Best Practices *for* Preventing ATM Gas and Explosive Attacks

International minimum security guidelines and best practices

Produced by the ATM Industry Association

Contributors Include:

Should you wish to join ATMIA's ATM Software Portal on www.atmia.com,
e-mail Mike Lee, ATMIA's CEO, at mike@atmia.com

Disclaimer

The ATM Industry Association (ATMIA) publishes this best practice manual in furtherance of its non-profit and tax-exempt purposes to enhance protection against gas and explosive attacks. ATMIA has taken reasonable measures to provide objective information and recommendations to the industry but cannot guarantee the accuracy, completeness, efficacy, timeliness or other aspects of this publication. ATMIA cannot ensure compliance with the laws or regulations of any country and does not represent that the information in this publication is consistent with any particular principles, standards, or guidance of any country or entity. There is no effort or intention to create standards for any business activities. These best practices are intended to be read as recommendations only and the responsibility rests with those wishing to implement them to ensure they do so after their own independent relevant risk assessments and in accordance with their own regulatory frameworks. Further, neither ATMIA nor its officers, directors, members, employees or agents shall be liable for any loss, damage or claim with respect to any activity or practice arising from any reading of this manual; all such liabilities, including direct, special, indirect or inconsequential damages, are expressly disclaimed. Information provided in this publication is "as is" without warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, or freedom from infringement. The name and marks ATM Industry Association, ATMIA and related trademarks are the property of ATMIA.

Please note this manual contains security best practices and should not be left lying around or freely copied without due care for its distribution and safekeeping.

Global Sponsors - 2014

Table of Contents

Foreword

In part, due to the success of implementing effective anti-ram raid and anti-cutting defences on ATMs, those who continue to attempt to physically attack ATMs are using more violent methods to access the cash inside. The use of explosives, both combustible gas and solid explosives, is a worrying trend which ATM deployers need to understand and address.

The ATMIA believes the information in this document will help to highlight potential areas where the ATM channel might become an area of focus of explosive attacks and assist ATMIA members in proactively adopting best practices at the ATM and premises level.

This document sets out international minimum security guidelines and best practices for preventing ATM gas and explosive attacks.

To combat crime, it is imperative that all ATM deployers in all regions and countries take best practices very seriously and implement all guidelines and best practices contained herein to the greatest extent possible.

ATMIA

March 2014

Executive Summary

Please note that this Executive Summary cannot replace reading the whole manual. The summary is merely a guide as to the content and main principles for the prevention of ATM gas and explosive attacks.

Explosive attacks against ATMs are of growing concern globally and are particularly prevalent in Europe.

Current explosive attacks in Europe predominately involve gas, although in some countries, there has been a proportional increase in the number of attempts using solid explosives.

A fundamental difference between a traditional safe and the security enclosures used in ATMs is that there are, by necessity, holes manufactured into the "box."

Holes in the security enclosure can be exploited to introduce explosives.

Prior to an explosive attack, there are often identifiable precursors and evidence that an attack is about to occur.

Building and perimeter security are often breached to gain access to the cash.

It is unlikely that one single solution or initiative will, in itself, significantly reduce the risks associated with explosive attacks targeting ATMs. It is important to adopt a layered approach to make the target less appealing.

Understanding how other organizations have successfully addressed explosive attacks is extremely valuable in designing a strategic and tactical response to reduce the risks from explosive attacks.

Pre-defined processes, procedures and checklists can significantly improve the effective management and response to explosive attacks.

ATMIA members concerned about ATM gas and explosive attacks are advised to implement all guidelines and best practices contained herein to the greatest extent possible.

Acknowledgements

ATMIA is indebted to the individual contribution of the following experts:

Technical Editor:	Douglas Russell, DFR Risk Management Ltd
Contributor:	Janine Randolph, British Bankers Association
Contributor:	Falko Adomat, ECB European Certification Body
Contributor:	Mauro Iannucci, BNL, Italy
Contributor:	PierLuigi Martusciello, BNL, Italy
Contributor:	Patrice Rullier, Oberthur Cash Protection, France
Contributor:	Eduardo Miguel Pereira, SIBS, Portugal
Contributor:	Martijn Docters van Leeuwen, Rabobank, NL
Contributor:	Jan van Oord, Rabobank, NL
Contributor:	Vagner Luis Valim Carlos, TecBan, Brazil
Contributor:	Kevin Botha, Standard Bank, South Africa

ATMIA is further indebted to the combined contribution of the European Gas & Explosive ATM Attacks Steering Committee:

Adrian Marshall, HSBC

Andrew Gwyther, Avon & Somerset Police

Douglas Russell, DFR Risk Management

Eduardo Pereira, SIBS Multibanco

Flora Hamilton, ATMIA Europe

Garth Graham, Danske Bank

Graham Mott, LINK

Jan van Oord, Rabobank

Janine Randolph, BBA

Mark Rolfe, Avon & Somerset Police

Martijn Docters, Rabobank

Mauro Iannucci, BNL

Patrice Rullier, Oberthur Cash Protection

Pete Lamb, Cashzone

PierLuigi Martusciello, BNL

Valentim Oliveira, SIBS Multibanco

Chapter 1. Definition and Background of Explosive Attacks

Explosives have been used to gain access to cash held in safes and security enclosures for almost as long as they have existed. While different techniques have been used, the most common attacks have involved attaching solid explosives, such as dynamite, to the external side of the safe door. An explosive charge detonated externally is less effective than if the detonation occurs within the safe. Because traditional safes normally have no openings while the door is closed, perpetrators had to either attach their explosives externally, or cut or drill a hole in the safe to allow the charge to be inserted into the safe.

A fundamental difference between a traditional safe and the security enclosures used in ATMs is that there are, by necessity, holes manufactured into the "box." The holes permit the movement of cash between the ATM and the consumer and allow cables that provide power and control the modules within the ATM security enclosure.

ATM explosive attacks, whether using non-gas (solid explosives) or combustible gas, exploit the existing holes to enable the explosive charge to be inserted and detonated within the enclosure. On detonation the explosive pressure puts enormous strain on all sides of the enclosure, including the door. If the attack is successful, the weakest side will detach, allowing access to the cash from within the ATM.

Solid explosives used in ATM attacks include dynamite, gelignite, plastic (putty) such as C4 and emulsion explosives, such as power gel. The mining and demolition industries are sources for many of these explosives. There are currently proportionally more ATM attacks in countries with a well established mining industry, such as South Africa. Explosives stolen from military organizations have also been used to attack ATMs, including a hand grenade used recently in a failed attack in Europe. Explosives such as ETN and PETN are also used in some European countries.

Sourcing solid explosive devices and the required detonators is generally more difficult than sourcing explosive gas. ATM gas attacks have occurred in many regions of the world since 2005. In 2008 there were a string of attacks in Australia using explosive gas which prompted a robust police and industry response. In Europe, explosive gas attacks, believed to have originated in Italy, have now spread to numerous European countries including the UK.

Most explosive gas attacks use hydro-carbon gas mixes, the most common being Oxyacetylene. Commonly used in welding and cutting equipment, explosive gas is easy to source and insert within the ATM. It can be detonated in a number of ways. Many consumer gas products, such as gas cookers, use piezoelectric igniters that generate a flame or spark that will detonate the gas.

Although current explosive attacks in Europe predominately involve gas, in some countries there has been a proportional increase in the number of attempts using solid explosives. For example, explosive attacks in Italy, which were predominately gas, at the time of this writing involve a mix of 30% gas to 70% solid explosives such as C4 (plastic explosive).

Chapter 2. Methods Used to Introduce Explosives into ATMs

ATM security enclosures are not constructed to be air tight like many other types of safes and vaults. The security enclosure of an ATM contains various modules such as the cash dispenser and depository modules. These modules must have a delivery or transport mechanism which projects through the security enclosure towards the consumer interface side of the ATM. Cables are often positioned external to the security enclosure and run through the security enclosure to power and control the modules.

Holes in the security enclosure can be exploited to introduce explosives.

Through the Wall (TTW) ATMs are normally rear-access ATMs where the door to the security enclosure is on the opposite side of the wall from the consumer facing side. Because cabling holes exist behind the wall, TTW ATMs are not easily accessible from the exterior, consumer facing side.

The most common way for explosives to be introduced into the security enclosure of a TTW ATM is via the dispenser or depository interfaces. This is generally done by one of the following methods:

- Performing a transaction to open the shutters;
- Smashing or bending the shutters using a tool, such as a crowbar;
- Cutting or drilling a hole in the shutters to introduce the explosives; or,
- Cutting or drilling a hole in the fascia beside the shutters to gain access to the gap between the dispenser or depository module and the hole in the security enclosure.

Explosive gas canisters connected to tubes or pipes with fairly small diameter deliver the gas mixture, most commonly to the security enclosure. The perpetrator often cuts or drills the shutter or fascia to allow insertion of the pipe and detonator. The attacker can also insert the pipes and detonators after smashing or bending the shutter, or after opening the shutters by performing a card transaction.

Solid explosives are generally larger in size than the tubes or pipes used to introduce explosive gas; therefore, it is more common for the attacker to insert the solid explosive charge and detonator by smashing the shutters or by opening the shutters by performing a transaction. A flat box containing the explosive (such as C4 plastic explosive) is often used.

Attackers often target standalone pod-style ATMs in a similar way to TTW ATMs.

If the perpetrator can gain undetected access to the rear of a TTW ATM or to a standalone lobby ATM, he has more opportunity to exploit the cabling holes to enter the security enclosure.

Most, although not all, cabling holes are too small to permit a sufficient quantity of most types of solid explosive along with a detonator, but they can be large enough to permit the insertion of pipes and detonator cables used in explosive gas attacks. The benefit in exploiting cable holes is that the perpetrator can avoid physical damage to the ATM that might activate alarms or other defences prior to detonating the explosives.

Whether the attack targets the front or the rear of the ATM, it can take only one minute to insert enough gas or place a solid explosive charge into the security enclosure. Detonation and subsequent theft of the cash can be completed within four minutes by expert perpetrators.

Chapter 3. Overcoming Building and Perimeter Security

As important as it is for perpetrators to be able to introduce the explosives into the ATM security enclosure, they must also be able to access the cash following a successful detonation.

Attacks to TTW ATMs, particularly using solid explosives, can create enough damage that the attacker can access some of the cash from the exterior or front of the ATM. However, access is usually limited to the cash in the retract/reject bin and the top cassette. To maximize their financial return, perpetrators must gain access to the interior room. If the attack is successful, the security enclosure door will be dislocated and the perpetrators will have access to more cash within the ATM.

In some countries there has been an increase in TTW ATM installations where the ATM is mounted on a glass wall. These types of locations are especially vulnerable to explosive attacks because the glass wall usually breaks during the explosion resulting in easy retrieval of the cash.

Premises with effective alarms are often accessed immediately after or simultaneously with the detonation. Premises without alarms or with alarms that can be easily sabotaged are often accessed prior to the detonation of the explosive, minimizing the time required to collect the cash and make a getaway.

Buildings with regular public access such as retail stores and bank branches allow perpetrators to perform close surveillance of the targeted environment and take advantage of opportunities to disable or redirect the angle of motion detectors and CCTV cameras prior to returning to attack the ATM.

Perpetrators can deliberately trigger alarms without leaving easily observable evidence. Multiple alarm activations can lead to the alarm system being disabled or any further responses being abandoned.

Premises with physically weak doors or doors with low security graded locks allow attackers easy penetration via a variety of easily obtained cutting and hand tools such as sledge hammers and crowbars. Buildings with higher physical security are more commonly ram-raided with a vehicle to gain access. The vehicle used to ram the building is often different from the vehicle used to make the getaway.

Premises with anti-ram raid protection such as security bollards or other heavy street furniture present the perpetrators with another security layer to overcome. However, perpetrators often use a battering ram such as a long pole or heavy beam attached to the vehicle to gain access to the premises without the need to physically breach the anti-ram raid protection.

Expert perpetrators can overcome perimeter security, detonate the explosives and take the cash within an elapsed time of four minutes.

Chapter 4. Precursors and Evidence Explosive Attacks May Be Planned or Attempted

Prior to carrying out an explosive attack against an ATM it is common for the perpetrators to carry out surveillance of the ATM and premises housing the ATM. While the number of perpetrators varies, and in some attacks a team of 10 individuals has been involved, the most common number of attackers is two to three persons, normally male.

The perpetrators often steal or hire a high performance getaway vehicle, such as an Audi A6 or BMW. In more central city locations, perpetrators have stolen motor cycles and scooters and used them as getaway vehicles.

Locations with a higher level of physical perimeter security often require the use of an additional vehicle to ram the building. Perpetrators often steal 4x4 vehicles and construction equipment prior to the attack.

Without assistance from an insider, sourcing physical explosives can involve burglary and theft from facilities that store explosives.

Perpetrators may purchase, hire, or steal explosive gas from suppliers of welding and cutting equipment. Specifically, motor vehicle repair shops have been burgled for the purpose of obtaining gas canisters and pipes.

Normally, the attackers will bring the needed equipment to the location at the time of the attack; however, there have been reports of explosive gas canisters being located and concealed close to the premises prior to the actual attack taking place.

Attacks that are abandoned either due to the perpetrators being disturbed or the explosives failing to detonate correctly can leave physical evidence. Examples include damaged, cut, or drilled dispenser or depository shutters and fascia damage. Partial explosions often leave burn or scorch marks on the ATM. There can also be evidence that the premises housing the ATM were attacked including partially damaged doors or locks.

Perpetrators planning to attack an ATM shortly after its having been filled with cash have been known to put surveillance on the Cash in Transit (CIT) teams or the ATM itself. Once filled with cash, the ATM can be partially sabotaged by the perpetrators to prevent consumers from depleting the cash. Sabotage can involve jamming the card reader or simply placing a notice on the ATM advising consumers that it is not functioning. Attackers have also been known to block CCTV cameras prior to an attack.

Chapter 5. Reducing Risk of Explosive Attacks

It is unlikely that one single solution or initiative will significantly reduce the risks associated with explosive attacks targeting ATMs. It is important to adopt a layered approach to make the target less appealing.

5.1. Detecting the Insertion of Explosives

Trained staff who perform real time monitoring of building alarms and CCTV covering the area around the ATM and the interior of the room housing the ATM can provide an early warning that an attack is about to be perpetrated.

Alarm grids such as penetration mats attached to the inside of the fascia and the rear of the dispenser and depository shutters can provide an early indication that the ATM is being attacked prior to the insertion of explosives. Monitoring shutter opening events that are not controlled by the ATM application can also provide an early indication that the ATM is being attacked by forcing the shutter to open.

Gas detectors fitted within the security enclosure can provide an alarm or activate a neutralization system for explosive gas attacks where gas is inserted directly.

Deployers can monitor the network for card numbers used to initiate an attack by opening shutters via a transaction.

5.2. Explosive Gas Resistant Security Enclosures

The European Standard EN 1143-1 covers requirements for ATM security enclosures (ATM safes) to be certified.

The full details of the standard are too complex for this document but the basic principle is that a wide selection of attack tools and techniques are used to test the security of the enclosure. Access to the cash is determined as either full access or partial access. The standard allocates a number of points to each type of attack tool and measures the time taken to breach the security of the enclosure.

A safe or security enclosure will never completely prevent access to the cash. Given powerful enough tools and enough time, a perpetrator will eventually breach any safe. The purpose of the enclosure is to make it more difficult and more time consuming to gain access to the cash.

The European Committee for Standardization (CEN) recognizes and certifies different grades of security. For ATMs these generally range from CEN L at the entry level up through CEN 8 (VIII):

- CEN L
- CEN 2 (II)
- CEN 3 (III)
- CEN 4 (IV)
- CEN 5 (V), etc.

Most ATM safes are not rated higher than CEN IV. An ATM safe will display the appropriate label based upon compliance with the standard indicating the level of protection provided.

Since April 2012 an optional GAS test has been integrated with the standard (EN 1143-1:2012). In contrast to the basic grades seen above, the "GAS" indicates that it is not possible to open the ATM safe solely by inserting and igniting gas at the type test.

In brief, the GAS test involves the following:

- Putting a flexible container similar to a balloon into the ATM safe
- Filling the container with a stoichiometric and homogeneous gas mixture (1 C2H2 + 2.5 O2, purity >99%) and igniting the gas
- After detonation, performing an additional physical tool attack in an attempt to gain access to the cash. The higher the grade, the longer the physical attack afterwards is performed.

ATMs with gas resistance must be in compliance with at least CEN II GAS.

The GAS test is designed to cover worst case scenarios in that the quantity of gas inserted (50% of the internal volume of the enclosure) is greater than is practical in the real world. For test purposes the enclosure does not contain standard ATM modules such as the dispenser or depository and no gas is allowed to leak from the enclosure prior to detonation. The gas mixture is also scientifically measured to provide maximum explosive power which perpetrators operating in the field are less likely to achieve.

An ATM security enclosure certified by CEN that provides a level of tested protection against gas attacks has the word GAS appended to the label.

Examples include:

- CEN 2 (II) - GAS
- CEN 3 (III) - GAS
- CEN 4 (IV) - GAS
- CEN 5 (V) - GAS

The most commonly deployed ATM security enclosures with gas protection are resistance grades III GAS and IV GAS.

Actual design and construction of the enclosure varies by manufacturer. An example of a design feature is specially designed and located bolts that prevent the door from opening enough to access cash but allows pressure caused by the explosion to escape.

5.3. Solid Explosive Resistant Security Enclosures

Similar to the GAS tests mentioned above, the European standard EN 1143-1:2012 documents in detail the test procedures for solid explosives and the approach used to gain access to the cash following detonation. The higher graded enclosures require resistance to a greater quantity of explosive, more powerful tools and more time.

An ATM security enclosure with the letters EX appended to the label has been certified and provides a level of tested protection against solid explosive attacks. If the enclosure also offers appropriate resistance to gas attacks, the label is appended with GAS EX

Examples include:

- CEN 2 (II) - EX
- CEN 2 (II) - GAS EX
- CEN 3 (III) - EX
- CEN 3 (III) - GAS EX
- CEN 4 (IV) - EX
- CEN 4 (IV) - GAS EX
- CEN 5 (V) - EX
- CEN 5 (V) - GAS EX
- CEN 6 (VI) - EX
- CEN 6 (VI) - GAS EX
- CEN 7 (VII) - EX
- CEN 7 (VII) - GAS EX
- CEN 8 (VIII) - EX
- CEN 8 (VIII) - GAS EX

The explosive used in the “EX” test is Pentaerythritol tetranitrate (PETN) which is used at the following mass:

- II, III, IV: 70g
- V, VI, VII: 100g
- VIII: 200g

The CEN working group is planning to update the EX test on the basis of the attacks which are now taking place. Actual design and construction of the enclosure varies by manufacturer.

5.4. Complementary Solutions

It is unlikely that a single solution will significantly reduce the risks associated with explosive attacks against ATMs. Thus, a layered approach to security is required.

In addition to selecting an appropriate grade of security enclosure, the following list of complementary solutions should be considered:

- Intelligent Bank Note Neutralization Systems (IBNS)
  - *Degrade notes (e.g., ink staining)*
  - *Activation sensors to detect an explosive attack in progress*
  - *Activation triggered by explosive shock wave*
  - *Signage to warn that IBNS is installed*
- Strengthened shutters for dispenser and depository modules
- Explosive gas neutralization or suppression systems
  - *Secondary enclosure to hold and protect large quantity of neutralization or suppression agent to prevent sequential attacks*
- System to dissipate gas with inert gas, such as CO2
  - *Secondary enclosure to hold and protect large quantity of inert gas to prevent sequential attacks*
  - *CO2 detector or alarm in room for health and safety reasons*
- Pilot flame or sparking mechanism to ignite gas prior to high concentration
- Internal cages or bars designed to jam in place when explosion occurs to prevent easy access to cash following explosion
- External cages, bars, or enclosure around ATM
  - *Restrict access to cash via security enclosure door and walls*
  - *Reduce explosive impact on building*
- Explosion absorbing modules or cladding inside safe
- Guillotine or other metal barrier as secondary shutter for dispenser and depository
- Strong cable hole plugs to resist gas pipe and solid explosive insertion
- Reinforced metal door and locks to room housing ATM
- Anti-ram raid bollards and street furniture to restrict access to the building
- Sensors or penetration mats to detect shutter or fascia damage
- Abnormal shutter opening monitoring (not controlled by the ATM application)
- Installing and monitoring alarms and CCTV, ensuring installation of the video and alarm systems minimizes the risk of tampering
- Activating local audio alarm (screamer) on detection of attack or detection of gas

- Using dense security fog or security smoke protection to fill ATM room on detection of attack
- Tracking device (GPS/GPRS/RF) within cassettes
- Signage to advise security measures in place to deter attack
- Managing cash balances to minimum required
- Overnight de-cash, leaving ATM empty of cash with security enclosure visibly open
- Internal branch or store lights left on overnight to deter attack
- Overt or covert security patrols to deter or disrupt attacks

When considering the adoption of complementary solutions, it is important to also consider potential issues such as:

- Health and safety
- Impact on ATM maintenance
- Training for staff, CIT, and maintenance crews
- Impact on any ATM warranty from the ATM vendor
- Any other solutions that must be mutually exclusive

Chapter 6. Case Studies

6.1. Explosive Attacks and Impact of Solutions Deployed, Italy

(Case study provided by BNL, Italy)

In Italy a significant number of gas attack threats to ATMs began in 2007. The number of gas attacks subsequently increased until a migration to solid explosive techniques surpassed gas attacks. Solid explosive techniques now represent the majority of attacks in Italy.

The high volume of explosive attacks in Italy can be related to the legal system. Consequences by law for ATM attacks are not severe, and do not deter criminals. Furthermore, there is inadequate information sharing between different police forces.

BNL banks today have some of the best practices in Italy for gas and solid explosive attack prevention.

In 2012 about 90% of attacks against BNL failed. BNL achieved this important target by deploying a large number of countermeasures in three main areas:

- Technical solutions designed to cover different phases of ATM attacks
    - *Prevention – a set of sensors attempts to intercept the time zero within the attack activities flow. There is strong coordination between events coming from the sensors, videos coming from the local video cams, and human control via a central room.*
    - *Cash Protection – ink-staining systems installed on 90% of the installed base start to stain all the cash as the attack begins. The ATM sensors invoke the system directly before the explosion occurs.*
    - *Safe Protection – anti-gas countermeasures and an external cage behind the ATM prevent the opportunity to access the cassettes after the explosion. In addition, because the cage absorbs part of the explosion, this prevents major damage to the branch.*
- Observatory solutions that include a market observatory committee comprising ATM and security vendors who meet periodically
    - *Identify new countermeasure solutions*

    - *Ensure adaptation of ATM architectures to new threats and techniques as they evolve*
- Relational solutions that promote effective communication and information exchange
    - *Integration of police force information and the bank network within a security risk database provides a continuous updated map of the events*
    - *Effective information exchange among the BNPP entities of BNL due to Global Group Security activity provides ability to*
        - identify cross border threats,
        - try to forecast the main risk areas for the next events, and
        - be updated quickly for the new types of attacks that the crime organizations are using, being ready to apply new countermeasures
- Operational solutions that include a central control room that receives all the information from the ATM installed base and has access to a security risk database
    - *Proactive remote / onsite surveillance dedicated to specific high risk areas*
    - *Immediate activation of local emergency procedures*
    - *Adjustment of cash replenishment levels to the local risk situation*

6.2. Explosive Attacks and Impact of Solutions Deployed, The Netherlands

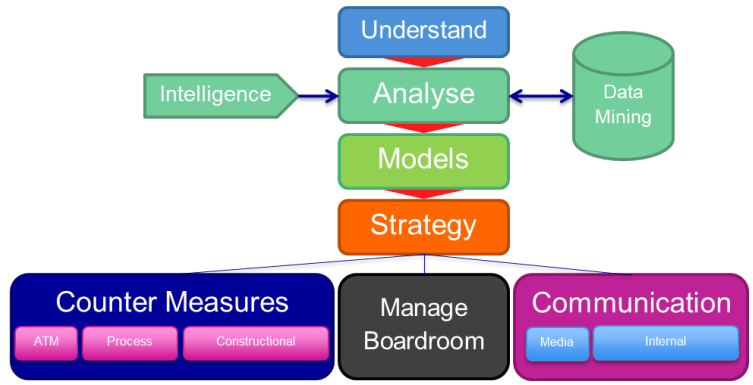
(Case study provided by Rabobank, The Netherlands)

6.2.1. Introduction

Gas attacks against Rabobank pinboxes started around the end of 2008. Shortly after pinbox attacks, perpetrators began to attack 24-hour ATMs. In 2009, Rabobank realized that gas attacks were a trend that was not going away.

The gas and explosive attacks were much more devastating than previously experienced ram raids. In addition to the stolen cash and property damage, Rabobank now had to deal with the risk of enormous collateral damage: the chance of human casualties.

In this case study Rabobank uses a model to describe how it addressed the gas and explosive attacks in stages. Although the model describes the stages consecutively, they can occur in parallel, and one stage can influence the other based upon how the crime was committed.



Work model

6.2.2. Stage 1: Understand the Seriousness of the Situation

When Rabobank first faced gas attacks it took a few months to assess the seriousness of the threats. Information about other countries that might be facing a similar problem was limited. It appeared that some Mediterranean banks were facing gas attacks, but a connection to the Rabobank attacks seemed unlikely. For almost three years Rabobank was the only bank in the Netherlands that was attacked.

To make matters worse, gas attacks against ATMs were not a priority for either the Police or the Justice Department who considered ATM attacks as business burglaries rather than high priority crimes. Rabobank realized it would have to deal with the attacks single-handedly, building their own defence mechanisms and taking countermeasures.

6.2.3. Stage 2: Analyze

The analysis stage required building an intelligence picture that included multiple aspects of the crime:

- How the crime was committed: the Modus Operandi
- The chances of attack on a particular ATM location and why certain ATM locations were attractive for the criminals
- Which locations would result in a major impact
- Cross-examination of bank financial systems with the attacks to build a perpetrator profile
- Information made available by the police and other banks (this required much persuasion at times)

Modus Operandi

The first step in the analysis stage was to determine how the crime was committed using several sources of information. Analyzers collected and studied images from cameras deployed at branches and ATMs, as well as incident logs from the emergency room where all alarms were collected. Bank security managers went to the crime scene to research the premises and the ATM soon after the crime was committed, taking turns because

the attacks took place in the middle of the night. Later, Brink's Security Services was thoroughly trained to take over crime scene research. Questions on the Modus Operandi are:

- Where on the ATM did the attack take place?
- How was the gas/explosive device inserted?
- What were the tools that were used to open the ATM shutter?
- What kind of explosive was used?
- What kind of gas mixture was used?
- What is the estimation of the explosive power?
- How much gas was used?
- How was the gas ignited?
- Which fuse was used?
- How was the door rammed?
- Which kind of vehicle was used for ramming?
- What kind of getaway vehicle was used?
- Was the vehicle stolen? Or were the license number plates stolen?
- Was the vehicle burned afterwards?
- How was the money collected?
- What was the total duration of the crime?
- Did the criminals use garages or other safe places?
- Was the ATM attacked TTW or placed inside?
- Did they use a beam to avoid anti-ram measures?
- Was the ram vehicle modified for ramming?
- Which type of ATM was attacked?

Attack Locations

Analysis of the ATM attack locations was important for two reasons: first, to determine the chance of an attack on that specific location; and second, to assess the impact on the ATM surroundings. Input from the Modus Operandi analysis provided valuable input to the locations analysis.

After assessing the chances of an attack on a location, the bank prioritized the locations to determine the order of installing countermeasures, and used the information to direct the police to the ATMs most likely to be attacked. How to determine the characteristics of the location (chance)?

- Is it a standalone ATM, TTW branch, or TTW off premise?

- Is the entrance to the vault room placed inside or in the outside wall?
- What's the construction of the rammed entrance of the value room and/or the branch?
- Is the location near a highway or another major road (max 10 minutes by car)?
- How many escape routes are there?
- Is there enough space to ram the door with a vehicle (3 meters/ 9.8 feet is enough for a car)?
- Is the location in a small village or in the outskirts of a major village/city?
- Is the location placed so that the criminals can work inconspicuously (around the corner, behind trees, etc.)?
- If in the center of a bigger village or city, are there escape routes for motorcycles or other two-wheeled vehicles where the police cannot follow by car?
- In which part of the country did the attack take place? Was it near a border?
- How long did it take for the police to arrive at the crime scene?

The impact assessment was very important because the kind of countermeasures can vary depending on how much risk is associated with the surroundings, such as a gas-station or a nearby retail store, and the people living directly next to or above the ATM. How to determine the characteristics of the location (impact)?

- Is it a standalone ATM, TTW branch, or TTW off premise?
- In what type of building is the ATM placed (apartment, branch, store, no building at all)?
- What is the construction of the building (concrete, bricks, wood)?
- What is the damage caused by the gas/explosive attack?
- How is the front of the building constructed?
- What is the damage of the ramming?
- Was the attack proportional? Did the criminals use just enough gas/explosives or did they use too much?
- Are there buildings across the street (<10 meters or 33 ft)?
- What was the reaction/sentiment of people living near the ATM?
- Are there victims?

Build a Perpetrator Profile

The Rabobank team used police information and information from the bank's financial systems to build a perpetrator profile. Information of interest included strange behaviour related to transactions of certain clients like small retailers or suspicious individuals, credit or debit card behaviour, and car insurance information.

The police focused not only on the criminals carrying out the attacks, but on the facilitators and other types of criminal behaviour. In the Dutch case, the criminals carried out various other crimes including car theft, shop lifting, and raids. The criminals used the stolen cash to invest in other criminal activities.

By studying the different Modus Operandi, Rabobank discovered that there were two types of perpetrators. The first group included the professional criminals who were well organized, used the right tools and knew where and how to engage the ATM. The second group included the copycat criminal. The copycat criminals exhibited dangerous behaviour by using other kinds of explosive material at the wrong spot on the ATM or vault room, causing enormous explosions and fires. Their Modus Operandi was easy to recognize. Copycats never succeeded in their attacks but caused a lot of damage. Almost 25% of the ATM attacks against Rabobank were carried out by copycats.

Intelligence Sources

Rabobank collected most of the intelligence itself through various research methods, including:

- Visiting the attack locations
- Gathering information from police forensics (this was difficult and required building good relationships with the police)
- Contacting bomb-squads and research institutes to learn about the effect of explosions
- Exchanging information with other banks about the attacks

The Rabobank team was also able to obtain information from abroad via foreign banks; Rabobank's ATM supplier; conferences, such as the ATMIA ATM Security Conference; and organizations, like EAST (European ATM Security Team). Information from the media proved to be quite unreliable and was useful only as an indicator.

Data Mining

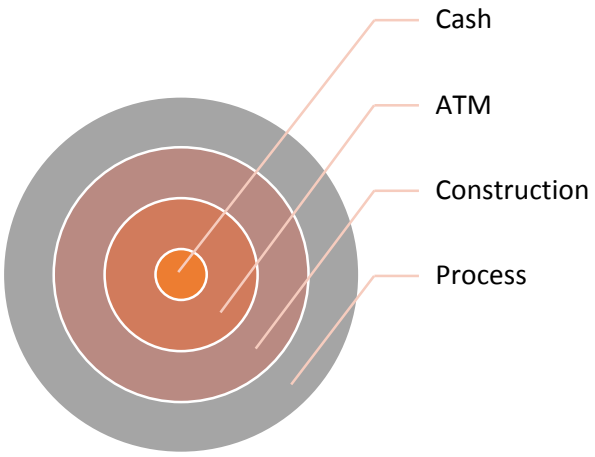
Rabobank used its own data mining unit to cross-reference and correlate factors associated with the attacked ATMs. Factors included weather influence, ATM transactions, ATM locations in relation to the size of the city or village, and the distance to highways and major roads. The results of their analysis yielded no surprises. The outcome of the data mining exercise confirmed prior analysis.

6.2.4. Stage 3: Build Models

Upon completing the Modus Operandi analysis, the location analysis, the perpetrator profile, intelligence gathering, and data analysis, the Rabobank team began to cluster the information to determine certain groups of criminals and their Modus Operandi. The team constructed models that they could use to determine which countermeasures should be deployed.

6.2.5. Stage 4: Develop a Strategy

Using the results of the analysis, Rabobank developed an effective strategy that addressed countermeasures, boardroom management, media communications, clients and local branches. Each aspect of the strategy was divided into several sub-layers.



Strategy: Multi-layer of Defence

Rabobank divided the strategy into three areas for attention:

- Processes and procedures
- Countermeasures at the ATM
- Constructional countermeasures

Each area was divided into several measures and processes to get a true multi-layered approach.

Processes and Procedures

The bank team examined its cash processes as well as processes that addressed informational sharing among Rabobank, the police and other banks.

Through examination of the cash process the bank discovered that lowering the amount of cash in the ATMs would lower their losses. Together with Brink's, Rabobank developed a cash management system that would take into account high risk locations while still achieving a logistically optimum level of cash.

To address information sharing, Rabobank established a structural meeting every month with the police, justice department and other banks to exchange experiences and information. In the beginning, there was considerable mistrust and it was difficult for country-wide operating banks to work with regionally-organized police. The process improved over time as the police developed national teams. At the time of this writing, the public-private cooperation is very good and an example for other organizations.

The Dutch Bankers Association took a central role in the exchange of information between banks. The team used the existing physical security working group (among others) as a platform and formed an expert group in intelligent banknote neutralization systems (IBNS).

The Rabobank central branch advisory analyzed all ATM locations and prepared a so-called "cold" advice for each local bank that provided insight into their ATM transactions. In addition, the advisory calculated the optimal spread of ATMs across the region. Taking this information into account along with local sentiments, the advisory converted the "cold" advice to a "warm" advice, in most cases resulting in a reduction of ATMs.

ATM Level

First, the Rabobank team examined the ATM thoroughly to find weak spots for attacks with gas and explosives. The opening in the safe at the front of the ATM where the money is dispensed was found to be the most vulnerable area. The opening is covered by a plastic shutter that can be removed easily with a screwdriver. The team also discovered that the standard CEN IV graded safe did not withstand the attackers' explosives. After an attack, safe doors were sometimes found on the opposite side of the room. In one attack criminals used excessive solid explosives, blowing a hole in the safe door from the outside and causing the surrounding building to collapse.

Rabobank researched multiple types of countermeasures at the ATM level, and within non-financial industries like the gas and petrol industry and army-protection. Their research concluded that no single measure would stop the criminals; therefore, multiple lines of defence would be required at the ATM.

Rabobank first installed an anti-gas system to target the gas attack. The system was far from perfect and required significant modifications during the process. It is still not ready. The bank also reinforced the safe by replacing most of its ATMs with a newer model containing a CEN IV-GAS safe. Rabobank continues to research methods to reinforce the shutter and identify a reliable IBNS system.

Construction

Though collateral damage was severe on several occasions, fortunately no one was injured during ATM attacks against Rabobank. The Rabobank team discovered that the first weak point of the vault room is the door, also known as the single person entrance. In most branches and off premise locations, the vault room door is placed in the outside wall so that CIT (Cash in Transit) can park their trucks against the door to accommodate a "closed delivery."

Attackers used several methods to ram the vault door to gain entrance to the value room. For example, attackers drove a car forward or backwards, ramming the door. When the perpetrators could not reach the door by car due to anti ramming objects, they used a heavy wooden beam that was long enough to bridge the distance between the anti-ramming objects and the door, and then rammed a vehicle against the beam placed against the door. At times, the perpetrators used a scaffolding pipe welded to the chassis of a van. As a last resort, criminals occasionally used a chainsaw or a manual ramming tool to gain entrance.

The explosion or ramming attack often caused the bank walls to collapse or the ceiling to come down. Inner walls were also damaged heavily and sometimes moved by inches or collapsed causing severe damage to neighbouring houses, apartments or businesses. However, in many instances the construction of the building was strong enough to hold.

Rabobank had two construction problems: the vault room entrance and collapsing inner and outer walls. To reinforce the vault room entrance, a manufacturer developed a reinforced door that could withstand ramming with a forklift. To resolve the collapsing walls issue, the bank and a manufacturer of explosive-proof walls developed a "box in the box" consisting of modular panels that could be installed in the vault room around the most vulnerable ATMs. The box was designed with the strength to withstand explosive attacks and ramming and the resiliency to absorb explosive blasts. Explosive-proof walls provided a particularly effective solution for locations with high risk of severe collateral damage and casualties.

One great danger that Rabobank could not solve was the risk of possible effects from fire flash-over caused by the criminals igniting the ramming vehicles parked against the façade.

Rabobank internal regulations are derived from the security police and documented in a manual. The bank ensures that the manual is current and consistent with the most recent developments in construction security related to ramming and gas/explosive attacks. Adherence to regulations is mandatory.

Managing the Boardroom

The Rabobank team realized that to make changes it would need to persuade the decision makers. To gain access to decision makes, Rabobank formed a taskforce for gas and explosive attacks. Members were required to be part of the relevant line management with easy access to the board of directors. Every gas attack was reported in the line, and, each month, security management presented an overview of the situation to constantly raise awareness of gas and explosive attacks.

Being a cooperative bank was also a good way to inform local banks about the developments in countermeasures. While the local banks appreciated the transparency, not every countermeasure was immediately effective.

Communication Strategy

The bank's communication strategy promoted vital transparency as appropriate for different groups. For example, the communications strategy included a plan around communicating with the media (a little less transparent than with the banks, but always fair). The strategy also addressed ways to inform and reassure Rabobank's clients and its local branches.

Media Strategy

As collective banks, Rabobank decided to let the Dutch Bankers Association be the spokesperson for all of the banks. Rabobank's Communications department developed the communications strategy for the media. The Dutch Bankers Association and other banks accepted it as the standard.

The strategy included allowing local banks to handle the regional press when it concerned single attacks. The Communications department also created a specific media strategy for local banks that included rules such as never mention the losses, don't talk about countermeasures or Modus Operandi, and never mention the type of ATM.

To illustrate the importance of not being too explicit about the Modus Operandi in the press, almost 25% of all attacks were carried out by copycats. Most of these attacks occurred immediately following a major press publication of a professional attack.

Communication towards Clients

Rabobank's policy was to limit communications with clients to avoid unrest. As needed, Rabobank assisted local banks with explanations to clients such as landlords, insurers and owner associations.

Communication towards Local Banks and Branches

To ensure transparency with the local banks and branches, Rabobank organized frequent meetings and presentations. The Bank used its intranet for more formal communications.

Lessons Learned

The first lesson learned was that criminals can often deploy attack methods faster than banks can deploy countermeasures. Although Rabobank successfully countered the gas and explosive attacks for almost a year, two successful attacks occurred thereafter. While Rabobank continues to roll out countermeasures and layer their defence systems, successful attacks are still possible, thus the importance of deciding on multiple measures at different levels.

The second lesson learned was that it is not possible to stop the copycat criminals. Rabobank learned that it could only deal with the effects of a copycat attack through damage control measures like the box in the box. Rabobank decided to focus its countermeasures instead on stopping the professional criminals who generally succeeded in their attacks.

The third lesson learned concerned the criticality of taking enough time for a thorough analysis to create a risk picture for all locations. The risk picture allowed the bank to prioritize the vast number of projects needed to roll out all of the countermeasures.

The last important lesson was that public-private cooperation is critical to dealing with the perpetrators. Transparent data exchange between banks and police/justice (in both directions) dramatically enhances the chances for apprehending the perpetrators.

Outlook

Gas attacks are still the most popular Modus Operandi, but there is a clear trend towards solid explosives. While gas is much easier to obtain than explosives, it appears the international trade in solid explosives is booming.

It also appears that criminals are more violent and have less regard for innocent bystanders.

Public-private cooperation will continue to be crucial in a world that is experiencing a global economic crisis. Public and private organizations are cutting budgets. Joining forces and working together may be the only way to beat the criminals.

6.3. Industry Response to Gas Attacks in the UK

(Case study provided by the British Bankers Association)

The first gas attacks against ATMs in the UK started in March 2013. In response the industry set up the UK ATM Gas Taskforce. Chaired by LINK (UK ATM network scheme), it includes ATMIA, BBA (British Bankers Association), Police, Safercash and a sub-set of the members of the ATM Security Working Group (ATMSWG).

The group agreed upon a number of areas to review:

- Media plan: Although LINK prepared a series of reactive responses, the group agreed that responses should be centralized through the ACPO (Association of Chief Police Officers) PR (public relations) plan drawn up by the police.
- Prevention/protection: LINK prepared for members a list of suppliers of various anti-explosive systems with details of how they work.
- Technical investigation of explosions: BRE (Building Research Establishment) who have expertise in assessing and investigating fires and explosive damage to buildings offered to investigate incidents for members who suffered an attack.
- Information sharing and alerts: All ATM attack data is collected on behalf of the ATMSWG via a secure website (collaboration). Incidents are reported as soon as possible. A detailed summary of gas attack incidents in the UK is available to members and police. Collaboration is also used to alert members when a gas attack has occurred.
- Liaison with global industry bodies: LINK is also collaborating with ATMIA and EAST (European ATM Security Team) to gain a global understanding of gas attacks. The BBA has produced a report based on data from countries who are members of the EBF (European Banking Federation) Security Working Group.

6.4. Industry Response to Gas Attacks in Australia

(Case study provided by the British Bankers Association)

Australia law enforcement response and strategies included the following:

- Establishment of a police task force
- Dedicated incident reporting telephone number
- Increased police patrols
- Media engagement and reward offerings
- Government identified public safety issue
- Industry liaison working group

Most of the attacks in Australia occurred in Sydney NSW (New South Wales). As a result of the volume of attacks and a directive from the state government, the NSW Police established a task force called "Poyner 2". Task Force Poyner was headed by a Police Superintendent and consisted of 30 full time detectives working 24 hours a day, seven days a week.

As part of Task Force Poyner the Police established a dedicated 1300 telephone number to allow incidents of gas attacks to be reported immediately. The task force briefed Police Local Area Commands (LACs) and advised them to increase patrols around high risk ATMs

The Australian Bankers Association (ABA) in conjunction with the NSW Police Minister and NSW Police held a media conference in which they announced that a $100,000 reward had been posted for information leading to the arrest and conviction of persons undertaking gas attacks on ATMs.

The state government saw the gas attack activity as a serious public safety issue. One member of the police alleged that "Sydney was the most bombed city in the world" at the height of the gas attack activity.

Sydney's Deputy Police Commissionaire called on the industry to establish a working group under the ABA to address the gas attacks issue as well as the recent increase in Cash in Transit (CIT) attacks. In response, the banks, cash carriers and ATM deployers established the ATM, CIT Working Group whose objective was to track local and overseas events, and identify a solution.

6.5. Industry Response to Gas Attacks in Brazil

(Case study provided by TecBan, Brazil)

Questions

1 When did explosive attacks start in Brazil?

The attacks with solid explosives began in mid-May 2010.

2 What type of explosives were used then and did that change over time?

Solid explosives (dynamite sticks, or emulsion) were used. There were no changes over time. In Brazil, we have no record of gaseous explosives attacks to equipments.

3 What type of ATM / location is most targeted? Branch TTW, 24hr Lobby, Stand alone POD...

Indicators show that about 65% of attacks occur in bank branches and about 35% in external points.

4 How is the explosive inserted into the ATM?

The mode of attack is performed via shutter. Criminals damage the shutter extending it so that allows the insertion of the explosive device. After insertion, the detonation occurs via the detonating cord. We realized, in 2013, that criminals have found another way to insert the explosives. In this case, criminals use the hole of the cabling module payer, that is connected to the CPU located on topbox, to insert it. In Brazil, the CPU is external and is located in the topbox.

5 How is it detonated?

The artifacts are exploded via detonating cord.

6 What is the first indication that an attack is in progress? Alarms, ATM out of service....

The attack occurs rapidly and takes 3 minutes in average. In some cases, you can identify the attack via ATM sensors and, in other cases, when the terminal goes offline. Another important point is that attacks are carried out very quickly, this prevents the prompt response of the police to curb criminal activity.

7 Are there any patterns to the attacks?

Yes, attacks occur with explosive artifacts insertion via shutter or other hole in the terminal.

8 How do they gain access to the rear of a TTW ATM or ATM room to get the cash following an explosion?

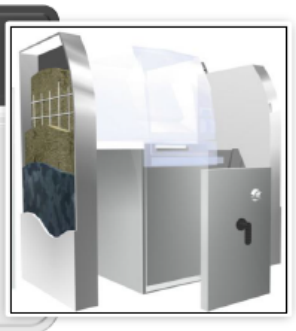
With the destruction caused by the explosion, the walls are destroyed allowing the access of criminals to the cash.

9 Have you experimented with different solutions? If so, how did the criminals respond and what are the most effective solution approaches?

Yes. We use three different solutions to curb the criminal actions. Our experience shows that this set of solutions inhibits and discourages criminals, since measures such as **shutter reduction** hinder the insertion of solid explosive in the safe, **ink staining** marks the cash and enables their tracking, and partial controlled **burning** ensures cash destruction. These actions hinder the circulation of cash arising from the crime, invalidating criminal action. Over time, these measures reduce the attractiveness factor and criminal reward.

10 What type of security enclosure / safe is used / best for resisting explosive attacks?

Our safes are made of metal (steel) and concrete.
Experience shows that as bigger strength or thickness of the safe is greater the potential of explosive attack. Increasing the thickness of the walls of the safe, there is incentives for criminals to use more explosive load in terminals during the attack.

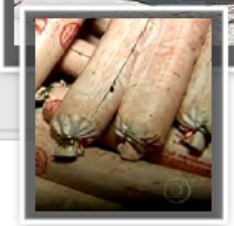


11 Do you liaise with other organizations, including competitors to share information about attacks and solutions that help?

Yes. Since the beginning of the attacks, in May 2010, we have monthly meetings with representatives of financial institutions, the Central Bank of Brazil, public safety agencies and equipment manufacturers in order to share data, information and expertise on security issues.

12 Are the Police helpful / part of an industry response?

Police make an effort to combat this sort of crime, acting in repressing these types of attack. However, it is not enough as the manufacture, storage, sale and transport of explosives are not properly supervised. It is also necessary to have greater synergy between the police forces of the states to investigate and combat explosives traffic by specialized gangs. Besides the overt police action, an important factor is the change of laws making the punishment more severe and non-bailable for this type of criminal activity.



13 What type of crime are perpetrators charged with? What type of sentence do they get if found guilty?

Larceny with low offensive power. The sentence provides a penalty of 2-4 years imprisonment.

14 Has anyone been killed by the explosions? Perpetrators or members of the public.

There were no deaths caused by explosions yet.

15 16 Any future plans or strategies for reducing the risks? What advice would you give to other countries that are concerned about explosive attacks?

The last 2 questions were joined, because we can explain both using the concepts of measures we call "6 pillars". We believe these actions are of greatest importance to fight against these criminal attacks, and they are all needed to curb these crimes:

- **Crime tipification (more severe laws)**

Crimes with explosive artifacts should be considered as terrorism action, especially if applied against life, public or private heritage. In case of bank branch and external ATMs assaults, thefts or robberies, these actions should be considered as crimes against financial system. Harsh non-bailable penalties should be applied.

15
16

Any future plans or strategies for reducing the risks? What advice would you give to other countries that are concerned about explosive attacks?

- **Proper control of explosive artifacts**

A strict control on the process of manufacturing, retailing, transportation, storage and technical dealing should be applied, preventing criminal access to these artifacts.

- **Synergy among the authorities**

All the police force (military, civil, army, federal, state and federal public ministry) should be combined to work together as a team to fight against specialized criminal organizations, exploring intelligence and counter intelligence actions to prevent and combat their crimes.

15
16

Any future plans or strategies for reducing the risks? What advice would you give to other countries that are concerned about explosive attacks?

- **Central Bank regulation**

Publish and keep up processes and rules for cash damaged by anti-theft devices embedded in ATMs, in custody in financial institutions (banks) and CIT (cash in transit) companies.

- **Technology**

Companies should develop, build and improve continuously anti-theft devices, neutralizing instantly cash in transportation process or stored in ATMs in case of attack.

- **Communication**

Create mass campaigns, allowing population to be aware of anti-theft devices, underscoring the importance of ATM service to the community. It s important to clarify that total or partially damaged cash (ink stained or burned) should not be accepted. Besides this, people should be encouraged to report suspect attitudes.

6.6. Industry Response to Gas Attacks in France

(Case study provided by Oberthur Cash Protection, France)

6.6.1. Situation

Due to increasing numbers of ATM attacks suffered during the last few years, Crédit Agricole Languedoc-Roussillon in France decided to equip their ATMs with a complete solution that would protect against different physical attacks including explosive gas. They realized they needed a layered approach to improve security.

Requirements to improve security included the need to detect and deter a large range of different attacks with a technical solution that allowed them to upgrade their installed base of ATMs. Detection and deterrence were key requirements for assessing the project's success.

6.6.2. Solution

To meet requirements, the bank installed an in-cassette ink staining solution combined with a gas sensor, penetration mat and alarm siren to achieve early activation of the staining solution.

Typical explosive attacks occur at speeds of up to 8000m/s. Therefore, the system needed to employ a fast staining process, preferably detecting the attack before the explosion actually occurs. For an effective attack, criminals need to insert the explosives into the ATM and a very common entry point is the shutter.

6.6.3. Explosive Gas Attacks Prevention

To prevent explosive gas attacks, the bank fit an explosive gas detection device inside the ATM safe. The device was designed to activate when an explosive concentration of a gas is detected. The device could detect a range of explosive gases such as Methane, Acetylene, Propane, Hydrogen, Isobutane, Ethanol, Ethylene, Ethane, Hexane and Benzene.

6.6.4. Solid Explosive Attacks Prevention

With a penetration mat added to the existing ATM shutter blade, the system could react to drilling of the shutter by a 6mm drill bit or larger. Any deflection of the shutter blade, with a screwdriver for example, could be detected by an optional sensor which was retro-fitted to the existing shutter mechanism.

Although both methods of attack detection are wholly independent from each other, they can both be installed in connection with the ink staining solution to counteract both gas and solid explosive attacks.

In August 2012 Crédit Agricole Languedoc-Roussillon approved and installed the solution in their ATMs.

6.6.5. Result

On June 25th, 2013, Crédit Agricole Languedoc-Roussillon suffered an ATM explosive gas attack in one of its bank branches in the South-East of France.

The ATM had been equipped with ink staining and sensor solutions a year earlier which limited the impact of the attack to a large extent.

During this particular attack, as soon as the combustible gas was detected by the gas detection sensor, the system sent an initial signal to trigger the audible alarm siren with the intent to stop the attack. However, the attackers continued inserting the gas, activating the ink system which stained more than 20% of the surface of the banknotes making them worthless to the attacker.

The criminals were stopped in their tracks and neither the branch nor the ATM suffered further collateral damage from an explosion. The siren in combination with the staining of the banknotes served as effective deterrence for the criminals who realized the futility of exploding the ATM.

6.6.6. Conclusion

Gas attacks have a huge impact on a bank's business operations and reputation, often significantly higher than the actual cash losses. Consequently, it is vitally important to understand the banks' specific needs in order to define the most effective defences.

Intelligent banknote degradation systems can be deployed successfully with sensor mechanisms as solutions for current and future security challenges for banks and ATM providers around the world.

This very recent case study was kindly shared by Crédit Agricole Languedoc-Roussillon and Oberthur Cash Protection.

6.7. Industry Response to Gas Attacks in Germany

(Case study provided by German Insurance Association, GDV)

6.7.1. Risk Analysis of ATM Explosive Attacks

Extract from "Guidelines for Security Automated Teller Machines" published by German Insurance Association, GDV, 2012.

Explosive attacks on ATMs are a recent phenomenon in Germany and Europe. While it is difficult to identify a specific risk factor or a universally applicable set of risk factors, there are some observations that can be made.

At this time there are four key risk factors that seem to be relevant to the selection of an ATM for an attack, and therefore should be included in an individual risk analysis of an ATM site:

- Machine opening(s), e.g., shutters
- Environmental conditions
- Positioning of supply openings and building structures
- Traffic connections

6.7.2. Machine Opening(s), e.g., Shutters

ATMs have a number of openings due to their design and functionality. However, gas attacks occur almost exclusively on the cash dispenser. ATMs with a cash shutter that is designed to prevent the insertion of a hose pipe reduce risk significantly. ATMs with only one shutter for both cash deposits and cash dispenser also reduce risk.

6.7.3. Environmental Conditions

The preparation for an ATM explosion is very conspicuous. To avoid observation, perpetrators typically carry out their attacks between midnight and dawn in locations that are not frequented regularly during this time. One can therefore assume that ATMs at locations with personnel on site throughout the night hours are subject to a low level of risk.

6.7.4. Positioning of Supply Openings / Constructional Conditions

ATM attacks are normally perpetrated from the front of the ATM on the cash shutter. It is crucial for the attacker to obtain easy and quick access to the ATM's cash after a blast. Cash access is easiest in a front loader ATM because the safe door opens into the customer area. Rear loading ATMs present more difficulties for the criminals because they have to gain access to the rear ATM safe doors shortly before or after the blast. If the walls are lightweight, have space above them, or man-sized windows in them, the perpetrators can assume that access to the rear of the ATM is already made available by the explosion. Experience suggests that TTW ATMs in fixed constructions (corresponding wall elements, burglar-resistant doors and windows) are less attractive.

6.7.5. Traffic Connections

In Germany, when an attack occurs, the public reports the explosions to the police and emergency services intervene quickly. Criminals tend to prefer ATM sites with longer police intervention times and with the fastest escape routes.

6.7.6. Supplemental Commentary

By members of ATMIA's European Gas & Explosive Attack Steering Committee

These factors are incredibly useful for the first stage of risk analysis on an ATM operator's ATM estate, i.e., trying to establish which of the ATMs are most likely at risk of attacks. An ATM operator should conduct a risk analysis exercise when dealing with attacks for the first time on their ATMs or when attacks have migrated for the first time into their market.

However, experience in some European markets has shown that as an ATM operator installs counter measures on the vulnerable ATM sites, the criminals will move their attacks to ATMs which are riskier for their purposes. For example, in the Netherlands one bank reported only attacks on rurally located ATMs at first, but as the rural ATMs were protected, the criminals moved to urban ATMs and started using scooters as their get-away vehicles in these high traffic and well-policed locations.

6.8. Industry Response to Gas Attacks in Portugal

(Case study provided by SIBS, Portugal)

Legal systems and penal codes dealing with criminals vary by country. An example of applicable laws in Portugal follows.

ATM gas and explosion attacks can be prosecuted under the following criminal charges according to Portuguese law:

- The act of the explosion hazard itself (Article 272.º - Fire, explosions and other especially dangerous behavior) with a penalty range from three to ten years
- The purpose for which the explosion is executed, i.e. the appropriation of high monetary amounts (Article 204.º - Qualified theft) with a penalty ranging up to five years, or from two to eight years in case of practical aggravating reasons
- In cases of organized groups, criminals can also be prosecuted for criminal association (Article 299.º - Criminal Association) with a penalty range from one to five years
- The damage itself (Article 213.º - Qualified Damage) with a penalty range from two to eight years

Other examples (in no particular order) of the type of charges that may be applicable are:

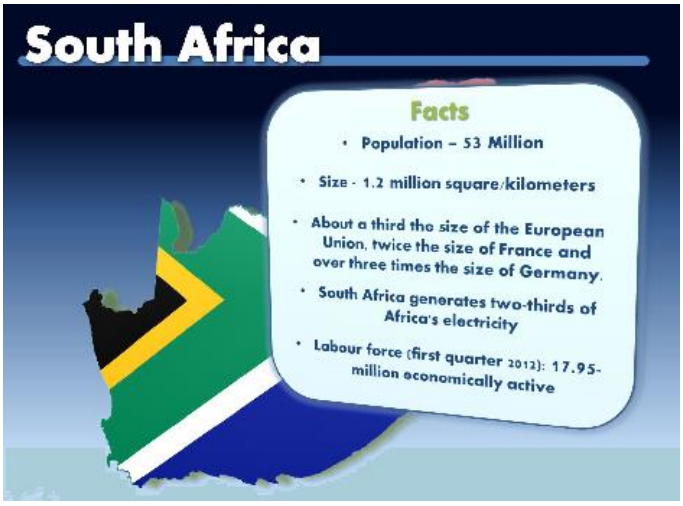
- Theft
- Burglary
- Robbery
- Aggravated burglary
- Vandalism
- Destruction of property
- Trespass
- Causing an explosion to the endangerment of life
- Reckless behavior to the endangerment to life
- Arson
- Possession of equipment for the purpose of committing a crime
- Possession or use of restricted munitions
- Possession of equipment that can be used to commit an act of terrorism
- Breach of the peace

6.9. Response to ATM Bombings in South Africa

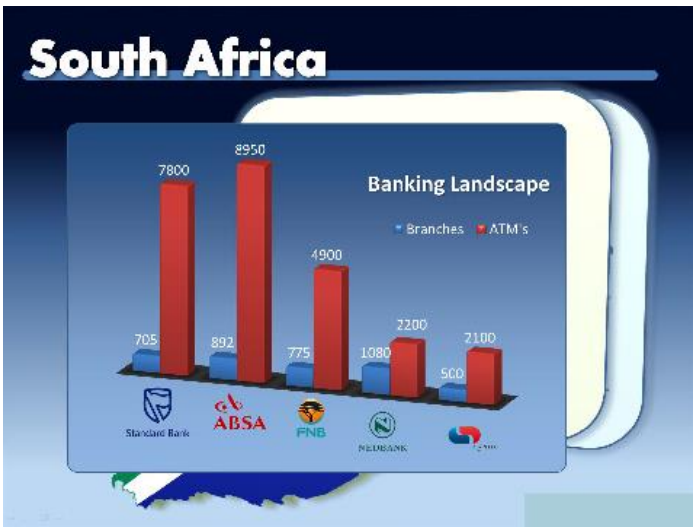
(Case study provided by Standard Bank, South Africa)

6.9.1. Banking Landscape of South Africa

With a population of 53 million and with a geography of 1.2 million square kilometres, South Africa is approximately a third of the size of Europe. The banking industry consists of five major banks: ABSA, Standard Bank, FNB, Nedbank and Capitec Bank.



These five major banks provide 3,952 bank branches and 25,950 ATMs throughout the country.



6.9.2. ATM Bombing Synopsis

ATM bombings in South Africa most commonly use solid explosives obtained illegally from the mining industry. In particular, an explosive substance known as PowerGel is detonated by lighting a fuse wire terminated with a Det Cap (detonator),

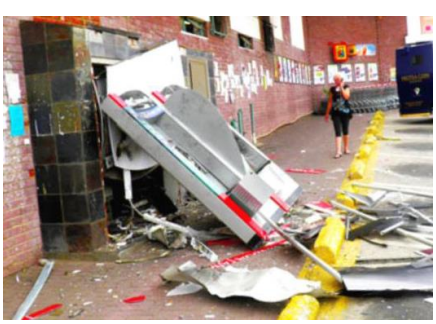
The explosive is normally inserted into the safe following vandalism to the cash dispenser gate from the front of the ATM.

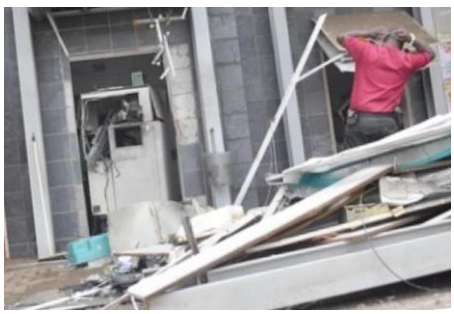
Most explosive attacks take place between midnight and 5 am. While different types of sites are targeted, the perpetrators prefer locations with no passing traffic and easy escape routes. Limited policing further reduces the risk of apprehension.

The Process

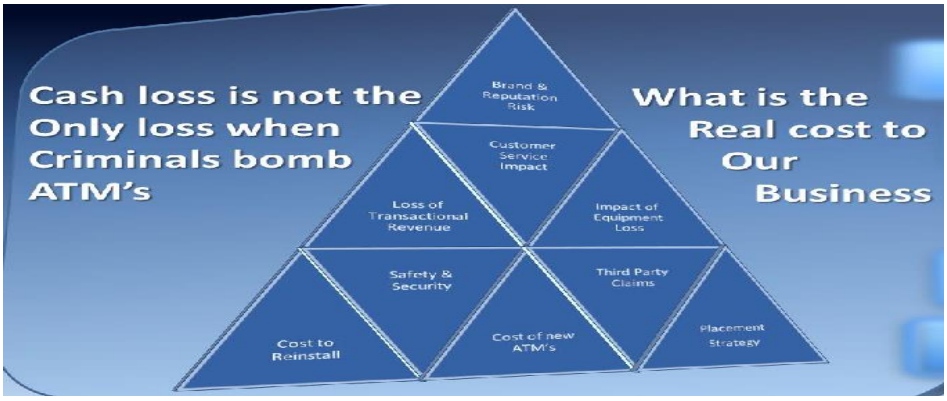
Criminals vandalize dispenser shutter, insert explosives, detonate, remove cash, exit location and secure escape. All of this can be achieved within three minutes.

ATM bombings using solid explosives often cause extensive collateral damage to buildings and the area surrounding the ATM targeted.





The business impact of ATM bombings is much greater than simply the cash loss from the ATM.

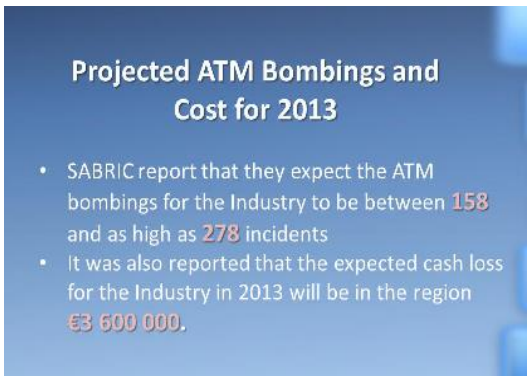


Additional impact includes:

- Brand and Reputation Risk
- Customer Service Impact
- Loss of Transaction Revenue
- Impact of Equipment Loss
- Safety and Security
- Third Party Claims
- Cost to Reinstall
- Cost of New ATMs
- Placement Strategy

The tangible costs are typically 65,000 Euros per ATM bombing attack.

The South African Banking Risk Information Centre (SABRIC) projected (during 2013) that ATM bombings for the full year 2013 to be between 158 and 278 incidents with a total industry cash loss estimated at 3,600,000 Euros.

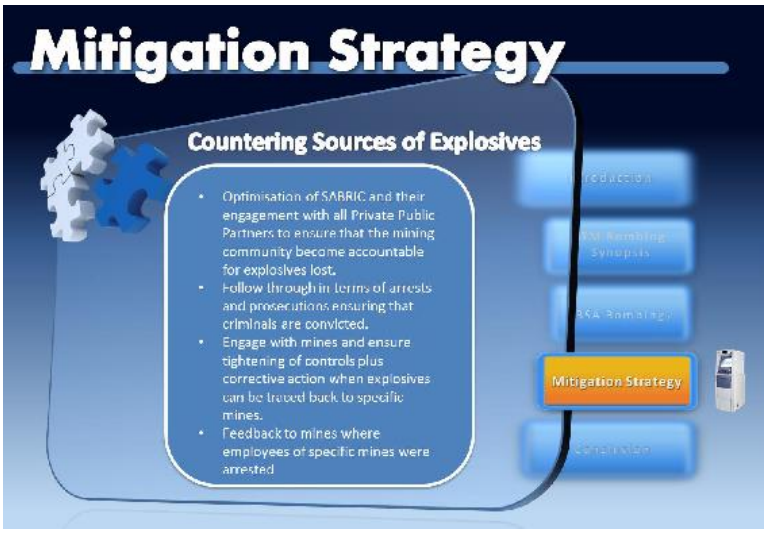


6.9.3. Mitigation Strategy

The core philosophy in mitigation is to remove the reward element. This is achieved by gaining pro-active intelligence, countering the sources of explosives, enhancing internal business processes and hardening the target.

SABRIC established a focus group bringing all the banks together to share and pool resources. SABRIC represented the banks while engaging with the judicial system to encourage harsher sentences and liaised with the Provincial Police Commissionaire and Serious Crime Task Team.

SABRIC also published a guide designed to assist the South African Police (SAP) in dealing with ATM bombing incidents and pressured the mining sector to be more accountable for the control of explosives.



Internal business processes were enhanced to reduce overnight cash holdings for high risk ATMs. A stringent security sign off policy was implemented and ATM deployment rules were tightened with strict adherence to ATM security specifications.

Additionally, weekly trend analysis of industry ATM bombing attacks was used to identify new high risk locations and in turn allowed realignment of high risk response teams.

Investment in target hardening was used to reduce the reward element from the attacks. Measures included a combination of initiatives and additional security measures. The aim was to ensure that the ATM safe door would remain closed when attacked and early warning devices and external security measures were deployed and enhanced to meet the threat.

Specific technical enhancements included a modification to the ATM known as the 'Presenter Bomb Mod'. This is integrated with the alarm panel to detect attacks and physically prevents the insertion of a crowbar into the presenter area. Integrated as part of the ATM safe, the cash opening throat is reduced in size.

The ATM safe is specified to be CEN 5 (V) EX. In the event of an attack, the safe is designed to 'breath' which releases energy from the explosion whilst maintaining structural integrity. In addition to enhanced designe to keep the safe door attached to the safe following an explosion, it also resists cutting attacks using grinders, thermal lances as well as other physical attacks used to gain access to the cash.

The building containing the ATM is also secured electronically and physically.

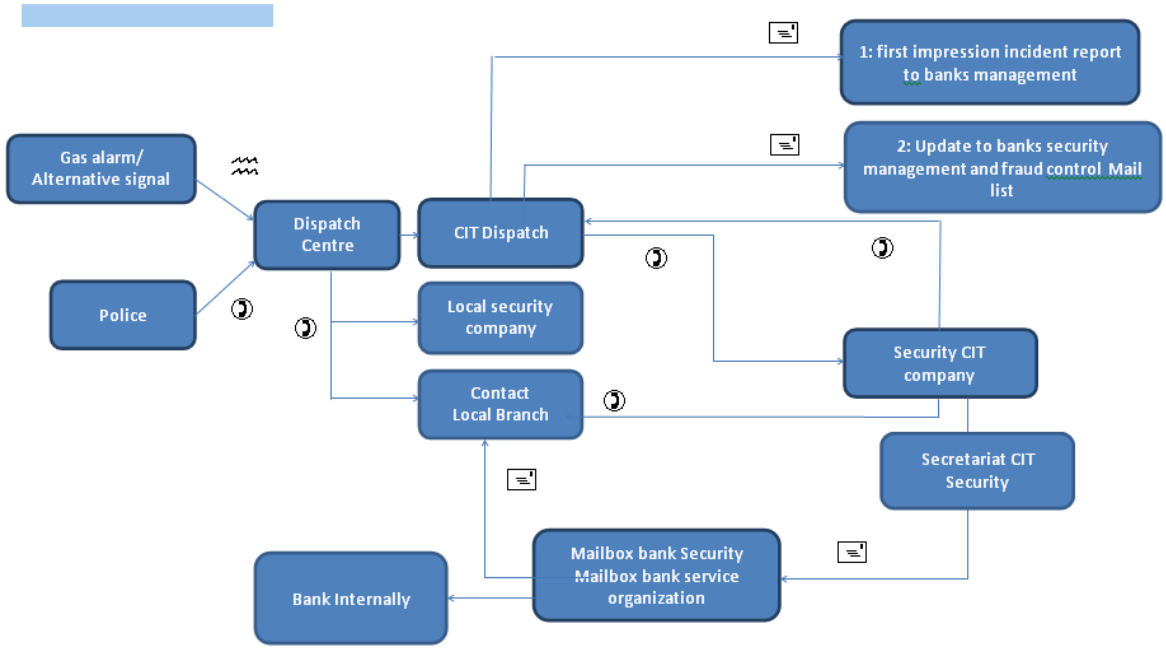
6.9.4. Conclusion = Collaboration

In conclusion, collaboration across the industry and a close strategic partnership between banks and their ATM vendors has significantly reduced the risks associated with ATM bombing attacks in South Africa.

Chapter 7. Example of Incident Processes, Procedures and Checklists

It is recognised that each ATM deployer will have unique organizational structures and relationships with third party service providers, such as Cash In Transit (CIT) companies and ATM vendors. The following example of procedures, processes and checklists are extracted and adapted from an ATMIA member with extensive experience in managing both gas and solid explosive attacks.

7.1. Process and Procedural Overview



7.2. Description

The description below starts at the moment the emergency successor is warned by CIT dispatch.

#	Action	Definition	Write down and take pictures

1	Central CIT Dispatch calls emergency successor CIT Security.	Message content:
		Short description situation:
		• Type of attack
		  • Action local police
		  • Action local security company
		  • Action taken by the Dispatch Centre
		• Location
		• Branch name
		• Name and telephone number contact local branch
			Write down message content.

	Central CIT Dispatch sends an email to bank.	Email content: • Short description situation • Type of attack • Name and telephone number emergency successor from CIT company • Branch name and location • Name and telephone number contact local branch	Send to mailing list at bank.
2	Emergency successor CIT calls contact at local branch.	• Report travel time • Emergency successor CIT gives first directions (see below)	
3	Emergency successor CIT moves to crime scene.	• Bring a camera • Depending on the situation, make arrangements for CIT to empty the ATM.	Write down the ETA of CIT (or let them call later).

#	Action	Definition	Write down and take pictures

4	On arrival at the crime scene:	• Find contact local branch.
		• Find commander on scene police/fire brigade.
		• Make an assessment of the situation together with the local branch contact:
		  • Is the location blocked with police tape?
		  • What was the form of attack?
		  • Are there and residents above or next to the attack location? How are the residents coping?
		  • Do you hear the CO2 alarm?
		  • Make sure the press / media stays outside the cordon.
		  • Describe the surroundings of the crime scene.
		  • Make a first estimate of the structural damage.
		• Arrange with the police when it is allowed to enter the crime scene.
			• Verify the name of the local branch contact and write it down.
			• Write down the names of the police representatives.
			• Take overview pictures.
			• Write down the situation overview:
			  • Type of branch: off premise or local branch
			  • Type of entrance to value room: via branch or via outside entrance (or stand-alone ATM)
			  • ATM through the wall or in vestibule
			  • Other cash equipment
			  • Describe the way the branch/ATM is situated: quiet/busy street, shopping area, crossing etc.
			  • Describe the location in relation to fast escape routes: motorways and back roads

5a	Make arrangements with the local branch contact.	• The local branch has to hire a local contractor to conduct emergency repairs. • The police is not allowed to leave the scene until CIT removes the cash from the ATM. • Make arrangements with the central dispatch about the alarm system reset. • The local branch has to make arrangements to repair the alarm systems. • Make arrangements with the local branch contact and the local spokesman. • Secure security camera footage and send it to fraud control at bank, sharing with the police in consultation with Fraud control.	Write down all the arrangements for the report.
5b	Report incident.	Local Branch or emergency successor reports the incident to the service desk for ATM and structural repair.	

#	Action	Definition	Write down and take pictures
6	Testimony witnesses	• What is the type, colour and license plate of the ramming car? • What is the type, colour and license plate of the getaway car? • How many persons? Description of criminals? Which language did they speak? Etc.	Write down information.

7	Inspect the outside of the building:	• Inspect fascia (front ATM) and take pictures:
		  • How has the gas/explosive been injected? Via the shutter, via a drilled hole, or via other openings in the fascia (like the card reader)?
		  • Damaged fascia
		• Inspect the entrance of the building/value room:
		  • How has the entrance been forced? By car, by ramming beam or pipe (welded to the chassis of the car)?
		  • Describe structural damage and estimate the repair costs.
		• Be sharp on other notable details.
			• Write down the damages.
			• Make a rough estimate of the repair costs.
			• Write down other notable details.

#	Action	Definition	Write down and take pictures

8	Inspection of the inside of the value room and ATM:	• **If possible, be the first to enter the room just after the forensic police have left!**
		• Reset the CO2 alarm before entering. Just to be sure.
		• Describe structural damage and estimate the repair costs.
		• Check the meter cupboard and the position of the electrical switches. Take a picture.
		• Estimate the ATM damage and determine the modus operandi.
		• When a gas attack has taken place and the door of the safe is still closed, bang with your fist on the door. If you hear shattered glass, the glass plate is damaged and it will not be possible to open the safe on the spot. You can call off CIT; the safe has to be transported to a secure location to be opened by a specialist.
		• Determine the ATM type and number.
		• If applicable, determine the gas neutralization system (open the canister safe):
		  • Seal still intact?
		  • What is the color of the seal?
		  • Is the gas canister valve open or closed?
		  • Tubes intact or cut?
		  • Is any ice accretion on the canister visible? Are there fluids beneath the canister when the ice has melted?
		  • Ticking relays yes or no?
		  • Check control light panel safe door.
		  • Reset gas neutralization system.
		• Just in case there's cash lying in the value room, collect, count and secure the bank notes. **It is important to stick to the four eyes / dual control principle while doing this!**
			• Write down a rough estimate of the repair costs.
			• Write down the actual content of the ATM (if counted).
			• Write down the administrative content of the ATM.
			• If possible, write down the losses.
			• Write down the results of the inspection of the gas neutralization system.
			• Take pictures of every relevant matter:
			  • Damages
			  • Machines
			  • Gas neutralization system
			• Write down the type of ATM and its number.

#	Action	Definition	Write down and take pictures
		• Check the content of the safe. Let the local branch check the administrative content of the banknote canisters in their system. • Secure the security camera footage and burn it on two DVDs (along with the player software) and send it to Fraud Control at bank. • Check the other cash machines for damage.	
9	Update by the emergency responder to CIT dispatch:	Short update containing damages to the ATM, structural damages, losses and other important details.	
10	CIT Dispatch sends second information email to bank (security) management and fraud control.	Content: • Damage to ATM • Structural damage to the branch and adjacent buildings • Losses yes/no?	Send email

11a	Final settlements	• If the safe door is closed, wait for CIT to open the safe. Inspect the inside of the safe for damage. • If the gas attack has succeeded, ask the CIT for a discharge form. • If the safe is damaged heavily and cannot be opened, the safe has to be transported to secure location to be opened by a specialist. The emergency responder calls the specialist. • A local contractor has to seal the location. Make sure the safe is empty! The contractor has to make an improvised passage so that entering the location is still possible! • If the alarm system is damaged, all the cash machines in the location have to be shut down and emptied by CIT. • The local branch has to inform the public that no service is possible and direct them to the nearest ATM. • When the results of the gas neutralization system inspection seem odd, the vendor has to be involved for research. A local branch contact has to be present when the research is conducted. Make sure the canister is weighed with a standard scale. • If the calamity is severe, central security management and fraud control have to be informed immediately. They will also inform the bank press officers/spokesperson. • Tell the local branch contact that the damage has to be determined by a qualified damage adjuster.	• Write down result of safe opening. • Send checklist and report to Security management and Fraud control.
11b	Settlements CIT	• CIT secretary sends the checklists to the bank Service organization. • Send the final report (including pictures) to bank Security Management and Fraud Control.	Checklist has to be sent before noon. The final within working hours, the same day.

7.3. Checklists

Common Data

Serial number	:		
Local Branch name	:		
Address Incident	:		
City	:		
Postal code	:		
ATM-number	:		
Date incident	:		
Day of the week	:		
Time of attack	:	Central Dispatch (alarm system)	
		CIT Dispatch	
		Local branch contact	
Situation branch	:		
Police region	:		
Duration attack	:		Minutes

Location Data

☒ Off premise

☐ Off premise stand-alone type 1

☐ Off premise stand-alone type 2

☐ Branch

☐ Property bank

☒ Property rented

ATM Type

- ☐ 5884
- ☐ 5885
- ☐ 5886
- ☒ 5887
- ☐ 6625
- ☐ Other: ……

Where has the gas/explosive been injected?

- ☐ Safe
- ☐ Top box
- ☒ Both
- ☐ Other: ……

Was there a blast?

- ☒ Yes, how?:……
- ☐ No

Gas neutralization system installed?

- ☒ Yes
- ☐ No

Did the gas neutralization system work properly?

- ☒ Yes
- ☐ No, reason:……

Is ice forming on the cannister or are melting fluids visible?

- ☒ Yes
- ☐ No

Color of the seal?

- ☐ Blue (CIT)
- ☒ Yellow (ATM vendor)
- ☐ White (Other vendor)

Has the seal been broken?

☒ Yes

☐ No

Has the gas neurtralization been reset?

☒ Yes, by:……..

☐ No, reason: ……

Safe door?

☒ Closed

☐ Open

Can the safe door be opened on the spot?

☒ Yes

☐ No

Has the cash been removed from the safe?

☒ Yes, by:……

☐ No

Is the safe to be checked?

☒ Yes, by: ……

☐ No, ……..

Is the ATM to be transported to a secure location?

☒ Yes

☐ No, reason: ……

Does the local branch wish to put the ATM in operation again (without an operational gas neutralization system)?

☐ Yes (be aware: this is for the risk of the branch)

☒ No

Has the local branch called in the incident correctly?

☒ Yes, to: ……

☐ No. Ask the local branch contact to do it still

Additional remarks:

Chapter 8. List of Best Practice Recommendations

ATMIA members concerned about preventing ATM gas and explosive attacks are advised to follow these best practices and recommendations:

- Enhance perimeter and building security to repel access to the security enclosure door side of the ATM:
  - *Strengthen building doors and locks*
  - *Install anti-ram raid bollards*
  - *Install and monitor Alarms and CCTV, ensuring installation of the video and alarm systems minimizes the risk of tampering by the perpetrators*
  - *Consider the use of dense security fog / security smoke protection*
  - *Post a notice at the site that enhanced security measures are in use*
- Detect attempts to insert explosives through the customer facing side of the ATM:
  - *Alarm grids or other sensors to protect dispenser shutter and surrounding area*
  - *Monitor for dispenser shutter being opened when it should not be open*
  - *Consult the ATM vendor about the availability of strengthened shutters and other solutions that could potentially prevent the introduction of a gas tube through the dispenser shutter*
  - *Consult the ATM vendor regarding minimising the aperture of shutters and the interface with ATM safe to reduce ease of inserting solid explosives*
  - *Activate local audio alarm (screamer) on detection of attack or detection of gas*
- Degrade notes using Intelligent Bank Note Neutralization Systems (IBNS):
  - *Include sensors that activate when gas is detected or there is penetration of the dispenser shutter or surrounding area*
  - *Include sensors to activate with explosive shock wave*
- Consider certified explosive gas resistant or solid explosive resistant security enclosures for new ATM deployments.
- Consider metal cages to inhibit removal of cash following an explosion.

- While the majority of such attacks occur during the quiet hours, educate staff and service vendors about activities that could be seen as a potential precursor to an attack, including suspicious individuals appearing to be focused on the ATM or damage to the ATM, as well as alerting staff and service vendors to be cautious of risk of injury.
- Install properly fitted steel plates over the cabling channels after cabling has occurred.
- Consider technologies that neutralize explosive gas:
  - *Gas detector activates non combustible suppressant*
    - *Ensure environmental safety measures such as CO2 detectors and alarms are operational in the ATM area*
  - *Perpetual or responsive electronic spark to prevent high concentration of gas*
- Manage cash balances in the ATM to the minimum required to minimize risk of loss in the event of a successful attack.
- Collect and analyze intelligence about attacks and regularly review suitability of solutions deployed:
  - *Consider migration from explosive gas to solid explosives,*
- Establish relationships with law enforcement to encourage rapid response.
- Create pre-defined processes, procedures and checklists for responding to and managing explosive attacks

Chapter 9. Further Reading and Links

ATMIA Best Practice Guides:

https://www.atmia.com/main/atmia-best-practices-library/

ATMsecurity.com search string for explosive related content:

http://www.atmsecurity.com/index.php?searchword=explosive+bombing&ordering=newest&searchphrase=any&limit=0&option=com_search

European Security Systems Association (ESSA)

http://www.ecb-s.com/_rubric/index.php?rubric=EN+Home