</td>
<td>Johannesburg</td>
</tr>
<tr>
<td></td>
<td>Location</td>
<td>Area</td>
</tr>
<tr>
<td>---</td>
<td>------------------</td>
<td>------------</td>
</tr>
<tr>
<td>82.</td>
<td>Actonville</td>
<td>East Rand</td>
</tr>
<tr>
<td>83.</td>
<td>Boksburg</td>
<td>East Rand</td>
</tr>
<tr>
<td>84.</td>
<td>Bedfordview</td>
<td>East Rand</td>
</tr>
<tr>
<td>85.</td>
<td>Fairlands</td>
<td>West Rand</td>
</tr>
<tr>
<td>86.</td>
<td>Magaliesburg</td>
<td>West Rand</td>
</tr>
<tr>
<td>87.</td>
<td>Hekpoort</td>
<td>West Rand</td>
</tr>
<tr>
<td>88.</td>
<td>Boipatong</td>
<td>Vaal</td>
</tr>
<tr>
<td>89.</td>
<td>Kliprivier</td>
<td>Vaal</td>
</tr>
<tr>
<td>90.</td>
<td>Bronkhorstpruit</td>
<td>Pretoria</td>
</tr>
<tr>
<td>91.</td>
<td>Pretoria central</td>
<td>Pretoria</td>
</tr>
<tr>
<td>92.</td>
<td>Silverton</td>
<td>Pretoria</td>
</tr>
<tr>
<td>93.</td>
<td>Villieria</td>
<td>Pretoria</td>
</tr>
<tr>
<td>94.</td>
<td>Hammanskraal</td>
<td>Pretoria</td>
</tr>
<tr>
<td>95.</td>
<td>Brixton</td>
<td>Johannesburg West</td>
</tr>
<tr>
<td>96.</td>
<td>Sandringham</td>
<td>Johannesburg</td>
</tr>
<tr>
<td>97.</td>
<td>Dunnottar</td>
<td>East Rand</td>
</tr>
<tr>
<td>98.</td>
<td>Zonkezizwe</td>
<td>East Rand</td>
</tr>
<tr>
<td>99.</td>
<td>Crystal Park</td>
<td>East Rand</td>
</tr>
<tr>
<td>100.</td>
<td>Sebenza</td>
<td>East Rand</td>
</tr>
<tr>
<td></td>
<td><strong>Total number of incidents reported</strong></td>
<td></td>
</tr>
</tbody>
</table>
ANNEXURE D: IMAGES – DAMAGE CAUSED BY ATM BOMBINGS
ANNEXURE E: MAPS

1. GAUTENG
2. GREATER JOHANNESBURG
3. WEST RAND
4. EAST RAND
5. PRETORIA
6. VAAL RAND (SOUTHERN GAUTENG)
RE: ACCESS TO INCIDENT REPORTS ON ATM BOMBINGS FOR RESEARCH PURPOSES: DR ANTHONY MINNAAR (SUPERVISOR) AND MS SARIKA SEWPERSAD (STUDENT)

1. This office has received a research proposal from Ms Sarika Sewpersad titled: "An investigation of the bombing of ATM's with intent to steal cash contents: Case study from Gauteng."

2. The aim of the research is to determine the nature and extent of theft of cash contents by means of bombing Automated Teller Machines (ATM's) in Gauteng and to evaluate the security measures that exist at ATM's.

3. This office has perused the proposal and it will be recommended to the Provincial Commissioner of Gauteng, for final permission.

4. At this stage the researcher needs information from SABRIC on Gauteng ATM bombing incidents (date, location and file number) in order to be able to identify the police stations where the (closed) dockets are kept. This information will enable the researcher to supply the SAPS with a list of names of docket numbers and police stations.

5. This office kindly request that the information is made available to Prof Anthony Minnaar of Unisa, who is the supervisor for the researcher.

Kind regards

[Signature]

ASST COMMISSIONER
HEAD: STRATEGIC MANAGEMENT
GE MOORCROFT
ANNEXURE G: LIST OF QUESTIONS USED DURING INTERVIEWS

1. What is your job title?
2. From your experience as a (job title…), what is the typical method of operation used by ATM bombing syndicates?
3. How many men usually make up the gang?
4. Which areas in Gauteng are most affected?
5. Which bank do you think is most affected?
6. What is the role of weaponry in the crime and do all gangs use deadly weapons or just a few?
7. What are the most common weapons used?
8. Where do they get their weapons from?
9. Will you consider the gangs dangerous?
10. Do you think that media reports of SAPS members being part of ATM bombing syndicates are true?
11. Do all gangs make use of vehicles to escape?
12. Do they use their own vehicles, or are they perhaps stolen or hijacked vehicles?
13. Why is it that the registration number of the vehicle is never known or does not lead to a suspect?
14. Where do you think ATM gangs get their explosives from? Do you suspect corrupt mine workers?
15. Do you have any idea as to how the explosives are inserted into the ATM?
16. Do all ATMs have alarms and are they linked to a central command centre or are they just there to be heard by a security guard on duty?
17. How do the gangs know when there is a lot of cash in the ATM?
18. Do you know of any cash-in-transit personnel who may have been working with ATM bombers?
19. Do the gangs consist only of South African males or are they a mixture of South Africans and foreigners?
20. What is your main source of evidence during investigations?

Questions were put forward on the basis of what was said by the interviewee. This is just a list of question used by the researcher to ensure that all aspects were covered.