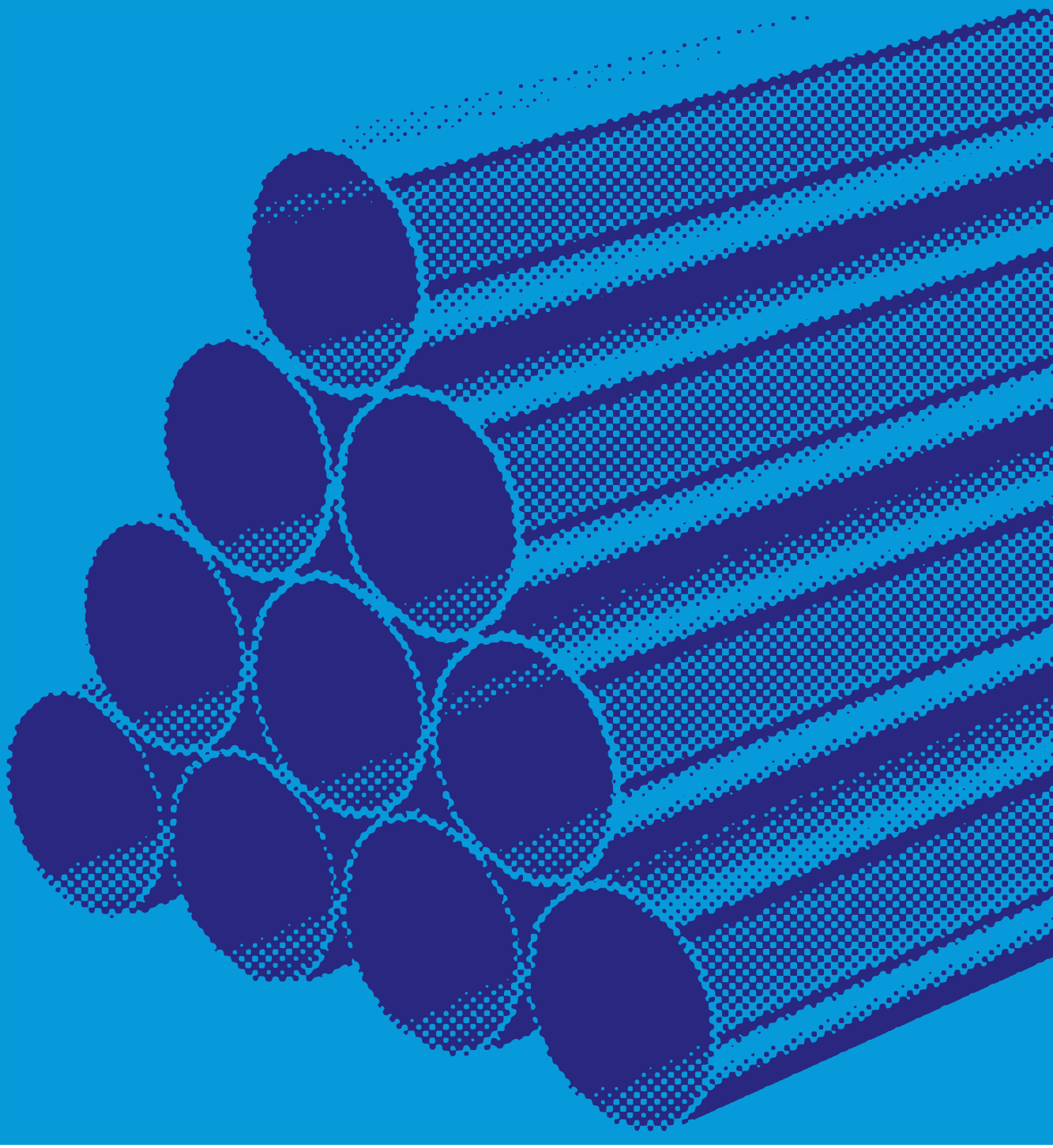
S21
First published 2012
Version 01

Security

Measures for the control of metal theft



RISCAuthority

administered by
FPA
Fire Protection Association

IMPORTANT NOTICE

This document has been developed through the RISCAuthority and published by the Fire Protection Association (FPA). RISCAuthority membership comprises a group of UK insurers that actively support a number of expert working groups developing and promulgating best practice for the protection of people, property, business and the environment from loss due to fire and other risks. The technical expertise for this document has been provided by the Technical Directorate of the FPA, external consultants, and experts from the insurance industry who together form the various RISCAuthority Working Groups. Although produced with insurer input it does not (and is not intended to) represent a pan-insurer perspective. Individual insurance companies will have their own requirements which may be different from or not reflected in the content of this document.

The FPA has made extensive efforts to check the accuracy of the information and advice contained in this document and it is believed to be accurate at the time of printing. However, the FPA makes no guarantee, representation or warranty (express or implied) as to the accuracy or completeness of any information or advice contained in this document. All advice and recommendations are presented in good faith on the basis of information, knowledge and technology as at the date of publication of this document.

Without prejudice to the generality of the foregoing, the FPA makes no guarantee, representation or warranty (express or implied) that this document considers all systems, equipment and procedures or state-of-the-art technologies current at the date of this document.

Use of, or reliance upon, this document, or any part of its content, is voluntary and is at the user's own risk. Anyone considering using or implementing any recommendation or advice within this document should rely on his or her own personal judgement or, as appropriate, seek the advice of a competent professional and rely on that professional's advice. Nothing in this document replaces or excludes (nor is intended to replace or exclude), entirely or in part, mandatory and/or legal requirements howsoever arising (including without prejudice to the generality of the foregoing any such requirements for maintaining health and safety in the workplace).

Except to the extent that it is unlawful to exclude any liability, the FPA accepts no liability whatsoever for any direct, indirect or consequential loss or damage arising in any way from the publication of this document or any part of it, or any use of, or reliance placed on, the content of this document or any part of it.

CONTENTS

1. INTRODUCTION

The damaging impact of metal theft on the community in recent times, nationally and internationally, has become widely known, dating from the sharp increase in metal theft driven by spiralling increases in global metal commodity prices. The crime was recently estimated to be costing the UK £770 million a year. Just one specialist UK insurer, mainly of churches, for which the theft of lead from roofs is a major problem, has received more than 12,500 metal theft claims since January 2007, costing nearly £30 million.

The problem can seem intractable as metal is found all around us and 'there for the taking' in industrialised western economies. Indeed one study found that metal thieves travel only between 3km and 5km on average and the supervision of disposal channels (scrap dealers etc) has been seen as lax. Consequently legislators have been looking chiefly to stronger market and law enforcement controls to stem the present crime wave and there is evidence that these are turning the corner. However the owner of metal assets is not powerless and there is a range of actions that can be taken to contribute to combating the crime and safeguarding the property.

In this document reference is made to standards documents (eg British Standards Institute, Loss Prevention Certification Board) by the standard number. Where applicable, the current edition should be referred to unless the edition (number/year) is given. The full titles of the standards cited appear under 'References' at the end of the document.

2. SCOPE

This guide looks at the problem of the theft of metal, chiefly from in the open or where attached to/forming part of a building, and considers the security options.

The security options included in the guide are slanted in favour of those with notable relevance to metal theft. As such the document does not set out to address in depth the *general* security of assets against all forms of crime. In the case of a business premises or site the assumption is made that a general security risk assessment has already been completed, possibly with the assistance or input of an insurer, police crime prevention advisor and/or security industry representative. If this is not the case, in-depth guidance on measures such as mechanical protection, intruder alarm systems, CCTV, access control, perimeter protection, lighting, anti-ram raid and manned security services is readily available from a number of sources (see 'Police crime prevention design advice' and also, at the end of the document, 'Useful links' and 'RISCAuthority documents').

The end user is recommended to exercise a degree of caution and healthy scepticism before making a commitment to the more 'innovative' solutions mentioned in this guide. Such has been the clamour for a 'magic bullet' with the recent and relatively sudden escalation of the problem that there are now a large number of solutions available for which claims are made that are not always supported by independent evaluation. Consequently no inference should be taken that any particular product or service seeming to match the general types described in the document are necessarily fit for the claimed purpose, can be relied on to operate in any particular way or would not carry risks of unintended consequences.

The escalation in the crime has spawned a number of providers claiming to offer a package of products/services that they claim can assure the ultimate solution. Some of these claims have been found to have a dubious basis in reality. Buyer beware! Always check with your insurer. Good basic advice on selecting security solutions can be found in the RISCAuthority document **Essential Principles for the Security of Property**.

3. THE PROBLEM

Typically targeted by thieves is metal:

- in the open
  - eg cable, on reels or drums or actually connected, in service and live (electricity supply, telecommunications etc), or signs, gates and catalytic converters from vehicles;
- attached to, or part of, an unoccupied building or premises (particularly if under construction, renovation or demolition or when falling vacant, having been normally occupied)
  - eg roof metal, metal fittings, pipework, tubing, air conditioning plant, lightning conductors, gates, fences, grids, chamber covers;
- located in normally unmanned premises/installations
  - eg sub stations, transformers, wind farm plant;
- attached to, or part of, an occupied building or premises (notably premises which are unattended for extended periods such as schools and churches)
  - eg roof metal, metal fittings, boilers, pipework, air conditioning plant, lightning conductors, gates, fences, grids, chamber covers; and
- found inside business premises
  - eg raw material, work in progress, components, stock.

Holders of metal in one form or another, particularly non ferrous metal, *inside* a building have long found it necessary to take special care to ensure that the premises security is adequate. For the most part, taking into account the preference of present day metal thieves for 'easy pickings' the security precautions already taken of necessity by occupiers of premises holding metal may well be sufficient, but complacency would be dangerous in light of the increased attraction to criminals of metal and review of current security arrangements is strongly recommended. For example, the quality of the connection (alarm transmission system) to the monitoring service (alarm receiving centre or ARC) of any intruder alarm system may well need an upgrade to reflect the determination of attackers in the present climate. An increasing number of alarm transmission systems are available which are certificated to the Loss Prevention Certification Board's Loss Prevention Standard LPS 1277.

4. LIAISON

Liaison with other interested parties should be considered. For example the landlord and/or an insurer will have a valid interest in the management of crime risk and need to be consulted. Neighbours and police are also potentially a source of help.

5. REDUCING THE FUNDAMENTAL RISK

Removing/reducing the target

As with business risks of all varieties, the starting point in the risk management process is the undertaking of a security risk assessment consisting of risk identification, analysis and evaluation, including the potential consequences, their knock-on effects and resulting business interruption and reputational risks. In the case of metal theft the currency of information is particularly important – eg market prices, crime trends and criminal methodologies.

Once the exposure is measured and understood it is often possible and desirable to alter the profile of the risk in terms of the target it represents to the potential thief and thus avoid the need to implement other countermeasures.

This may be achievable through the removal, relocation or reduction of the metal at risk. One strategy is the use of substitute materials (see below). Another example may be ensuring that materials arrive at agreed times to coincide with installation or that metal stocks are available for call-off, avoiding the need for on-site storage. Procedures can be set up whereby metal is ordered in accurate quantities and on an as-needed basis so that surplus is not available on the premises.

If possible, scrap should be out of view and collected frequently to minimise the interest to opportunists. Residual risk needs to evaluated and made subject to controls and protections such as those identified in the next section.

Substitute materials

Cable:

There are alternatives to copper cable such as copper coated aluminium or aluminium/tin coated copper which either have less scrap value, and/or increased scrap processing costs, but thieves may not know the difference so this will probably not deter them in most cases. There may also be practical/performance issues with such cable in the field.

Lead roofing:

Of course it may be possible to replace sheet lead roofs with tiles, slates or mineral felt but if appearance and performance similar to lead are desired (or required by an authority such as English Heritage) the most popular choice is Terne coated stainless steel (much less scrap value than lead). Again, due to the similarity in appearance to lead it may still be attacked (perhaps carefully drafted notices on the building would help deter some potential thieves).

There are proprietary roofing systems being marketed as alternatives to lead, but it is not thought that these fully succeed in replicating the appearance of lead.

It is important that the insurer is consulted about alternative roofing materials in advance, as altering construction materials can have an impact on insurance terms.

Other metal products:

Many products taken by thieves such street signs, drain covers, gratings, steps, handrails etc are available in fibreglass or plastic and are almost as durable as iron/steel and with a similar appearance.

Note: Planning permission may be required for certain changes to the appearance of premises – this being especially likely if listed building/conservation area status applies. Check with the relevant planning authority.

6. PRIMARY PREVENTION AND DETERRENCE MEASURES

Networking in the local community

In many cases a material mitigation of risk can be achieved simply through promoting a sense of metal crime prevention solidarity and criminal intelligence in the local community, especially where neighbours have a similar stake in keeping metal thieves away. Some theft victims report that they have found it difficult to convince the public and the authorities that the problem is a serious risk for the community, employment etc. Joint intelligence and 'educational' efforts to bring home the actual impact on the local community of this crime wave can pay dividends.

This starts with networking at senior level with local businesses and owners to encourage awareness and the reporting to the police, and the other stakeholders, of suspicious activity. If what is observed does not really justify a 999 call, the authorities nonetheless want to hear about behavior that could have a link to crime through the recently launched national '101' non-emergency number. That said, some events clearly demand a '999' call – eg 'workmen' on a roof without scaffolding and/or at an unusual time (say between 6pm and 8am); a cable drum being manhandled into an unmarked van; suspicious persons accessing a cable inspection chamber. If metal thieves are in the area, commercial premises of all kinds are at risk (not just the utilities) as all have materials that can be turned into cash to one extent or another.

Linking up with the local crime prevention group or Neighbourhood/Business/Farm Watch or the forming of a new local intelligence sharing scheme should also be looked at in order to take opportunities to share information received on incidents, crimes and criminal methods. It may be possible to link up with the neighbourhood policing team panel, which sets local priorities for the police and has a say in the kinds of work being done by convicted criminals serving community sentences. Trends and guidance may also be available from a trade body and the myriad national and international websites on which news and advice is posted these days.

Police crime prevention design advice

The local police crime prevention officer or crime prevention design advisor can provide news and advice on metal theft prevention. The British Transport police also have a wealth of knowledge and experience. Contacts and guidance documents are available via Secured by Design – the official UK police scheme aimed at 'designing out crime': See http://www.securedbydesign.com

Impact statements

It is import for businesses and owners unlucky enough to have suffered a theft to understand the importance of the drafting of the Impact Statement that is presented in any court proceedings that may follow. A theft of metal that realises only a small amount for a criminal can have a big impact on an operation or community (eg a theft value of £100 may deny a whole town its electricity for a night).

Helping the police and courts to understand the importance of what has happened is crucial. Preparation of an impact statement that spells out the full extent of the damage done to the business or enterprise gets across that this in not just another victimless property crime and as such is much more likely to secure a meaningful sentence for the future benefit the organisation and other stakeholders when it comes to the risk of re-victimisation.

It is also noticed that in selected cases where the sentence is clearly out of proportion with the impact, the victim operation has been successful in pursuing a civil recovery although this would naturally require careful legal examination and consideration of the possible cost implications.

Asset marking and recovery systems

Physical marking

Marking allows a security operation or the police to trace back any subsequently recovered lost or stolen asset to its original owner. Examples include the attachment of a secure label, embedding an identifier such as a micro dot or continuous ID tape (in a cable), printing or embossing the asset or simply inscribing or etching the asset with characters (eg a post code, name or code word) with an overt or covert marker.

The Loss Prevention Certification Board's Loss Prevention Standard LPS 1225 contains provisions specific to these products and services and a number of certificated products are available.

Forensic marking

When reference is made to 'forensic marking' it is generally taken to imply a coding system that, in addition to serving to identify the legitimate owner or original location of an asset, can link a suspect with the theft in a stronger way than other marking systems; in fact a way that would enjoy enhanced credibility in a court of law and materially assist the prosecution of the offender. By one definition the key represented by the 'forensic' code used by the system can only be discovered using 'laboratory analysis'.

Such systems generally consist of a medium that itself serves as an overt or covert marker (eg a liquid that glows in ultra violet light) in which the forensic code is suspended. The medium alerts the security or law enforcement officer to the presence of the forensic marking. In this example the forensic fluid is sprayed or painted onto assets, but there is also an application when used with triggering devices whereby a suspect is splattered/sprayed with the material, and which then uniquely links the suspect to the offence – the material remaining detectable on skin and hair for several weeks.

Non-drying forensic 'gels' or 'greases' which transfer and stick to thieves handling marked assets are also available.

Secure database services

Marking that cannot be read and readily linked to the legal owner without reference to records must be supported by a secure database.

Such services should operate to recognised management and security standards. BS ISO/IEC 27001 specifies high level requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented information security management system. In the UK, LPS 1224 contains provisions of a similar type, but specific to secure asset registration services

Wireless security tags

This technology, more usually associated with individual items of exceptional intrinsic or heritage value, is used effectively in detection and 'sting' operations eg to track the illegitimate movements of metal.

Anti-vandal paint

Painting down pipes and roofing with non-setting paint, sometimes called 'anti-climb' paint, deters and hinders access. Occupiers' liability issues need to be taken into account and suitable warning signs displayed.

7. 'PASSIVE' SECURITY OPTIONS

Passive security consists of physical barriers and security devices. For example a fence or the building shell or an item used to secure part of it, eg a door lock. There is no active intervention in the criminal event but, instead, the measure is said to 'buy time' to allow intervention to take place or for the attack to be abandoned. As well as providing tangible security, passive security acts as a good deterrent.

Site perimeter

Given the amount of force and determination that metal thieves bring to bear a secure perimeter barrier must be provided for metal in the open.

Fencing

Perimeter fencing should be a minimum height of 2.4m. High security and maximum security fences should be a minimum of 3.0m high. The most popular types are:

- welded mesh fencing to BS 1722-10: a small mesh size frustrates finger holds and climbing;
- open mesh steel panel fencing ('expanded metal') to BS 1722-14; and
- steel palisade to BS 1722-12: vertical steel rods, with the top end flattened, split and splayed into sharpened points to deter climbing.

Notes:

- Barbed wire or razor tape further deter climbing but occupiers' liability issues need to be taken into account and suitable warning signs displayed to help discharge any liability that may attach by virtue of the Occupiers' Liability Act 1984 and the Health and Safety Act 1974.
- Planning permission may be required for certain types of fencing/gates – this being especially likely if listed building/ conservation area status applies. Check with the relevant planning authority.

Perimeter gates

Gates must be of the same height, material and strength as the fencing. Hinges should be designed to prevent the gate from being lifted. Gates are best secured by welded high security proprietary locking bar(s) and padlock(s) to BS EN 12320, grade 5 or 6. Remember that, in addition to failing to exclude intruders, an insecurely hung and locked gate at an isolated site may itself be targeted by metal thieves!

Where there is vehicular access to the perimeter, particularly in isolated locations, a ram raid attack must be considered if the investment in secure personnel fencing is not to be in jeopardy. A purpose designed vehicle barrier such as a trench, high kerb or large concrete obstacles outside the fence, or a series of substantial steel posts just inside the perimeter, can be considered. Further advice is contained in RISCAuthority document S10.

Planning permission may be required for certain types of fencing/ gates. Check with the relevant planning authority.

Lighting

If the thief perceives he might be observed but for the benefit of darkness, lighting can be an effective measure and good deterrent. On the other hand, in a remote, unsupervised location, the presence of lighting may actually assist the thief.

If security lighting is assessed as a cost-effective measure the site, buildings and features should be bathed in a good and even overall level of light. Uneven lighting assists the thief by providing light to work with and shadows to hide in.

Scenes and objects with low reflectance (dark walls, bitumen surfaces etc) will require more light than reflective surfaces.

The deterrent effect can often be magnified by having the lighting on anticipated approaches facing outwards to 'blind' the approaching intruder. This strategy in particular may however be subject to challenge in the local community or through planning law. Check with the relevant planning authority.

Lighting can be switched on automatically by timer and/or photocell but domestic self-contained movement triggered lighting is to be avoided as it may have erratic performance, is easily interfered with and lacks the deterrent impact of a fixed, continuous installation.

The advice of a security lighting specialist might be sought. This expertise will help ensure that an optimum and secure installation is achieved using vandal and sabotage resistant lamps, connections and power sources appropriate to the risk level.

Secure access covers

Metal covers in yards, paths and roads are a target for thieves in their own right and/or in order to reach the services (eg cable) to which the cover gives access.

Lockable access covers are strong covers with robust integral locking arrangements to help prevent opening/removal with simple tools.

Alternatively, secondary security covers increase the time/effort required to gain access to a service chamber using proprietary assemblies secured by special bolts or locks.

Certain covers have achieved certification to the Loss Prevention Certification Board Loss Prevention Standard LPS 1175.

Other passive cable theft prevention solutions

There are both in-house and proprietary options:

Cable/component removal:

Traditional anchoring methods (a 'nut and bolt' approach) or proprietary devices of various types that frustrate the simple dismantling of valuable copper components such as ground bars.

Cable clamps etc – cable is clamped with purpose-designed security fittings intended to prevent the cable being easily pulled out of the ground or a duct or conduit.

Tack welding of access points, burying pull boxes.

Upgraded physical security (eg locking components/padlocks) to sub station/plant room/cabinet access points.

Inhibiting roof access

Access to a roof can be hindered by installing barbed/razor wire along roof edges and/or anti-climb spikes to down pipes, etc. Occupiers' liability issues need to be taken into account and suitable warning signs displayed.

8. 'ACTIVE' SECURITY OPTIONS

An active security measure is one designed to instigate a response to, and intervention in, an incident. Examples of active security are the presence of alert staff, a security guard or an electronic security system such as access control, intruder alarm or CCTV. As well as providing tangible security, overt active security acts as a good deterrent.

External video surveillance

CCTV surveillance used specifically to tackle metal theft can be an attractive solution in certain cases but the user/specifier needs to be clear as to the objective eg:

a) to monitor assets or the approaches/surroundings so that a response can be made if necessary; or

b) to make a video record of events that could be used by prosecutors and possibly deter thieves into the bargain.

It goes without saying that one implication of a) is that unless a significant investment is available for the cost of providing an effective observer at all times that the metal is at risk, the (probably considerable) investment in the CCTV installation is at jeopardy. And secondly that an implication of b) is that the undetected theft of the metal may still take place without even, for a variety of reasons, the satisfaction of seeing the perpetrators punished. For these reasons detector-activated CCTV (see below) is seen more often as the preferred solution in the applications needing protection against for this type of crime.

The range of issues that need to be taken into account when it comes to making an investment in a permanent CCTV installation that has either a) or b) (or both) as the objective is such that comprehensive and balanced advice can not be attempted in a document of this type and competent advice should be sought. Installations should be carried out in accordance with BS EN 50132-7.

External electronic intruder detection

Certain detection systems, for the most part intruder alarm systems (IAS) protecting assets inside buildings, can qualify for a police URN (Unique Reference Number) which entitles them to a level 1 (immediate) police response in the event of an activation.

Such systems must be installed by a company approved by a United Kingdom Accreditation Service (UKAS) listed inspection body, currently the NSI (National Security Inspectorate) and SSAIB (Security Systems and Alarm Inspection Board).

A current British Standard for external alarm systems exists in the BS 4737 series (which consists of suite of Intruder Alarm System standards, the majority of which have been withdrawn and replaced) viz BS 4737-4.3. These are intruder alarm systems in situations in which the balance of the system is located exterior to any building. However the standard dates from 1988 and it is understood that no providers are currently claiming to be installing to this standard which is now in need of revision. The police would not award a URN to such a system. This has been a factor leading to the development of BS 8418 systems (see 'Detector-activated CCTV' below).

That said, a wide range of alarm devices designed for external use exists such as passive infrared detectors, infrared beam detectors and microwave fence detectors. There are providers that will integrate such devices into an effective external alarm system that would alert a monitoring centre (ARC) who could then summon a keyholder even though they would not be permitted

to automatically summon police. An even more effective solution is achieved when such external detection is integrated with a high quality CCTV surveillance system (see 'External video surveillance' above).

An increasing number of alarm transmission systems are available which are certificated to the Loss Prevention Certification Board's Loss Prevention Standard LPS 1277.

Electric security fence

An electric security fence consists of a series of tensioned bare metal wires carrying a pulsed high voltage current which is insulated from the carrying posts/mountings.

Anyone in contact with the ground interfering with the fence and touching these conductors, or touching two or more wires simultaneously, will receive a sharp electric shock. The shock is very painful and the miscreant is obliged to discontinue the attack. However the providers and the governing authorities are satisfied that the electric pulse is not physically harmful. Nevertheless this is an 'aggressive' device so occupiers' liability issues need to be taken into account and suitable warning signs displayed (invariably supplied by the provider).

This solution is usually used to deter, or failing that repel, unauthorised entry to sites, typically open areas around buildings or storage yards/compounds, etc, and most usually outside business hours. They are most effective when provided with a fence activation sensor (alarm) system; as by this means an alarm can either be sent to on-site personnel or, via a remote signalling intruder alarm or CCTV system, to personnel elsewhere.

These are specialised products, requiring careful manufacture, design, installation and maintenance. The applicable standard is BS 1722-17 and the Secured By Design website lists providers meeting their criteria.

Detector-activated CCTV (DA CCTV)

Normally implemented in the open, DA CCTV systems blend IAS technology with CCTV. They provide flexible and adaptable protection for metal that can not be included in IAS coverage (ie typically within the perimeter of the site but not within the buildings) and, being located in a hostile environment, they demand the intervention of a remote operator at a monitoring centre before an event can be notified with confidence as a 'confirmed incident' to the police or responding party.

To be assured that such systems have a high degree of credibility with the police and are state of the art they should be certificated by the NSI or SSAIB to BS 8418.

Such systems define a 'secure area' within which movement is detected using methods similar to those of an IAS. Notification of this event, along with associated CCTV images, is transmitted over a network to a monitoring centre denoted a remote video response centre (RVRC). If, in the judgement of the RVRC operator, a crime is underway, or seriously threatened, the RVRC is entitled, in the majority of police force areas of the UK, and where the system has been allocated a police URN, to make direct contact with the police control room. A voice warning ('audio challenge'), audible in the secure area, may also be played at the site.

One of the key issues with such systems is to ensure that the connection (usually internet based) between the protected site and the RVRC is itself reliable and secure, ie frequently monitored for failure and able to report such an event. In this regard it should be noted that an increasing number of internet based alarm transmission systems are available which are certificated to the Loss Prevention Certification Board's Loss Prevention Standard LPS 1277.

Temporary alarm systems (TAS)

Temporary alarm systems are available both for internal and external applications, most being designed to be battery powered only.

Systems usually comprise a portable control/power unit and various wire free intruder alarm sensors, although some use various forms of audio or visual detection and/or alarm confirmation. Fire detection sensors can be added to some systems.

Most systems provide silent/covert notification of activations to a monitoring centre (ARC) via a GSM network but some have an option to use additional local warning devices. Some products have the option to send periodic test calls to and from site to check the operational status of the system and the means of notification. Notified faults would normally include 'low battery'.

As these systems do not meet police rules, they do not qualify for a URN and thus a routine emergency police response. However, once a keyholder/response service attends site they would be able to request police attendance via normal means if there was evidence of a crime in progress or having occurred.

Such systems may be purchased but the great majority are rented. Many of the companies specialising in this field provide a commercial response and keyholding service.

Temporary alarms are a cost effective and proven way of providing protection against metal theft in selected situations that are without adequate conventional security and/or mains electricity. However, their effectiveness will depend on many factors and competent advice should be sought. At the time of this document's preparation the SSAIB are preparing a providers' approval scheme supported by their **Code of Practice for Temporary Alarm Systems**.

Underground cable theft detection

Several proprietary solutions have become available in the last few years. Typically they consist of alarm systems that detect when:

A cable chamber or duct is opened:

- A light sensor inside the enclosure triggers the system if daylight or torchlight enters;

A cable is severed or disconnected:

- Fibre optic strand is run, or integrated with, the cable and monitored by a detection device that can detect both severance and its location, and/or, through analysis of sounds and vibrations, detect disturbance of, or close to, the cable.
- Monitoring signal superimposed on live or dead cables detects severance/disconnection; and

A security zone established near the cable run is entered or disturbed:

- Buried miniature motion/disturbance detectors and associated cameras watch for movement/shock/vibration.

The method of notifying the alarm condition to the monitoring point with such systems invariably consists of a battery-powered radio or GSM transmitter sending alerts/images to the monitoring point, or smartphone or radio network.

Bearing in mind the sheer quantity of cable and the distances they are run (eg along a rail line), it is usually only economic to deploy them to a tiny fraction of the asset on a 'spot' basis as 'trap' protection or as an element of a 'sting' operation.

Roof access detection systems

Church insurers recommend the use of passive infrared (PIR) motion detectors, similar to those used in IAS, fanning out zones of movement detection across the surface of roofing and linked wirelessly to control equipment. These devices are specifically configured for the outside environment in such a way that false alarms from the movements of wildlife are minimised. When the alarm is triggered, strobe lights unsettle the intruder(s) and they may also be warned off by an audio challenge. Simultaneously an alert is transmitted to a monitoring centre (ARC) and keyholders are informed.

There are alternative methods also specially designed for roof surveillance:

One system comprises a detection cable which is secured to leaded areas with a weather resistant, externally rated adhesive. Each zone, terminates in a small wireless transmitter that sends its signals to the control equipment inside the building. Severance or severe vibration will trigger an alert.

Similar results are given with individual vibration detectors attached to the underside of the roof substrate. Depending on the substrate characteristics, each detector can cover a radius of about 2m.

General 'active' premises security measures

The enhanced risk of metal theft may call for the reinforcing or supplementing of the security arrangements already in operation. Traditional tried and tested security solutions include:

Access control

Control of access to metal assets may entail elaborate keyholding arrangements or the presence of human supervision at points of entry. A proprietary access control system frequently forms a practical and secure solution through automatically allowing only authorised personnel access without the risks and inconvenience associated with traditional locking or the costs of manned security.

These systems have the incidental benefit of 'hardening' the target premises in the perception of thieves, particularly of the type typically involved in metal theft. The advice of a reputable electronic security provider should be obtained.

Manned security services

In one sense the presence of an intelligence on site in the form of human surveillance has no rival amongst alternative technical solutions but caution is required. In reality manned guarding is expensive and fallible.

Static and mobile guards supplied by a manned security service must legally hold a Security Industry Authority licence. Certain security firms in this sector enjoy the endorsement of accreditation by the National Security Inspectorate (NSI) and/or the Security Systems and Alarms Inspection Board (SSAIB) and/or the Security Industry Authority Approved Contractor Scheme (ACS). Firms with one or more of these approvals may be viewed as likely to provide a more reliable service.

If the security risk assessment suggests that a manned presence is the optimum solution, the provision of the services needs to be discussed with a specifier, consultant crime prevention officer or service provider.

Intruder alarm systems

Traditional intruder alarm systems for the buildings and their contents are well established as a basic building block of business premises security. Certification by a inspectorate accredited by the United Kingdom Accreditation Service (UKAS) – these bodies currently comprising the NSI and/or the SSAIB – allows a system to enjoy the benefit of a police Unique Reference Number (URN).

Organisations holding metal assets and relying on intruder alarm systems providing modest, general levels of protection may find, in the face of the increased threat, that they need additional detection capability, focused on the metal holdings. They may also need to review the security of the remote monitoring arrangement (alarm transmission system) to ensure it is capable of resisting interference by criminals. One of the key issues with such systems is to ensure that the connection between the protected site and the monitoring centre (ARC) is itself reliable and secure, ie frequently monitored for failure and able to report such an event. The need for enhancement should be explored with a specifier (eg the insurer), consultant, crime prevention officer or service provider.

An increasing number of alarm transmission systems are available which are certificated to the Loss Prevention Certification Board's Loss Prevention Standard LPS 1277.

9. MAINTAINING THE DEFENCES

Generally, the adequacy and suitability of the security protection afforded to assets needs more frequent review and more awareness of fluctuation than 'fortuitous' hazards such fire, storm and flood for the obvious reason than crime patterns are subject to rapid change through market conditions and social trends. The frequency of these environmental changes seems to be increasing.

Consequently security should must be subject to continuous review eg as the nature or value of the assets change, as external factors alter, eg a marked increase in the activities of metal thieves in the area, or, in particular, after any security breach/loss.

'Repeat victimisation' is a familiar criminal pattern. It is generally held by risk managers that any revised security measures applied in response to a security breach/loss should be significantly stronger than might have been deemed necessary had no previous breach occurred.

The effective operation of the installed security needs to be continuously checked and also actually tested if appropriate. Certain security solutions must have routine or periodic maintenance to preserve their effectiveness in terms of ease of use, reliability and credibility.

Finally, the users and operators of the security measures (staff, management, contractors) need to understand the purpose and functioning of the measures and be trained in their correct operation. An adequate introduction to the security measures and suitable initial and ongoing training are essential elements of the implementation of the security strategy.

10. POTENTIAL SOLUTIONS FOR SPECIFIC SITUATIONS

Situation	Issues	Generic solution	Specific measures (examples)
Roof metal	Surveillance, access, removal	Roof access prevention solutions	Access prevention: anti-climb paint etc; electric security fence
		Roof access detection systems	Movement, vibration, stretched wire (etc) detectors
		Substitute materials	Terne coated stainless steel etc
Metal stored outside	Security of the enclosure	External video surveillance	CCTV (monitored and/or recorded)
		Electronic intruder detection	External detection system (beams, vibration sensors etc); detector-activated CCTV
		Temporary alarm systems	Portable, battery powered intruder alarm
		Fencing and gates	Electric security fence
		Risk removal/reduction	
Unoccupied premises	Absence of supervision/ surveillance	Temporary alarm systems	Portable, battery powered intruder alarm
		External video surveillance	CCTV (monitored and/or recorded)
		External electronic intruder detection	External detection system (beams, vibration sensors etc); detector-activated CCTV
		Fencing and gates	Electric security fence
		Risk removal/reduction	
Cable theft	Ubiquity, ease of removal, absence of supervision/ surveillance, exposure of metal in support facilities (sub stations etc)	Underground cable theft detection	Chamber access detector, cable severance detector, miniature/covert CCTV, vibration detectors etc
		Underground cable theft prevention	Lockable covers Cable clamp Locks/padlocks/anchors etc
		Substitute materials?	Fibre optic, aluminium
All situations		Asset marking and recovery systems	Overt: label, marker, tape etc
			Covert: wireless security tag, micro dot; forensic paint, grease, etc
			Intruder tagging (spray)

USEFUL LINKS

http://www.bsia.co.uk

https://help.aviva.co.uk/risksolutions

http://www.ecclesiastical.com

http://www.english-heritage.org.uk

http://www.police.uk

http://www.crimestoppers-uk.org

http://www.nidirect.gov.uk

http://www.bcrc-uk.org

http://www.recyclemetals.org

http://www.securedbydesign.com

http://www.nsi.org.uk

http://www.ssaib.org

REFERENCES

BS 4737-4.3: **Intruder alarm systems in buildings. Codes of practice. Code of practice for exterior alarm systems**.

BS EN 12320: **Building hardware. Padlocks and padlock fittings. Requirements and test methods**.

BS ISO/IEC 27001: **Information technology. Security techniques. Information security management systems**.

BS 8418: **Installation and remote monitoring of detector-activated CCTV systems. Code of practice**.

EN 50132-7: **CCTV surveillance systems for use in security applications. Application guidelines**.

BS 1722-10: **Fences. Specification for anti-intruder fences in chain link and welded mesh**.

BS 1722-12: **Fences. Specification for steel palisade fences**.

BS 1722-14: **Fences. Specification for open mesh steel panel fences**.

BS 1722-17: **Fences. Specification for electric security fences. Design, installation and maintenance**.

SSAIB:

Code of Practice for Temporary Alarm Systems.

LPCB:

Loss Prevention Certification Board (BRE Global Limited) Loss Prevention Standards:

- LPS 1175: **Requirements and testing procedures for the LPCB approval and listing of intruder resistant building components, strongpoints, security enclosures and free-standing barriers**.
- LPS 1224: **Requirements for companies providing secure asset registration services**.
- LPS 1225: **Requirements for the LPCB approval and listing of asset marking systems**.
- LPS 1277: **Requirements for LPCB Approval and Listing of Alarm Transmission Equipment**.

RISCAuthority documents:

- BDM10: **Code of practice for the protection of empty buildings. Fire safety and security**.
- S4: **The selection and use of electronic security systems in empty buildings**.
- S6: **Electronic security systems: guidance on keyholder selection and duties**.
- S10: **Guidance for the protection of premises against attacks using vehicles (ram raids)**.
- S11: **Security of emergency exit doors in non-residential premises**.
- S12: **Police response intruder alarm systems: ten-step guide for purchasers**.
- S16: **Guidelines for shop front protection**.
- S7: **Security fog devices**.
- **Essential principles for the security of property** (in preparation).

(These documents may be downloaded from: www.riscauthority.co.uk)

Fire Protection Association
London Road, Moreton in Marsh
Gloucestershire GL56 0RH, UK
Tel: +44 (0)1608 812500 Fax: +44 (0)1608 812501
Email: administrator@riscauthority.co.uk
Website: www.riscauthority.co.uk

RISCAuthority

administered by FPA Fire Protection Association