

SECURITY

Reduce the impact
of crime on business





Contents

- Introduction2
- Understanding crime: Know your risks4
- Prevention and protection: Secure your business5
- On the money: Look after your cash6
- Lock up: Secure your premises 9
- Electronic security: Beyond the physicals.....13
- Help from AXA Insurance16

The information contained within this document is intended as a general guide only and is not necessarily comprehensive. You should seek appropriate professional advice when devising any risk assessment or management programme. AXA Insurance will not be liable for loss or damages arising, in contract, tort or otherwise, directly or indirectly from the use of or reliance upon any information contained in this document.

Introduction

This guide is designed to help small businesses protect themselves from the effects of crime. The practical help and advice it offers is drawn from AXA's unique insight into crime against businesses, based on:

- Data from the UK's only quarterly measure of business crime - the AXA Business Crime Index.
- AXA's practical experience of helping small businesses to cope with the effects of crime.

The AXA Business Crime Index

In 2003, AXA became the first insurance company to share details of business insurance claims for loss through crime - the basis for the AXA Business Crime Index - and has continued ever since. The index is based on an analysis of trends in the level and types of crime committed against British business from up to 20,000 insurance claims made every quarter.

The statistics generated by this analysis represent a comprehensive survey of business crime in the UK and can be tailored to cover whole regions or single postcode areas. The AXA Business Crime Index is calculated quarterly to help small businesses identify the key threats posed by crime, and secure their businesses accordingly.

AXA Business Security Guide

This guide is designed to help small businesses do just that. It draws on a wealth of experience within AXA, which deals with many thousands of crime-based business insurance claims every year. In particular, AXA has a valuable insight into the security flaws that could encourage criminals to target your business.

Accordingly, the AXA Business Security Guide sets out best practice security measures for small business that could:

- Discourage criminals from targeting your business.
- Minimise losses and disruption should the worst happen.
- Help you to manage your insurance premiums.



Understanding crime: Know your risks

The first step in minimising your exposure to crime is to understand the risks you face. Clearly risks vary according to geographical location and line of business, so it always pays to contact your local crime prevention officer for advice specific to your circumstances. You may be familiar with utilising the formats of risk assessment and this can be suitable for security and crime protection to take into account all factors likely to have an impact on security.

However, the AXA Business Crime Index 2013 highlighted a number of crime related risks that all small businesses have in common.

The most common crime committed against business remained as theft in 2013, accounting for around three quarters of all crime against small businesses. The average cost of business theft claims is around £4,000.

In terms of the likelihood that they will affect small businesses, three types of crime dominate:

- Theft: Break-ins and theft pose a significant threat to the success of small businesses - for instance, through damage to or theft of critical equipment. According to the AXA Business Crime Index theft accounts for around 75% of crime against businesses.
- Malicious damage: Whether it's a result of vandalism or carried out by disgruntled staff, malicious damage to premises, products and equipment can cause significant business disruption. According to the AXA Business Crime Index malicious damage accounts for around a quarter of crime against businesses.
- Robbery is sadly also a feature of crime which involves threatening, perceived or actual physical assault resulting in loss of property or cash.

Any small business seeking to reduce its exposure to risk from crime should start by looking at measures to prevent theft, malicious damage and arson. Clearly, there is a social dimension to this, and AXA would encourage small businesses to get involved in initiatives designed to reduce the incidence of crime in their communities.

AXA also strongly recommends that small businesses review their security arrangements to ensure that they meet best practice standards, and provide the business with the protection it needs. The following pages in this guide detail these best practice security arrangements, focusing specifically on the physical security of premises and measures to prevent and deal with arson attacks.

Prevention and protection: Secure your business

It is very difficult to stop a determined criminal and predicting the actions of a 'casual' vandal or arsonist is virtually impossible. However, criminals rarely act without weighing the risk to themselves - even in the case of apparently spontaneous acts of vandalism.

AXA understands all too well the factors that can determine the likelihood that a business will be affected by crime. To an extent, this will be determined by geographical location and line of business. However, putting in place effective security procedures will also have a huge impact.

Businesses with good security arrangements are:

- Less likely to be targeted by professional criminals.
- More likely to minimise the losses they suffer, should criminals strike.
- Less likely to suffer repeated attack by criminals - including vandals.

A review of business practices and security can greatly reduce the chances of the premises being targeted. The following practical guidance draws exclusively on the experience and expertise of AXA's Risk Control team who inspect thousands of business premises each year. It provides guidance on the key areas of security that should be viewed as a priority by any businesses aiming to better protect itself from crime.

On the money: Look after your cash

Money is the primary motivation behind the majority of break-ins, either through the removal of valuable equipment and stock, or through the theft of cash. Chip and Pin devices have reduced the cash takings within many retail premises but most thieves will still initially focus their attention on cash, so it is also the first area you should think about. Commonly used measures include:

- Plastic till-guards - offer a cheap but effective way to prevent till snatches.
- Counter cache(s) - lockable metal containers kept close to the till, which are intended for the temporary holding of bank notes before transfer to the safe or bank.
- Smoke and dye money pack systems designed to emit coloured smoke and spoil stolen cash.
- Regularly remove cash from tills during the working day and place takings within the safe – this will reduce the amount of cash stolen should a hold-up attack occur.
- Pneumatic cash transfer system - an air-powered tube system to convey cash to a secure area or safe could be considered where large amounts of cash are being handled.
- External access safes - where cash collection companies can supply or take away cash without the need to enter premises.
- Time-delay safes - secure and only possible to open after a pre-set time, these safes will keep any cash not in the till, or not yet banked, safe from all but the most determined robbers.
- Attacks on security safes are now rare although modern safes can often be lighter in weight. These should therefore be bolted (anchored) to a concrete floor or be an underfloor safe.

On the money: Look after your cash

Banking procedures

Your cash could be at the greatest risk when it is in transit between your premises and the bank. Following the guidelines below could help to keep your money safe and your staff out of harm's way:

- If large amounts of cash need to be banked or collected on a regular basis, then the safest method is to employ a recognised cash carrying company.
- If you do undertake your own banking, be especially careful. Remember you are most vulnerable at the start or end of your journey.
- Choose the right staff for the job.
- Be alert. Look out for suspicious people or vehicles.
- Always use a secure container for carrying cash, but don't draw attention to it.
- Don't be predictable. Vary the times and routes taken. Try and use the busiest roads and walk in the centre of the pavement, towards oncoming traffic.
- Never use public transport.
- If you use a car, try not to use the same one each time. If possible, use a decoy vehicle as well.
- Make sure all vehicles are well maintained. Keep all doors locked and don't make unnecessary stops or leave the vehicle before you reach your destination.
- If you are attacked - surrender the cash. NEVER FIGHT BACK!

ATMs

In recent times, there has been significant growth in the number of retail premises introducing ATMs as an additional service to their customers - according to BBC News, there are now over 66,000 ATM's in the UK. ATM's within retail premises will normally increase business and foot fall for the retailer, but it is essential that the business owner consults with their insurer, prior to the introduction of the ATM. This will ensure their business continues to be adequately protected, both physically and financially, should a burglary occur.

Whilst the amount of cash within retail ATM's can be as little as £1,000, this is rarely known by criminals - who often go to significant trouble to gain access to premises where ATMs are located. Ram-raid type attacks can result in losses in excess of £40,000, and severely affect the operation of the business whilst the shop front is rebuilt. In 2013 a new threat of gas and explosion attacks on ATM's started. Major amounts of force are therefore common to steal cash.

On the money: Look after your cash

ATM attacks are also not just an inner city problem. There is evidence that rural areas are being targeted as much as the traditional high crime areas - it is thought that this is partly due to lower level security precautions and longer Police response times.

There are a number of basic precautions that businesses operating ATMs can take to protect themselves:

- The ATM should be securely fixed to the floor through its security container and be located away from external glazing.
- Intruder alarms should qualify for 'Level 1' Police response, include confirmable technology and remote, dual path signalling monitoring telephone/broadband and GSM/GPRS signals. Consideration should be given to provision of panic attack devices for employees.
- Remove cash from the ATM at the end of each trading day to a safe of adequate security quality, sited within the premises. This must be done with the premises locked and customers excluded.
- Replace cash in the ATM prior to opening for the next period of trading.
- Place notices prominently around the perimeter of and within the premises stating that the ATM holds no cash when the premises are non operational.
- Leave the door to the ATM and the security container therein open when the premises are closed.

In addition to security considerations, it is vital that business owners remember their responsibility for providing a safe place of work and adequate training of staff in the duties they are asked to undertake.

Insurers, ATM providers and local police crime prevention officers can provide support for retailers on the security of ATMs. Liaison with insurers will provide not just information on security but also specific issues in relation to insurance cover.

Lock up: Secure your premises

Criminals forcing entry to premises is a nightmare scenario for most businesses. As well as the likely losses through theft, the damage to doors, windows, stock and other equipment can add to the cost and cause significant disruption. There is however a lot that you can do to prevent criminals targeting and entering your premises, and steps you can take to limit damage if they do get in:

Keep crime out

Doors are the first port of call for any criminal wanting to gain access to your premises. Don't make it easy for them:

- External doors must be secured using two 5-lever mortice deadlocks conforming to at least BS.3621. These, together with matching metal box striking plates should be fitted approximately 375mm from top and bottom of the door(s). Cylinder mortice locks on uPVC or aluminium doors should be to EN1303 although this standard for cylinder locks will not protect against lock snapping. (For this protection, comply with TS007 (Level 3*) or SS312 (Diamond Level).
- "Lock bumping" has been a recent phenomenon around cylinder locks. Anti Lock Bump locks are now readily available and should be used.
- Where the doors are outward opening, the hinge stile should be strengthened using two hinge bolts fitted approximately 375mm from top and bottom of the door.
- Side & rear doors, where vulnerable, should additionally be protected by fitting a single panel of 1.6mm steel sheet, facing externally. The steel sheet should be coach bolted through the door face at 150mm centre intervals (with nuts and bolts spot welded together for greater security), or alternatively secured with clutch head screws of maximum practical length at 100mm centre intervals. The steel sheet must be of sufficient size to be folded around the edges of the door to prevent peeling and, where practicable, all fixing screws should be concealed when the door is closed.
- Side & rear doors can be additionally secured internally with a centrally fitted full width horizontal metal bar of minimum 80mm x 10mm. The supporting brackets must be of metal construction and be secured by either:
 - coach bolts or screws (using no. 12 countersunk steel screws of maximum practical length) to the surrounding doorframe
 - fixing to the surrounding building fabric using suitable proprietary wall plugs and no. 12 countersunk steel screws long enough to ensure that there is not less than 50mm of screw in the brickwork.

The bar(s) to be secured in position whenever the premises are unattended using heavy duty close shackle padlocks.

Lock up: Secure your premises

Where the premises are located within a high-risk area, or have been subjected to previous attack, then it may be necessary to provide further protection:

- To prevent the door and its frame being removed, the hinge and lock jambs of the frame must be screwed and plugged to the surrounding brickwork at intervals not exceeding 300mm using suitable proprietary wall plugs and No. 12 (or larger) countersunk steel woodscrews long enough to ensure that there is not less than 50mm of screw in the brickwork.
- Where double leaf doors are secured with padlocks, a heavy-duty close shackle padlock and matching padlock bar should be fitted centrally in accordance with the manufacturer's instructions. The padlocks should be tested and approved to an appropriate standard - such as CEN Grade 5.

NOTE - Protection of designated fire doors must be agreed with the local fire authority prior to work being undertaken.

Windows are the point from which many break-ins start. Remember, your premises are only as secure as their weakest point:

- It is preferable that the opening sections of windows are screwed or bolted shut permanently. Where windows must be able to open, these sections must be fitted with key operated locks - where the hinged side or pivot axis is less than 1 metre, one lock will be sufficient, but if one metre or longer, then two locks will be required.
- Vulnerable windows may need to be protected with steel bars internally. Bars should be 19mm diameter (or square) solid (preferably case hardened) steel of not more than 100mm centres, passed through holes in and welded to tie bars of 50mm x 9.50mm flat steel. Tie bars must be provided whenever the bars exceed 450mm in length and must be spaced at intervals not exceeding 450mm when the bars are longer than 900mm.
- Bars fitted externally, must be welded to a frame constructed from flat metal with minimum dimensions of 38mm x 6mm. This must be fixed to the brickwork surrounding the window (not to the window frame) using 76mm x 9.5mm Rawlbolts at intervals not exceeding 300mm all around the opening.

External steel grilles may offer an alternative to steel bars. "Expamet" expanded steel mesh No. 2073F or 2074F, or 2mm (12 gauge) steel mesh at 25mm centres must be welded to a frame constructed from angle iron with minimum dimensions of 38mm x 6mm. This must be fixed to the brickwork surrounding the window (not to the window frame) by inserting into "reveals" and fixed to the brickwork using 76mm long x 9.5mm Rawlbolts or 76mm x no. 12 countersunk woodscrews inserted into suitable proprietary wall plugs at 300mm intervals all around the opening.

Lock up: Secure your premises

- Security film attached to the inside of the glass can also help to deter burglars. Although it is mainly used to prevent injury when glass shatters, thicker versions are available (in excess of 360 microns) which can delay intruders, but will not defeat a determined attack.

Sadly, even the strongest locks will not put off a determined criminal - and even if they fail to gain entry, the likelihood is that they will cause significant damage trying. There are a number of steps you can take to further tighten security of doors and windows. Roller shutters can operate as a "layered" approach to security but can also stand alone, especially commercial/industrial premises.

Roller shutters

- Shutters should be made of steel and either manual or electrically operated.
- Higher security risks should be protected with metal roller shutter which are approved to standard LPS 1175 (www.brecertification.co.uk).
- Manually operated shutters should be secured using two security-locking pins, such as the "Shutter guard" lock - each of these locking pins must be positioned as close as possible to the bottom of each side guide channel.
- In the case of electrically operated shutters, operating controls must be fitted with a key operated isolation switch. The electrical power must be isolated and the key removed whenever the premises are unattended. Electrically powered operating controls should be secured within a welded steel box housing with detachable or internally hinged steel cover plate, all of not less than 6mm thickness. The cover plate should be secured by a heavy-duty close shackle padlock securely bolted or welded to the box housing/cover plate.

Retractable security grilles

- Retractable security grilles can be an acceptable alternative to bars, grilles and shutters where aesthetics are important. The grilles should be designed and certified to test standard LPS 1175.
- Retractable grilles are made of steel and comprise interlocking lattices, which concertina out to provide a strong barrier protecting both doors and windows. The system would need to incorporate locking mechanisms to a standard acceptable to the insurance company. The grilles can be powder coated to suit internal décor or corporate image.
- Internal installation is a clear disadvantage of retractable security grilles since substantial damage, impinging on trading, can occur as intruders attempt to force entry to premises.

Lock Up: Secure your premises

Cut Your Losses

Despite all this, there is always a chance that criminals will gain entry to your premises. It is best to approach your security arrangements based on the assumption that they will. This means putting in place measures designed to limit losses once criminals are on site. These could include:

Security cages

High value security cages can be constructed within storage areas for the increased protection of portable hand and/or hand tools. Such storage areas slow down intruders' attempts to remove goods and can reduce incidence of staff pilfering.

Security cages should be formed from steel sections with welded mesh directly attached. Openings within the cage should be kept to a minimum.

Electronic security

Given time and necessary expertise, determined criminals can breach most physical defences. The important thing then is to ensure that criminals entering your premises have very little time to damage or remove your property.

It is normal these days to have intruder alarm protection to your premises, but technology has moved a long way and a combination of electronic devices can help make your premises secure and provide the added benefit of deterrent:

Intruder alarms

An intruder alarm backs up good physical security and should signal the presence of intruders in an area monitored by its detection devices:

- Ensure that the system is installed by a UKAS (United Kingdom Accreditation Service) company which is then approved under National Security Inspectorate (NSI) or Security Systems and Alarm Inspection Board (SSAIB).
- Provide a remote signalling transmission system to a 24 hour manned alarm receiving centre to ensure police attendance in the event of the alarm being triggered - to generate priority police response the alarm should incorporate confirmation technology to ensure the activation is not false. This can be sequential (more than 1 detector activating), audio or visual, and often a combination of these.
- Take special care to ensure that false alarms are not generated, as the police will not respond to alarm systems which cause an unacceptable number of false calls.
- External audible warning devices must be sited at least 3 metres off the ground or out of normal reach. If this cannot be done, then two external sounders must be provided.
- It is essential that intruder alarm installations are designed, maintained and operated correctly. Prior to installing an intruder alarm, guidance from AXA Insurance should be requested to ensure it is suitable for the premises.
- On completion of the installation work, it is important that all employees required to set/unset the alarm are provided with training by the alarm engineer - this will assist in reducing possibility of false activations and reduction in police response.
- Regularly check your alarm system to ensure detectors haven't been masked (by tape), damaged in any way or blocked by contents, stock etc. One blocked sensor can significantly restrict the effectiveness of your alarm system.

Electronic security

Security Fog

The use of a non toxic security fog (often referred to as smoke) has become a reliable tool in the fight against theft. It is estimated that there are now over 35,000* approved security fog installations in the UK being used regularly by large retail chains and the banking sector. AXA's preferred type of products utilise a glycol/glycerine substance which is vapourised to form the fog. This deploys rapidly and can stay suspended in the air for up to 45 minutes. Due to the very small particle sizes they typically leave no residue upon dispersal.

Following activation of an intruder alarm (to avoid accidental activation), the rapid release of the fog obscures vision and disorientates intruders. When confronted with the fog release, intruders will usually escape quickly before they are surrounded, leaving your contents safe. Police and keyholders should then attend before the fog has dispersed, allowing security to be re-enabled.

Systems when linked to the intruder alarm must comply with EN50131-8. However, systems must be designed not to provide a "man-trap". AXA also do not recommend use for day time "robbery" scenarios.

*According to Concept Smoke

CCTV

CCTV can be utilised as part of an integrated security system, for the reduction of distraction shoplifting/ theft and to discourage malicious damage/vandalism.

CCTV is intended to complement physical and electronic security protection and should not be seen as a replacement for these measures.

The following guidance should be considered prior to CCTV installation being installed:

- Quotations should be obtained from at least three NSI/SSAIB registered companies approved for CCTV installations. Consider closely the ongoing costs of the system and not only the installation costs. No contract should be signed until specification is agreed with AXA Insurance.
- Consider how the CCTV system is to be monitored and by whom. The recording image of any system is critical if it is intended that it be utilised later for identification purposes. Remote monitoring of systems is now possible - installations can be activated during working hours by pressing a personal attack hold up button linked to a remote monitored intruder alarm.
- Consider the use of digital recording rather than traditional video tapes – digital recording provides higher definition images and the technology assists in searching over a long time period.

Electronic security

- Consider what areas of premises/external environs need to be covered.
- Ensure that adequate lighting will be provided for both day and night operation.
- Design the system to incorporate existing security protection.
- Ensure the system has capacity for future expansion.
- Arrange adequate maintenance contract for installation.
- Ensure the system cannot be misused or sabotaged by employees.
- All CCTV systems must be Data Protection Act complaint - this can be achieved on-line at www.ico.org.uk, or you can call 0303 123 1113 to request an application form.

Access control

There are many ways to control access to your premises during the daytime from unwanted visitors. These unwelcome visitors offer numerous threats to your business, including theft of equipment or data and the risk of other malicious acts. There are other health and safety issues especially if your premises are industrial in use.

Doors that do not open from the outside (i.e. fire doors) are beneficial to the sides and rear of the building to prevent access. Away from the retail environment, a permanently manned reception desk is common or even a phone in an unmanned secure waiting area to call staff to allow access.

Visitors should be signed in and provided with visitor passes. Staff must also be prepared to challenge anyone unaccompanied and unknown within the premises (for safety reasons if the visitor was there for genuine reasons).

Access control can be used on internal doors and in some cases are used to restrict floor access within lifts. Typically, swipe cards are used. In offices, gate opening systems are employed which also prevents tailgating on access controlled doors. Key considerations:

- Think about areas to restrict access. Unless comms and data rooms are under lock and key, these should always be part of an access control system, likewise stock and store rooms. Offices should work under these systems also where there is sensitive data and where office spaces can be empty for periods during working hours.
- Maintain good control over issuing and returning cards. There have been cases of disgruntled ex-employees having access and returning to the premises.
- Watch out for tailgating where access control is on doors - do you know the person following you in? Also, be careful that doors are closing properly and/or are wedged open, disabling the access control system.

Help from AXA Insurance

AXA insurance recognises the problems small and developing businesses encounter in obtaining information and advice on effective risk management - of which crime prevention is a critical element.

This guide is designed to make easily available the wealth of risk management experience and expertise within AXA Insurance - to help small businesses identify the threats posed by crime, and implement measures designed to reduce exposure.

Beyond this, AXA Insurance has a team of 40 Risk Control surveyors, covering the whole of the UK, who are available to provide advice, guidance and assistance with loss control measures.

Finally, get involved in crime prevention initiatives in your area. By working together, small businesses can help create a better local business environment, one in which the impact of crime is greatly reduced. As an example of local initiatives, visit www.bcr-uk.org.



ACLD0819-A

www.axaconnect.co.uk

AXA Insurance UK plc Registered in England and Wales No 78950. Registered Office: 5 Old Broad Street, London EC2N 1AD. A member of the AXA Group of companies. AXA Insurance UK plc is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority. Telephone calls may be monitored and recorded.