ATMSWG

Recommended

Physical ATM Security Guidelines

CONTENTS

DEFINITIONS

Dedicated ATM Room - A room which is constructed as a secure area to house ATM's where the cash carrier or site operator can securely replenish the ATM's. The ATM's are normally installed through a wall onto a public area (which may be within the building or out to a public thoroughfare). The access point to the room may be in a public area or via a secure area. Typical sites include shopping malls and bank branches.

Adapted ATM Room - A secure room which is suitably altered to provide the same facilities as above but will contain other functions such as cashiering, stock etc. Typical sites include petrol stations, shopping malls, bank branches etc.

Freestanding ATM - the ATM is placed with a public area which is used for other functions. There is no external unit around the ATM and physical protection is limited to the ATM itself. Access is typically from the front and these are often situated in convenience stores, supermarkets etc.

ATM Lobby – Similar to free standing except the space containing the ATM(s) is solely for that purpose. ATM service functions and replenishment will be from the front, ie within the lobby area and the lobby may be open (up to 24/7) for longer than the "parent" store.

ATM Sited Through Glazed Shop Front - ATM's are usually sited on the external fascia of a building giving public access to the ATM. All cash servicing takes place at the rear of the machine, and typically this will not be within a secure service area. Typical sites include bank branches.

ATM Sited Through a Masonry Shop Front - As for ATM's sited through glazed shop fronts but may also include a metal construction rather than masonry.

ATM Sited Within Unoccupied Premises - These are typically bank or building society premises which are closed pending disposal or refurbishments. A variety of ATM locations are possible.

Freestanding ATM with a Servicing Shroud - The servicing of the machine may take place when the public are present at the host site after a secure shroud has been extended around the ATM. Typical sites include retail malls, petrol stations and converted phone boxes.

INTRODUCTION

ATM Security Working Group. The ATM Security Working Group (ATMSWG) was formed in July 2001 to consider crime and security issues relating to the 'stand-alone' or 'freestanding' type of Automatic Teller Machine (ATM) normally operated by Independent ATM Deployers (IAD) in non-financial type premises. Since then it has been expanded to cover all ATMs and ATM operators including Banks, Building Societies and Independent ATM Operators

The success rate of ATM attacks is relatively low: only one third of attacks on successful. However, even when the attack is unsuccessful then collateral damage caused (eg. by explosives) to building structures is equally important. The success of a physical attack depends on a number of factors including an ATMs characteristic, the setup of an ATM attack and the experience and know how of the perpetrators.

The most vulnerable are through the wall ATMs which are situated outside or stand-alone ATMs which are mostly situated inside. ATMs situated inside and fixed in the wall are less vulnerable. When attacking an ATM inside, OCGs prefer ATMs situated in commercial premises over ATMs situated in bank premises where surveillance is typically stronger. Banks mainly operate ATMs located inside or outside a bank building. However, bank remote locations (bank remote) in the street or in the commercial premises of merchants such as petrol stations, supermarkets, hotels, casinos, airports, etc. are gradually becoming more important with bank branches being closed. Besides banks, also independent providers operate ATMs as a self-standing service without offering other banking services. Their ATMs are often located in retail locations, hospitality and leisure locations, transport locations (railway stations, airports, etc.), public buildings and in the street.

With the increasing popularity of online banking, many bank branches are likely to be closed in the coming years leading to an overall decrease in the number of ATMs.[3] However, this could entail an increase in the number of bank-remote ATMs and independent-provider ATMs located in more vulnerable locations.

The preparation of an attack can take up to several weeks or even months. Offenders need to collect the necessary tools and resources such as vehicles, equipment, establish the necessary contacts with persons supporting the crime and gather the necessary intelligence on the targets. Vehicles are an essential tool for physical ATM attacks; perpetrators mainly travel by car and after the attack they most often make their escape with fast vehicles. These are often stolen but can also be hired or purchased (e.g. via the internet). Most of the equipment for physical ATM attacks is readily and legally available in normal shops. This further lowers the threshold for stepping into this crime area. Tracing the origin of a tool is difficult for law enforcement so the risks for the perpetrators are limited.

OCGs often perform extensive surveillance to identify suitable targets; assess the time of day the ATM is filled, the surroundings of the ATM, the technical specifics of the ATM, the escape routes and the security measures that are in place, such as closed-circuit television (CCTV), alarm sensors and shutters.

Action are taken by OCGs to frustrate law enforcement before the attack. They tamper with

1.0 GENERIC CONSIDERATIONS

The minimum physical security recommendations in this chapter refer to the ATM itself, its host premises and the general movement of cash within the premises. The security of cash replenishment by Cash-in-Transit providers will not form part of the guidelines in this best practice manual for ATM physical security.

The security guidelines listed are recommended as crime reduction "good practice". They are designed to provide minimum security guidelines. Additional security measures and practices may well be required and will depend on existing local premises security and the assessed risk carried out prior to site selection and installation. These guidelines are intended to complement the advice of local police and government, insurers and security advisers, as well as the manufacturer's guidelines.

The crime reduction advice in this document is given free without the intention of creating a contract. The authors of these security guidelines do NOT take any legal responsibility for the security advice contained in these guidelines.

2.0 THE THREATS

These guidelines focus on the key issues, being:

2.1 Ram Raid/ Drag Out - A ram raid is an attempt to remove an ATM, and its contents, from its location, usually after battering through to the ATM with a motor vehicle. A ram raid involves an attempt to rip the ATM out of its position and remove it from its premises with the intention of breaking into the machine later to steal its cash. Ram raids often take place in the early hours of the morning in areas where police response times might be slower than normal. This type of incident invariably causes considerable damage to the premises and, often, to its contents.

2.2 ATM Burglary - An ATM burglary is when an ATM is broken into in-situ to steal its cash. The attack takes place on site and may be a traditional "safe breaking" method such as angle-grinders or oxyacetylene burning or perhaps as explosive attack using solid explosives or gas.

2.3 ATM Replenishment Attack - Where directly employed staff, merchant or CIT courier are attacked by criminals in the process of replenishing or dealing with cassettes within the machine. Attacks usually take place when the ATM safe is open to receive / remove cassettes, or when staff are transporting moneys through unsecured areas. These attacks usually place personnel under considerable duress or physical threat.

2.4 Gas Attacks – Attacks to the machine via the introduction of mixed gases which are ignited and exploded to specifically remove the rear door to gain access to the cash.

2.5 Solid Explosives – rarely seen in the UK at the moment but more so in Europe. The UK threat is from a method whereby powdered explosive is placed on a thin tray and put through the cash dispenser, more commonly known as the pizza slide and subsequently ignited.

2.6 Jaws of Life – Equipment legally used by Fire Service to expand and gain entry to premises are being stolen and utilised to force entry to ATMs.

2.7 Fascia Attacks – This is where the front fascia of the ATM is attacked with the intention to gain access to the top cash box.

Nb: Black Box/ Jackpot attack – This is where access is gained to the ATM via the front fascia. Perpetrators connect a remote PC to the ATM technical systems to override and subsequently de-cash the machine.

3.00 TYPES OF ATM DEPLOYMENT

Typical examples of ATM deployments include:

3.1 Purpose Built Standalone Site (Kiosk) - Typically sited in motorway services, shopping malls, retail parks, etc. They may be a proprietary security pod which is secured to a prepared concrete base and then given exterior finishes e.g. cladding or alternatively a purpose-built structure, typically constructed of masonry or metal. All cash servicing will take place within the secure unit. alarm systems and public lighting, use diversion techniques, set up roadblocks or attempt to tamper with law enforcement vehicles.

In recent years it has become clear that the risks associated with ATMs overlap all the various installation scenarios and therefore it was easiest to produce a single set of guidelines to cover all ATM locations. This document is therefore a combination and revision of these documents.

Site selection and installation of ATMs should always be preceded by risk assessments. During initial site validation, or at subsequent site risk assessment visits, an ATM should be classified by the deployer as Low, Medium or High Risk.

Risk assessment criteria can depend on organisational, insurance and law enforcement recommendations and requirements (e.g. Crime Prevention Offices, Crime Prevention Design Advisors or Architectural Liaison Officers). Industry advice may also be sought from industry approved consultants. It is not intended to give specific advice on the process of risk assessment in these guidelines, however, as a minimum. Such assessments should take account of:

- the safety of all staff, ATM users, and the public
- crime history of area and site itself, aided by local police intelligence
- general conditions of site, including lighting, proximity to other community services, visibility, access/ escape routes etc
- proposed positioning of the ATM within premises of selected site
- existing / proposed security measures on site
- cash replenishment model – own staff, merchant or CVIT Fill
- the cash rating of the security container fitted to the ATM employed or to be employed.

It is recommended that details of site risk assessments be recorded in defined reports and stored in an organisational database. Risk assessments will be tailored to fit the requirements of each deploying organisation.

Where CVIT couriers or merchants are involved in the replenishment process, they may also wish to undertake their own risk assessment, which will need to be used in conjunction with the deployer's assessment to ascertain the overall risk rating for the site.

It is also recommended that each ATM deploying organisation conducts a detailed and thorough ATM risk analysis for their own country, and geographical areas of operation, and that based on this,

a detailed ATM security strategy is prepared and up-dated on a regular basis, say every two years, or in response to emerging trends.

5.00 SITE PREPARATION

Contracts relating to ATM deployment should clearly define the party (or parties) responsible for the following actions:

- preparation of the site (including specified physical protection against Ram Raids)
- provision, installation, testing and commissioning of all security equipment
- provision of a dedicated telephone line (if required)
- the ATM Base preparation (as required)
- the electrical preparation (as required), including the provision of clean power.

6.00 INSTALLATION

Contracts relating ATM deployment should clearly define the party (or parties) responsible for the following actions:

- Installation, testing and commissioning of all security alarm equipment
- Installation, testing and commissioning of the Lock (testing and commissioning only if the lock is preinstalled by the ATM Supplier)
- Defining and ensuring compliance with all general Site Requirements
- Provision of all plans/documentation relating to the construction of the building and ATM Anchoring.

7.00 LIAISON WITH POLICE AND LOCAL AUTHORITY

It is strongly recommended that liaison take place with the local Police crime reduction department (may be Crime Prevention Officer, Crime Prevention Design Advisor, Architectural Liaison Officer or even local CSO) and the Local Authority in advance of submitting a planning application in order to obtain any site-specific information that may be relevant to the installation of the ATM.

8.00 INSURANCE

Before installation of an ATM the premises / business owner is strongly advised to inform their Insurer so that they can advise their minimum-security requirements for the premises in view of the additional risk presented.

9.00 SAFE

The security provided by the security container (safe) within the ATM should be to a level commensurate with that required for the value of cash loaded in the ATM, or to a level that meets

the deployer's documented minimum standard. Reference should be made to the relevant EN 1143-1 or UL 291 ATM security standards.

Where lower quality safes are the only option available (due to the fact that some ATM manufacturers will only offer their own preferred model of safe), then it may be appropriate to consider imposing a limit upon the amount of cash that may be loaded into the machine at any given time to reduce exposure / potential loss in the event of an attack against a lesser strength ATM safe.

ATM manufacturers offer a standard range of ATMs which have a number of safety features which are rated according to the European Committee for Standardisation (CEN) grades of security. Generally, ATMs have a CEN-marking ranging from the lower grade CEN1 to the highest, CEN4. Features such as body strength and resistance to attacks determine the grade. Gas resistance is mostly offered as an option (CEN-GAS).

9.01 Safe Type Recommended – High/Medium Risk Area

For higher risk locations, it is recommended that a minimum CEN 3 (or equivalent) safe be used. This can be lowered to a UL 291 Level 1 / CEN L safe used in conjunction with other, optional risk reduction measures where it is not possible to obtain such grade of safe from the ATM supplier.

9.02 Safe Type Recommended - Low Risk Area

For locations defined as lower risk it is recommended that a UL291 Level 1 / CEN L safe be used, in conjunction with other, optional risk reduction measures as identified via the risk assessment process.

10.00 ATM LOCK INSTALATION - SECURITY CONTRACTOR

For installed ATMs where a Bank requires a Time Delay / Time Lock, the Bank's security contractor should fit it in accordance with the manufacturer's requirements. It should then be connected to an appropriate alarm system with monitoring via an ARC and a test made. For ATMs supplied with locks which have external alarm monitoring capabilities, the lock should be connected to an appropriate ARC and a test made.

If there is a requirement to monitor the status of a remotely monitored lock, it should be monitored from an appropriate ARC 24 hours daily. The ARC should automatically generate an alarm signal if the telephone line fails or is cut. The ARC should be able to monitor the functionality required by the ATM deployer e.g. lock open/closed, time access windows.

11.00 ALARM EQUIPMENT INSTALLATION - SECURITY CONTRACTOR

All equipment should be correctly fitted in accordance with the manufacturer's specifications. Once the equipment has been fitted a live test of each item mentioned above must be conducted and a check made that the ARC picked up each signal.

12.00 INTRUDER ALARM SYSTEM - PREMISES

The premises should be protected by an intruder alarm system with monitored remote signalling to an ARC to a security level commensurate with the risk level:

- The system should qualify for the required local police response
- If it is a "confirmable" alarm system, a dual signalling facility should be provided
- The system should be designed to give the earliest possible warning of potential / actual attack on the ATM
- Consideration should be given to including personal attack alarms in the system
- A maintenance record should be kept for the alarm detection system and routine maintenance should be conducted. The minimum should be one planned maintenance visit each year (dependent upon the grade of system installed).
- Reference to the relevant BS/EN Performance Standards will be necessary.

13.00 INTRUDER ALARM SYSTEM – ATM

In addition to alarming the premises consideration should be given to alarming the ATM itself. This can be achieved by means of a stand-alone alarm system with its own unique reference number (URN) or may be a separate area of the premises alarm system. This will be jointly determined by the site host and deployer (who, in some circumstances, will be the same organisation):

- The system should be monitored by remote signalling to an ARC and should qualify for an appropriate local police response.
- If it is a “confirmable” alarm system a dual signalling facility should be provided. The design should ensure that the system is armed at all times other than for maintenance, for servicing and cash replenishment.
- It should give the earliest possible warning of attack on the ATM
- Consideration should be given to including personal attack alarms for the use of CIT crews / replenishment staff in the event of an attack during cash replenishment.
- A maintenance record should be kept for the alarm detection system and routine maintenance should be conducted. The minimum should be one planned maintenance visit each year (dependent upon the grade of system installed).

14.00 ALARM EQUIPMENT

The following alarm equipment is recommended for installation at each ATM location:

- Seismic Detector / Stress Detector. A seismic / stress detector should be fitted to the ATM safe body and safe door.
- Magnetic Contact A dual reed magnetic contact switch should be fitted to the door of the ATM Safe.
- A dual reed magnetic contact should also be fitted on the door of the ATM Secure Service Room (if provided). This should be on a different circuit to the alarms fitted to the ATM safe.
- A Volumetric Detector should be placed on the wall of the ATM Secure Service Room. This should be able to detect any movement in the area surrounding the ATM. This should be on a different circuit to the alarms fitted to the ATM safe.

- If the Bank Branch has a cellar, which is under its direct control, a volumetric detector should be fitted to cover the area underneath the ATM anchoring.
- Personal Attack Alarms should be fitted in the ATM Secure Service Room as close as possible to the ATM. This is to provide protection to staff servicing or replenishing the ATM. If ATM's are in a public area, then consideration should be given to installing a radio based Personal Attack Alarm, such that staff can be issued with portable devices.
- Alarm Control Panel(s) should be fitted in the immediate vicinity of the ATM where necessary. If access control is used to secure the room, then an additional panel does not need to be fitted at the room door.
- Access Control, where possible, access to the rear of the ATM should be restricted and a door swipe or keypad system should be used to control the ATM secure Service Room door.
- Heat Sensor A heat/smoke sensor should be fitted inside the ATM. This should detect any form of oxy-acetylene or burning bar attack on the ATM and should be on the ATM security circuit.

15.00 CONTROL & MONITORING

15.0 Alarm Receiving Centre (ARC). The alarm system should be monitored from an ARC 24 hours daily. The ARC, which should conform to ISO and local police standards, should automatically generate an alarm signal if the telephone line fails or is cut. In the event that an alarm signal is received, the ARC should respond according to its standard operating procedures.

15.2 Response. In the event of an alarm the ARC should be able to request a response from a third party to visit the ATM within an agreed (ideally contractually binding) time period.

15.3 System/Line Failure. In the event that the alarm detection system fails to operate for any reason, or there is a fault in the telephone line, the ATM should be cleared of all cash until such a time as the system is operational and has been tested. Attacks on these systems are often a precursor to an attack.

16.00 CCTV

Should the site risk assessment require it, the premises may be protected by a CCTV system, with or without detection facility, viewing the ATM, but not viewing the ATM keypad. As a minimum, CCTV should be digitally recorded and, where risk dictates, may be remotely monitored by a third-party ARC.

In the case of a street-based ATM, this should be located in an area where a public CCTV system operates.

When an ATM is located in an area where a public CCTV system operates, the deployer or agent should liaise with the agency responsible for the CCTV system to include the ATM site in any pre-set automatic camera settings or to request regular sweeps of the site. The CCTV system should not be able to view the ATM keypad thereby preventing observation of PIN entry.

17.00 PASSIVE COMPLIANCE

In the event of an attack during opening hours, staff should be advised to passively comply with the raiders' demands and must be trained accordingly.

18.00 PIN PROTECTION

For locations deemed to have a high risk of ATM fraud, it is recommended that a written siting policy be submitted, subject to audit, confirming that the ATM is positioned to prevent oversight of the PIN pad from any source (cardholders in the queue, passers-by, mirrors, etc).

19.00 ATM LIGHTING

Where a national standard for illumination of the keyboard and surrounds of an ATM does not exist, an ATM Deployer should set its own standard. 200-300 Lux is recommended for ATM keyboard illumination. 50 Lux is suggested as the minimum ambient illumination at floor level up to a distance of 1 metre from the face of the ATM and extending 75 cm either side of the mid-point of the ATM. This is also the minimum level recommended should a CCTV camera be fitted. 200 Lux ambient illumination at floor level should be considered in areas deemed to pose a higher risk to customers at night.

20.00 ANCHORING (REFER TO APPENDIX 1)

21.00 FREE-STANDING ATMS

Free Standing or Stand-Alone ATMs are not installed in the wall of a building, for example, at a bank branch. Typically, they are situated in convenience stores, petrol stations, supermarkets, shopping malls, etc.

The security guidelines distinguish, where necessary, between:

- ATMs regularly filled with cash by the premises' owner (the 'Merchant Fill' cash replenishment model). The merchant will retain ownership of the cash and in most cases the risk will sit with them.
- ATM's filled with cash by the ATM supplier, who uses a Cash and Valuables In Transit (CVIT) provider to replenish the ATM (the 'CVIT Fill' cash replenishment model) and the risk will sit with the ATM operator or CVIT company depending on the circumstances.

21.1 Location. The ATM should be sited within the premises well away from perimeter glazing, particularly shop fronts, preferably directly against a strongly built internal or perimeter wall, which does not have vehicular access to its external face and positioned to avoid a direct and unimpeded line of access from a door or other access point.

To reduce the risk of vandalism to the ATM and to increase user safety, the ATM should be positioned in a highly visible and well-lit area that allows maximum surveillance by counter staff and other customers.

21.2 Security Measures. Once the ATM has been securely positioned on the premises and correctly anchored, it is important to decide on which additional security measures listed below will be

required to counter the risks highlighted in the assessment. It is essential to implement the appropriate level of security as determined by the risk assessment.

21.3 Cash Removal and Replenishment for Merchant Fill ATMs.

- Fill the ATM with cash sufficient for one day/session trading only
- Remove cash from the ATM at the end of trading to a safe of adequate security quality sited within the premises. This should be done with the premises locked and customers excluded
- Leave the door open to the ATM, and security container (safe) within, when the premises are non-operational.
- Merchant-fill ATMs require 'line of sight' from the outside of the premises in order for the would-be offender to see clearly that the ATM has been de-cashed outside of business hours
- Replace cash into the ATM with the premises locked and customers excluded prior to opening for the next period of trading
- Place notices prominently around the perimeter of the premises and on the ATM stating that the ATM holds no cash when the premises are non-operational

21.4 Cash Removal and Replenishment for CVIT Fill ATMs

It is good practice that the premises should be locked, and customers excluded during replenishment; or, alternatively, it is recommended that a full enclosures security kiosk/area should be provided for CVIT staff during removal/replacement of cash

- Cash removal/replenishment should take place in accordance with the CVIT Company's procedures, a copy of which should be provided upon request.
- This is of particular importance dependent upon liability for the cash inside the ATM and a clear liability statement is required.

21.5 Maintenance of ATMs When an ATM is being serviced, if access to the safe is required, it is good practice to remove the cash during the service, locking the premises and excluding customers while the cash is being removed and while it is being replaced into the ATM, unless a security area or surround secure kiosk is provided.

Whilst the service is being undertaken, the cash should be temporarily transferred to a locked safe of adequate security quality for the risk involved

21.6 Key security for CVIT Fill ATMs

For CVIT Fill ATMs, signs should be prominently displayed on the ATM and within the premises indicating that there are no keys available on the premises to allow access to the contents of the ATM. It is likely that the CVIT carrier will provide their own PIN operated lock with rolling code encryption, rather than relying on physical keys.

22.00 RECOMMENDED ADDITIONAL SECURITY MEASURES FOR HIGHER RISK DEPLOYMENTS

22.1 External Measures External approaches to the area of the premises where the ATM is sited should be protected by the installation of anti-ram bollards, vehicle-arresting systems, high rise kerbs, raised planters, reinforced lamp posts or similar street furniture, usually subject to local authority approval.

Where perimeter glazing extends down to the floor of the premises this should be protected by visually permeable metal roller shutters, security grilles or retractable anti-ram bollards configured to keep vehicles away from the vulnerable perimeter elements of the premises outside the premises operational hours, for example, when the removal of the ATM from the premises is considered a risk, or when the area is more risky from a crime history point of view.

Where perimeter glazing cannot be protected in this way – e.g. premium retail unit or planning approval is not received – the use of enhanced anchoring systems to prevent uplift and removal should be considered.

22.2 Enhanced Anchoring. Instead of the anchoring system recommended in Generic Considerations the ATM should be anchored by an enhanced anchoring system specifically designed to provide superior fixing for ATM's.

22.3 Anti Ram Protection. Can be fitted where ram raid attack to remove the ATM, is considered a risk. This protection might take the form of a purpose designed anti-theft plinth, chain anchoring systems or other enhanced anchoring / fixing.

Where such devices are deployed these should be attached to the main body of the ATM safe itself and not to the exterior facings.

22.4 Tracking System. Advances in technology have made tracking systems a viable method when protecting ATMs, enabling its position to be determined and monitored by Police and commercial operators in the event of theft from the premises. Assisting in arrests and recovery of stolen property.

22.5 Intelligent Banknote Staining (IBNS). IBNS is installed and when activated renders the banknotes unattractive to thieves. With the recent introduction of polymer banknotes, the need to consider methods other than dye and stains is important. Other products such as glue and complete note destruction are being developed and should be considered. The IBNS should be designed to activate immediately the ATM is moved or attacked by any means. If required the system may incorporate a unique chemical identifying system, although such identification systems should not be used in isolation. Where a banknote degradation system is utilised notices to this effect should be displayed prominently around the perimeter of the premises and on the ATM itself.

An independent test house should check any banknote degradation system used and should certify that it does operate according to the manufacturer's claims. Such a system should meet any national standards relating to usage of ink/dye systems. Each national Central Bank should also test the system on real banknotes and should verify that the ink is safe, and that the required percentage of notes, are stained on the required percentage of the printed area. Some banknote degradation systems can link with CVIT to provide end-to-end security between the ATM and the cash centre.

22.6 Fogging System. As an alternative to a banknote degradation system, a smoke generating system may be installed to protect the internal area of the premises where the ATM is installed to provide a deterrent to theft of, or from, the ATM. Such systems should be designed to activate immediately the ATM is moved or attacked by any means. The means of activation must be provided only when the area of the premises in which the ATM is sited is non-operational. Such systems must not negate any procedures associated with fire and emergency, particularly in means of escape in the case of an actual fire. It is recommended that advice be taken from the local fire safety officer

before installation. Where such system is utilised, notices to this effect should be displayed prominently around the perimeter of the premises and on the ATM itself.

22.7 Unique Chemical Taggant. A Unique Chemical Taggant system may be installed. The system is a water-based spray containing a unique chemical identifying agent which stays on skin, clothing or materials and can be used by police to associate a person with a crime if they are in custody. Such identification systems should not be used in isolation. Where a system is utilised notices to this effect should be displayed prominently around the perimeter of the premises and on the ATM itself.

These systems can be fitted to the premises or to each ATM cassette, to provide a deterrent to theft of, or from, the ATM. The system should be designed to activate immediately the ATM is moved or attacked by any means or can be activated by personal attack alarm activation to guard against replenishment attack.

22.8 Cassette Interlocking. Physical interlocking of cassettes within the ATM safe to prevent removal of more than one cassette at any given time and usually incorporating a time delay between each cassette removal. This is designed to deter replenishment attack and, in the event of such incident, reduce potential loss exposure to the contents of one cassette.

22.9 Gas Protection. At sites which may be considered at high risk of explosive gas attacks then specialist gas detection and neutralisation systems may be deployed. A Gas Protection Unit (GPU) neutralises the introduction of gas into the machine therefore preventing explosion. The system should be effective against repeated attacks (i.e. allow for more than one activation). Fogging systems may also be effective.

22.10 Solid Explosive. Solid explosives are harder to detect. The speed of the explosion makes it more difficult to prevent. Therefore, enhanced physical protection should be considered.

23.00 THROUGH THE WALL ATMS (TTW)

A TTW ATM does not stand on its own but is installed within the wall or perimeter glazing of a building (interior or exterior) to which it is affixed to allow customers to conduct transactions at the ATM outside of, or even away from, a bank branch. Many of these machines are ‘bunkered’, meaning they are contained within a wall that is part of a lockable room, providing access to the rear of the ATM during cash replenishment, although some are serviced in public areas.

This type of machine contrasts with free standing ATMs, which are not fixed within the perimeter wall or glazing of a building. The ATM is affixed to the floor at its location. Free standing ATMs are also known as ‘lobby’ or ‘pedestal’ ATMs.

For the purposes of cash replenishment, the assumption is made that cash replenishment will be conducted by Bank Branch staff, not by an external service supplier. For TTW ATMs installed at other types of locations (hypermarkets, petrol stations etc) and requiring cash replenishment by a commercial security organisation, please refer to Stand Alone ATM’s section of this document.

24.00 STREET-BASED ATMS

Street-based ATMs are typically in public telephone kiosks and columns/pods situated on public footways. Unless otherwise stated the advice contained in this document relates to both ATMs in telephone kiosks and in columns/pods.

With the advent of the mobile telephone in recent years the use of public telephone kiosks has significantly reduced. In order to optimise the efficient use of these existing structures a number of ATM deployers have developed an innovative business model to utilise telephone kiosks as ATMs. Telephone kiosks offer a combination of three features that make them ideally suited for conversion to ATMs - publicly convenient locations, electricity and communications.

24.1 Columns/Pods. These are stand-alone structures of varying shapes and dimensions that house an ATM and in some locations Web/Internet connection facilities. These structures have typically been situated in car parks and other open locations to which the public have access and, more recently, on public footways.

24.2 Location/Position of Street-based ATM.

The street-based ATM should be positioned in a highly visible, well-lit area that provides maximum casual surveillance by the general public and allows the replenisher or service engineer rapidly to survey the immediate area.

In the case of columns/pods, the ATM should be positioned to take advantage of any existing street furniture such as railings, high-rise kerbing, raised planters, lamp posts, etc., which may offer a deterrent against ram-raid type attacks.

The ATM should be located in an area served by wide footpaths or thoroughfares that do not unavoidably funnel pedestrians into close proximity with ATM users.

Ideally, the ATM should be located away from bus stops, pedestrian crossings, or other features where the public may have a legitimate reason to gather or loiter.

Ideally, the ATM should be located as far as possible from doorways, recesses, passageways, secondary roadways, shrubberies, hoardings or other features that may conceal a potential threat such as hidden long-range surveillance equipment or a criminal hiding from view.

The ATM should be positioned to prevent physical observation of PIN entry from adjoining telephone kiosks or payphones. Telephone leads in adjacent telephone kiosks or payphones should be shortened to prevent observation of PIN entry from these. Where necessary, the door hinges of adjacent telephone kiosks should be reversed in order that payphone customers exit away from the ATM user.

The ATM should be positioned to allow the replenisher’s vehicle to park in the immediate vicinity and avoid an unnecessarily long distance to walk between the vehicle and the ATM, in addition to allowing constant line of sight between the replenisher’s vehicle and the ATM.

In consultation with the replenishing company, the deployer or agent should liaise with the appropriate authority to request that a parking area adjacent to the ATM be restricted for use by the replenishing company.

24.3 Sounders and Flashing Warning Lights. The street-based ATM should be installed with an audible alarm sounder and/or visual flashing warning light to indicate when the ATM is under attack and attract the attention of the public and assist police in positioning the exact location of the ATM.

The sounder and/or warning light should be automatically disarmed during replenishment and servicing and automatically re-armed when replenishment / servicing is complete.

24.4 Anchoring.

The street-based ATM should be securely fixed to a specifically designed anchoring system or concrete base through its security container by a minimum of four high tensile M16 bolts with appropriate washers of 6mm minimum thickness. When fixing into a concrete base it is recommended that these bolts should be to a minimum depth of 150mm and that either resin anchor bolts or expanding anchor bolts are used to adequately anchor into the concrete.

In addition to the anchoring system recommended above, the ATM should be secured with a restraining chain that is bolted to the anchoring system using a high tensile anchor fixing, connected through the rear of the ATM and attached to the security container using a high tensile bolt with double nut and washer.

24.5 Bollards

In addition to the anchoring system recommended above, approaches to the ATM should be protected by the installation of anti-ram raid bollards, vehicle arresting systems, high-rise kerbing, raised planters, reinforced lamp posts or similar street furniture. These will usually be subject to local authority planning authority.

24.6 Armoured Anti-Bandit Shroud

As an alternative to a banknote degradation system, the ATM should be fitted with an armoured anti-bandit shroud to provide a deterrent to theft and to enhance the safety of operatives during replenishment or servicing.

24.7 Servicing of ATMs

In the event of an ATM needing servicing in the absence of an armoured anti-bandit shroud and subject to the second paragraph of this item, the use of cash in transit services should be employed to secure the ATM cassettes when a service engineer needs access to the ATM security container.

25.0 CUSTOMER SECURITY

Many of the principles will have been covered above as the requirement s for the security of the ATM and CVIT crews are often identical to that of customers using the machine however there are a number of additional considerations. It should always be borne in mind that many ATM users are less physically able and confident than CVIT crews, for example, and may find gangs of youths etc threatening and uncomfortable.

25.1 Defensible Space

Defensible space ground markings should be employed at the front of the ATM, to indicate only one ATM user at a time may enter the space. These will usually be subject to local authority planning authority.

25.2 Concealment opportunities

Potential assailants will often look for areas where they can either lurk without being spotted or can loiter without causing suspicion. Therefore, blind corners, alleyways, large bushes or trees should all be considered when surveying the ATM's location. In addition, areas where "legitimate loitering" occur should also be considered, for example bus stops, convenience stores, fast food restaurants as well as nearby public seating /street furniture.

25.3 Escape Routes

Potential attackers will often choose the location of their attacks on the basis of suitable escape routes. Consideration should therefore be given to alleys, access roadways, nearby waste ground etc which are close to an ATM which would give assailants an easy opportunity to escape.

25.4 Seek local advice

The advice of Crime Prevention Design Advisers and Architectural Liaison Officers should be sought as appropriate. In addition, organisations such as Secured by Design[1] can be approached as well

26.0 TEMPORARY RISKS

ATM operators, CVIT crews and engineering staff should always be aware of and report any changes to an ATM's environment which could lead to additional risks. This may include restrictions to access, changes to lighting or other environmental factors or nearby /adjacent premises becoming vacant. In addition, one of the biggest risks is the nearby availability of building plant and equipment such as diggers and JCBs. If these are in the area then serious consideration should be given to additional security features, up to and including de-cashing the ATM during high risk periods such as at night.

Further information on European Standards can be accessed via the Europol website with reference to Preventing Physical ATM Attacks document 2019.

[1] http://www.securedbydesign.com/index.aspx

Effective approach to preventing physical ATM attacks

Situation Assessment

Identify the risk profile of ATM
Work with stakeholders and partners and work in collaboration
Use all information available in relation to physical attacks

Preventive approach

Identify the main risks and priorities
Identify the best preventative measures to cover the risks
Identify parallel measures needed to strengthen the preventative measures taken

Preventative measures

1. **Reduce the reward**

Lower the cash holding
Empty ATM at night
Increase the number of replenishments
Consider Note degradation (IBNS)

2. **Increase the risk**

Use of CCTV
Use of shared Forensic data
Identify re-offenders
Early and real time detection of possible attack
Review punishment and sentencing for offenders

3. **Target hardening**

Review location of ATM
Introduce prevention products (GPS, fog, IBNS, CCTV etc)
Identify physical obstacles and surveillance
Physical structures around machines

Parallel measures to strengthen the preventative approach

Effective legislation including preventive measures against physical ATM attacks, consequential sentencing etc.
Effective media strategy
Strong collaboration between stakeholders and partners both private and public sectors in the fight against physical ATM crime
Be aware of the possibility of collateral damage and the effects on the community.

APPENDIX

ANCHORING

There are a number of methods of anchoring. The appropriate method will be determined by the nature of the deployment and the perceived risk as identified through the risk assessment process.

20.1 Basic Anchoring. The ATM should be securely fixed to the floor through its security container by a minimum of four resin anchor bolts (minimum 16mm diameter to a minimum depth of 150mm) into a substantial concrete base.

Where a timber floor is involved the ATM should be bolted to a steel base plate by a minimum of four bolts, which is bolted through the floor joists by a minimum of four bolts. When anchoring, reference should be made to the manufacturer's guidelines.

20.2 Base Composition. During the Site Validation an assessment should be made of the base to ensure that it is of sufficient strength and depth to anchor the ATM. It is recommended that screed is not included in any measurements of base depth.

20.03 On Solid Ground - Use Existing Base if it is deemed possible to use the existing base, the existing concrete should be reinforced and of a minimum depth of 15cm to meet the requirements of the anchor bolt manufacturers. The ATM can then be anchored directly into it.

20.4 On Solid Ground - Plan for New Base. If it is not possible to use the existing base without modification, then arrangements should be made to strengthen the base. A minimum depth of 15cm reinforced concrete should be retained with the existing base, in order to anchor the new base to it.

20.5 ATM Plinth – the Plinth Type required for the ATM to be properly anchored it should be able to sit on a plinth that will enable it to exactly reach the required height. When deciding on an ATM plinth, ATM deployers should assess its construction from a security perspective. Plinths specially constructed to withstand 'ram raids' and other brute force attacks may be considered for higher risk locations.

20.6 Anchoring ATM to Plinth. For installers using CEN approved plinths, the anchoring arrangements should be those that are approved in the CEN documentation for that product. The correct implementation of those arrangements will guarantee good anchoring.

20.7 Anchoring Plinth to Base - No Cellar – Sufficient concrete. This assumes that the ATM will be anchored into solid ground with sufficient concrete. Sufficient concrete is reinforced concrete to a minimum depth required for the length of bolt used. For details of required depths it is recommended to consult the handbooks of the major anchor bolt manufacturers e.g. Hilti.

20.8 Anchoring Method - Installation Contractor. The installation contractor should anchor the ATM in accordance with the relevant CEN (or other) standard relating to the grade of safe used.

20.9 Anchoring Certificate - The Installation & Maintenance Contractor should complete a Certificate stating that the anchoring has been done in accordance with these requirements. All exact measurements relating to the anchoring should be recorded. A copy of this Certificate should be passed to the ATM deployer for audit purposes.

20.10 Anchoring Plinth to Base - No Cellar – Insufficient concrete. This assumes that the ATM will be anchored into solid ground with insufficient concrete. Insufficient concrete is concrete that is not

reinforced and does not meet the minimum requirements of the anchor bolt manufacturers. When this is the case a concrete base should be constructed and properly attached to the existing floor.

20.11 Base Preparation - when preparing a base the Building Contractor should follow the minimum requirements of the anchor bolt manufacturers. Guidelines for the preparation of a 30cm base are as follows:

- the base should be constructed using as standard two U-sections (UPN 160 - 160mm x 65mm x7.5mm). Larger U-sections may be used depending on the required height of the base
- a minimum of 16 x Steel (BE50) Rods (4x4) should be used to anchor the base to the floor. These Rods should be 12mm diameter. They should be anchored into holes drilled to a depth of 8cm and with a diameter of 16mm
- anchoring must be done using HILTI Chemical Paste HIT-HY 150
- a Steel Grid (BE50 - 150mm x 150mm x 8mm x 8mm) must be constructed to lie on top of the Steel Rods
- the existing floor surface must be roughened and wetted concrete (Class C40/50) must be poured into the construction, which must meet a crush resistance of 35N/mm2 after 7 days.

20.12 Base Construction Certificate - the Building Contractor should provide a Certificate stating that the Base has been constructed and anchored in accordance with these requirements. A copy of this Certificate should be passed to the ATM deployer for audit purposes.

20.13 Anchoring Method - the installation contractor should anchor the ATM in accordance with the relevant CEN (or other) standard relating to the grade of safe used.

20.14 Anchoring Certificate - the Installation Contractor should complete a Certificate stating that the anchoring has been done in accordance with these requirements. All exact measurements relating to the anchoring should be recorded. A copy of this Certificate should be passed to the ATM deployer for audit purposes.

20.15 Anchoring Plinth to Base over a Cellar. If the ATM is to be anchored over a cellar/basement/garage to which the public may or may not access, and for which entry/egress control may or may not be under the direct control of the Bank, or other TTW ATM deployer. After the Site Validation visit, the ATM Deployer Security Representative should approve the proposed anchoring plan.

20.16 Installation in Solid Wall. If accessible from an area with vehicular access, the ATM should, if possible be installed behind a solid brick or concrete wall. If one does not exist, it should be constructed. If this is not possible, the options laid down under “Steel Section Wall” and “Steel Girders (HEB-100 Sections) below should be followed, and should be approved by the ATM Deployer – Security Department.

20.17 Wall Construction - the Building Contractor should construct a wall that must be at least 14cm thick and with a mass of 1,900 kg/m3. Any deviations from the above should be cleared with the ATM Deployer before installation takes place, and should be shown in the Construction Certificate.

20.18 Wall Construction Certificate - The Building Contractor should provide a Certificate stating that the wall does comply with the required standard and stating the exact composition and depth of the Wall. A copy of this Certificate should be passed to the ATM Deployer for audit purposes.

20.19 Installation in Steel Section Wall. In the event that it is not possible to install the ATM behind a brick or concrete wall, then the next preferred method is to install it behind a solid steel section.

20.20 Steel Section Anchoring to Floor - The Building Contractor should anchor the steel section to the floor as follows:

- Use a minimum 4 x M10 Chemical Bolts HVY (Hilti)
- Anchoring only to be done in concrete - minimum depth 9 cm.
- Hilti anchoring requirements should be mandatory
- Non-destructive quality control of the anchoring should be made (resistance up to 25-35Nm)

20.21 Steel Section Anchoring to Ceiling/Walls – the Building Contractor should anchor the steel section to the ceiling/walls as follows:

20.22 To concrete ceiling

- Minimum 4 x M10 chemical bolts HVY (Hilti)
- Anchoring only to be done in concrete - minimum depth 9cm.
- Hilti anchoring requirements are mandatory
- Non-destructive quality control of anchoring to be made (resistance up to 25-35Nm)

  To beams. The anchoring must be done directly into the Beam. If required a 'bridge' can be made using a Profile 60mm x 60mm x 4mm, to be anchored with 4 x M10 bolts.

  To walls. Anchoring must only be done in the mortar between the bricks with chemical bolts M10 HVU HAS (Hilti)

  There must be 2 x M10 Bolts every 50cm with a minimum depth of 9cm. In the corners, top and bottom, a 15cm x 15cm steel plate must be used.

  In cement blocks 1 x M10 bolt with injection of HIT+HY20 must be used, with the anchoring at least 15cm from the edge of the block.

20.23 Steel Girders (HEB-100 Sections). In the event that it is not possible to install the ATM behind a brick or concrete wall, or a steel section, then the next preferred method is to install it behind steel girders.

20.24 HEB-100 Section Construction - the Building Contractor should ensure that HEB-100 sections (or equivalent) are used for the frame as follows:

- The HEB-100 sections should be installed on both sides of the ATM
- The distance between the base sections must not exceed 1.25 Metres (and must be as small as possible)
- If telescopic hollow sections are used, both sections must overlap for at least 50cm.
- 2 x Cross sections (hollow section casing profiles 80mm x 60mm x 6mm) must be attached to the H-Sections, above and below the outer edge (or 'nose') of the ATM.
- Each Cross section must be a hollow section of 80mm x 60mm x 6mm.

20.27 HEB-100 Section Anchoring To Floor – the Building Contractor should anchor the HEB-100 section to the floor as follows:

- Use a minimum 2 x M10 Chemical Bolts HVY (Hilti)
- Anchoring only to be done in concrete - minimum depth 9 cm
- Hilti anchoring requirements should be mandatory
- Non-destructive quality control of the anchoring should be made (resistance up to 25-35Nm)

20.28 HEB-100 Section Anchoring to Ceiling – the Building Contractor should anchor the steel section to the ceiling as follows:

To concrete ceiling

- Minimum 4 x M10 chemical bolts HVY (Hilti)
- Anchoring only to be done in concrete - minimum depth 9cm
- Hilti anchoring requirements are mandatory
- Non-destructive quality control of anchoring to be made (resistance up to 25-35Nm)

To beams

- The anchoring must be done directly into the Beam
- If required a 'bridge' can be made using a profile 60mm x 60mm x 4mm, to be anchored with 4 x M10 bolts