Griffiths & Armour

SECURITY

RISK DIRECTORY 2021/2022

Griffiths & Armour

SECURITY
RISK DIRECTORY 2021/2022
INTRODUCTION

Each year, hundreds of thousands of burglaries occur at business locations throughout the United Kingdom. As such, it is considered important for businesses to establish appropriate security protections to minimise the risk of theft, damage following burglary and potential arson attack, the latter being the cause of approximately 40% of all fires.

Undertaking a security risk assessment is good practice and it is recommended that opportunities to re-assess security be considered, particularly when constructing or moving into a new building, when refurbishing or altering an existing site, or following a security breach.

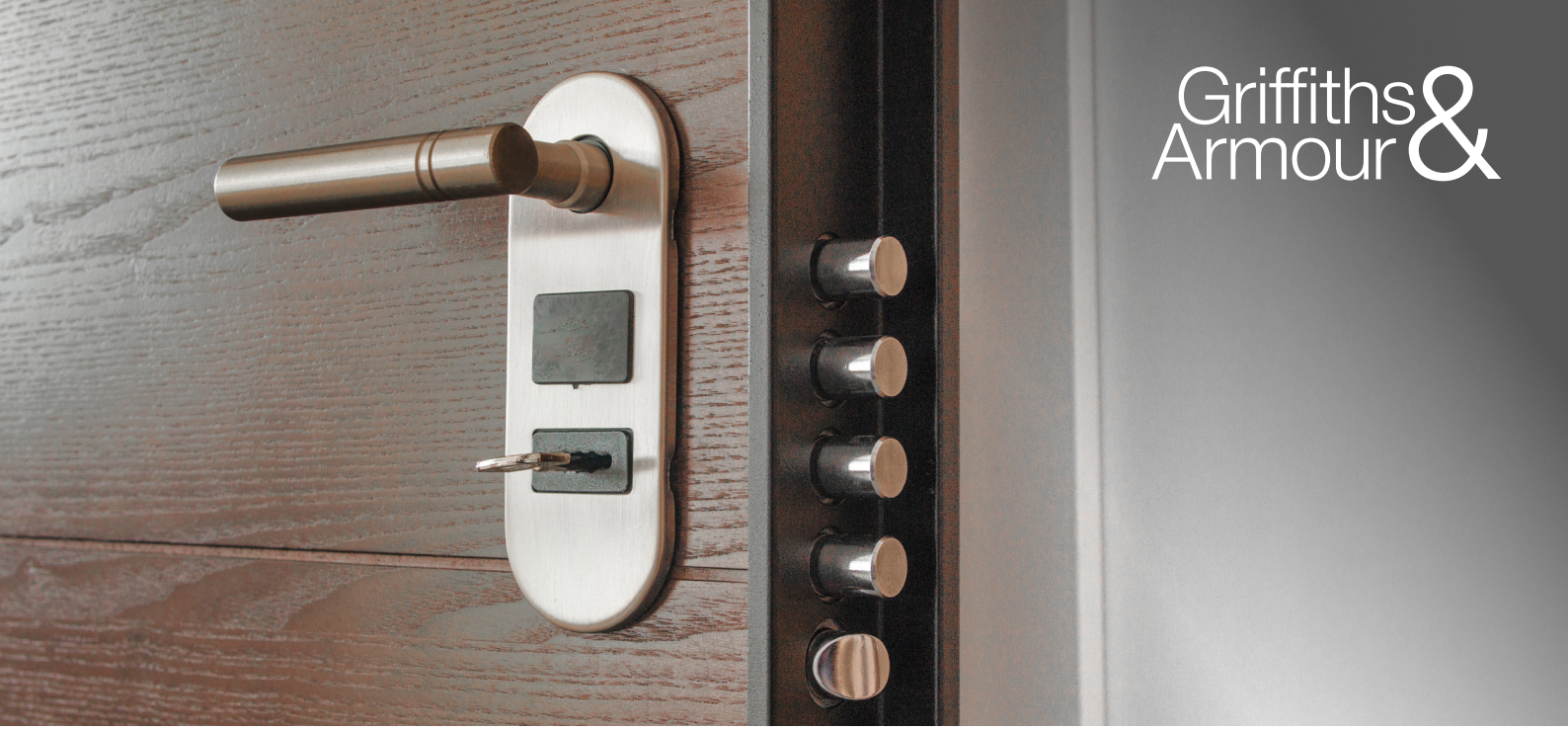
This guidance seeks to highlight some of the protections that may beestablished and is broken down into four main sections:

PHYSICAL PROTECTIONS

ELECTRONIC PROTECTIONS

SECURITY STAFFING

PROTECTIONS TO HIGHER RISK ITEMS OR AREAS



PHYSICAL PROTECTIONS

DOORS

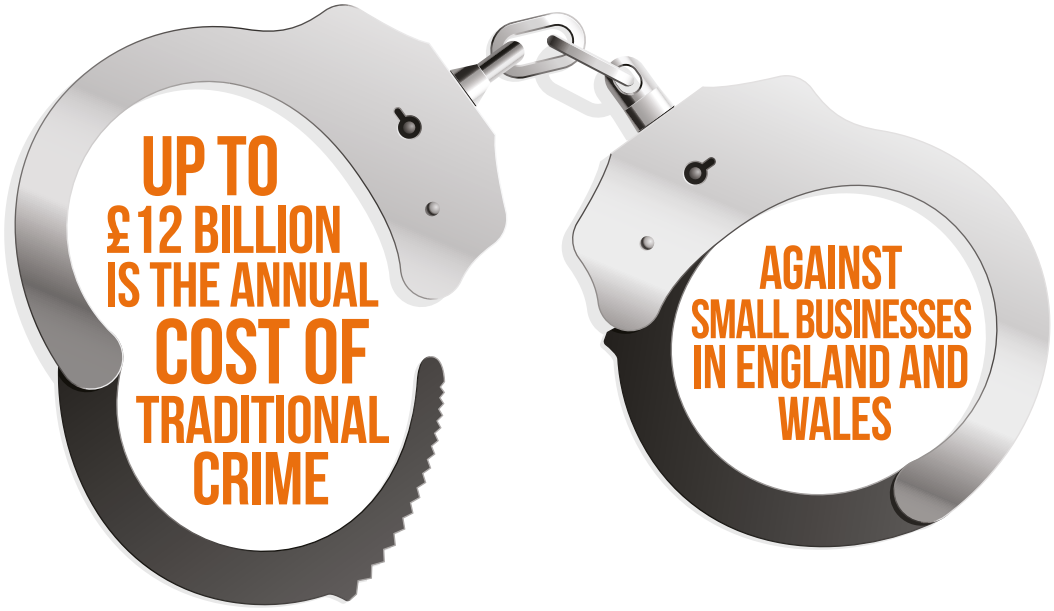
The following are recommended for consideration:

- The number of external doors should be minimised, as far as is practicable. They should be of solid construction, with a minimum thickness of 44mm (for wooden doors). For external fire exit doors and all other external doors that open outwards, it is recommended that these be fitted with hinge or dog bolts to the hinged side of the door, one near the top and one near the base. For higher risk locations where panic bars are utilised, it is recommended that external fire exit doors be protected with external sheet steel secured to the doors by either coach bolts or non-return screws. Where possible, the metal plate should overlap the door edge and part of the frame. As an alternative, solid steel security doors and frames of both standard and heavy gauge steel, are available which have integral dog bolts.
- As a minimum, locks in external doors should comply with BS3621 or incorporate cylinders that have been certified to BS EN1303. Care should be taken to ensure that locks are fitted with the appropriate steel-boxed striking plate. For higher security applications, reference should be made to LPS (Loss Prevention Standard) 1175.
- Larger external doors should ideally be secured by close shackle padlocks (minimum 5-lever or 6-pin tumbler mechanism) on a substantial locking bar, or, as an alternative, shutter doors can be secured by cylinder bolts, which are inserted into either side of the guide rails. For electronically operated larger external doors, it is recommended that these be fitted with lockable power isolators secured with padlocks as specified above and any override chains similarly secured.
- Glazing in external doors can prove to be a weak point, particularly where doors operate on an internal panic bar system or snib, and such instances should therefore be minimised (subject to approval by the local Fire Officer for designated fire escape doors). Where this is not possible, additional protection to glazing should be considered.

WINDOWS AND SKYLIGHTS

It is recommended that, as a minimum, all accessible opening windows (such as those at ground floor, basement and upper floor areas that can potentially be reached without the use of a ladder), be fitted with key-operated window locks. Alternatively, windows that are not required to open can be permanently secured shut.

For higher risk situations, consideration should be given to the installation of internal steel grilles, shutters, trellis gates or bars. For grilles and shutters, these may be approved to LPS1175. Where bars are considered appropriate, these should, as a minimum, be solid mild steel, at least 20mm in diameter, spaced at 100mm centres and have horizontal tie bars at no more than 600mm apart. Whilst window protections installed externally can reduce the risk of windows being broken as a result of vandalism, particular care should be taken so as not to provide an access or climb point to higher windows, floors, roofs, etc. It should be noted that the fitting of external shutters may require planning permission from the local council if the feature extends beyond the building line.



FENCING

Fencing often forms the first barrier against any potential intruder. As a starting point, it is suggested it be ensured that fencing meets the appropriate British or European Standard. Fencing used for security purposes should ideally not be below a minimum height of 1.8m and, where possible, be fixed to a concrete-based foundation to prevent both lifting and under-crawling. There are a variety of fencing types available and some of these are considered, in order of preference, as follows:

- **Weld Mesh Fencing**

  Provides an excellent level of resistance, whilst maintaining good visibility.

- **Steel Palisade Fencing**

  Very robust, subject to the proper use of vandal resistance rivets, sheer bolts and saddle head bolts to prevent the removal of individual sections. Unless looking at the fencing head-on, visibility can be impaired.

- **Metal Railings**

  Whilst providing excellent levels of visibility, these are often installed at heights too low to prevent a determined intruder. Particular attention should be paid to horizontal tie bars and ornate, decorative metalwork, which could potentially provide footings for climbing.

- **Chain Link and 'Heras' Fencing**

  Excellent visibility, although can be easily distorted, moved and/or cut so as to limit its resistance. In addition, these weaknesses can lead to a high level of maintenance being required.

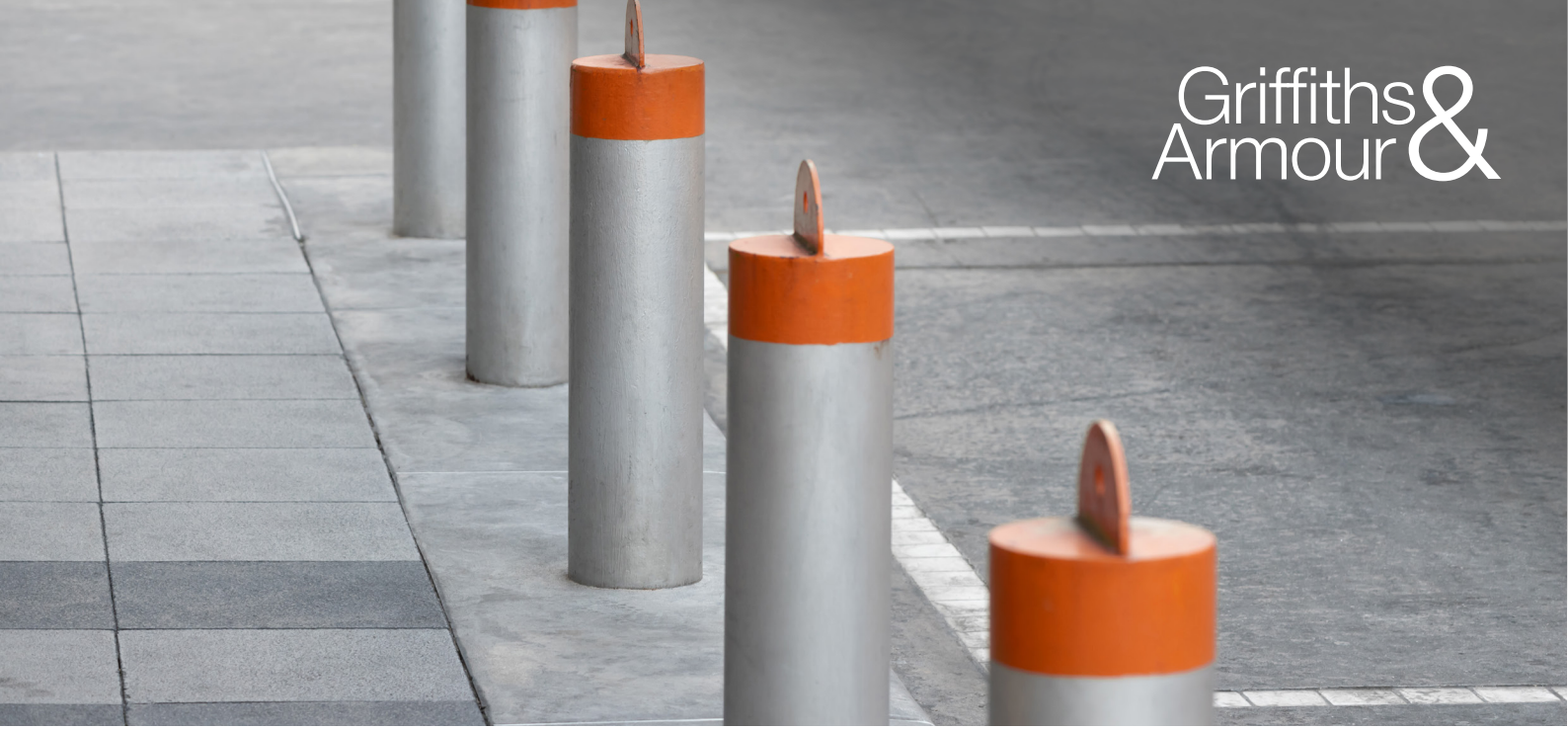
- **Hedges**

  Poor visibility and should generally only be used to supplement other perimeter protections. Layout should be carefully planned so as not to create blind spots.

- **Timber Fencing**

  Often of little structural integrity and installed to heights below recommended levels. As a result, it should generally only be considered as a means to identify a boundary, rather than protect it.

The security of fencing can potentially be improved by fitting the fence with barbed wire, razor wire, concertina coils or anti-climb spikes to prevent injury to third parties. These should be restricted to those fenced areas that are not readily accessible. It is recommended that when considering the same, reference should be made to the local Crime Prevention Officer and/or Local Authority. In some circumstances, such as high-risk situations, power or alarmed fences can be appropriate.



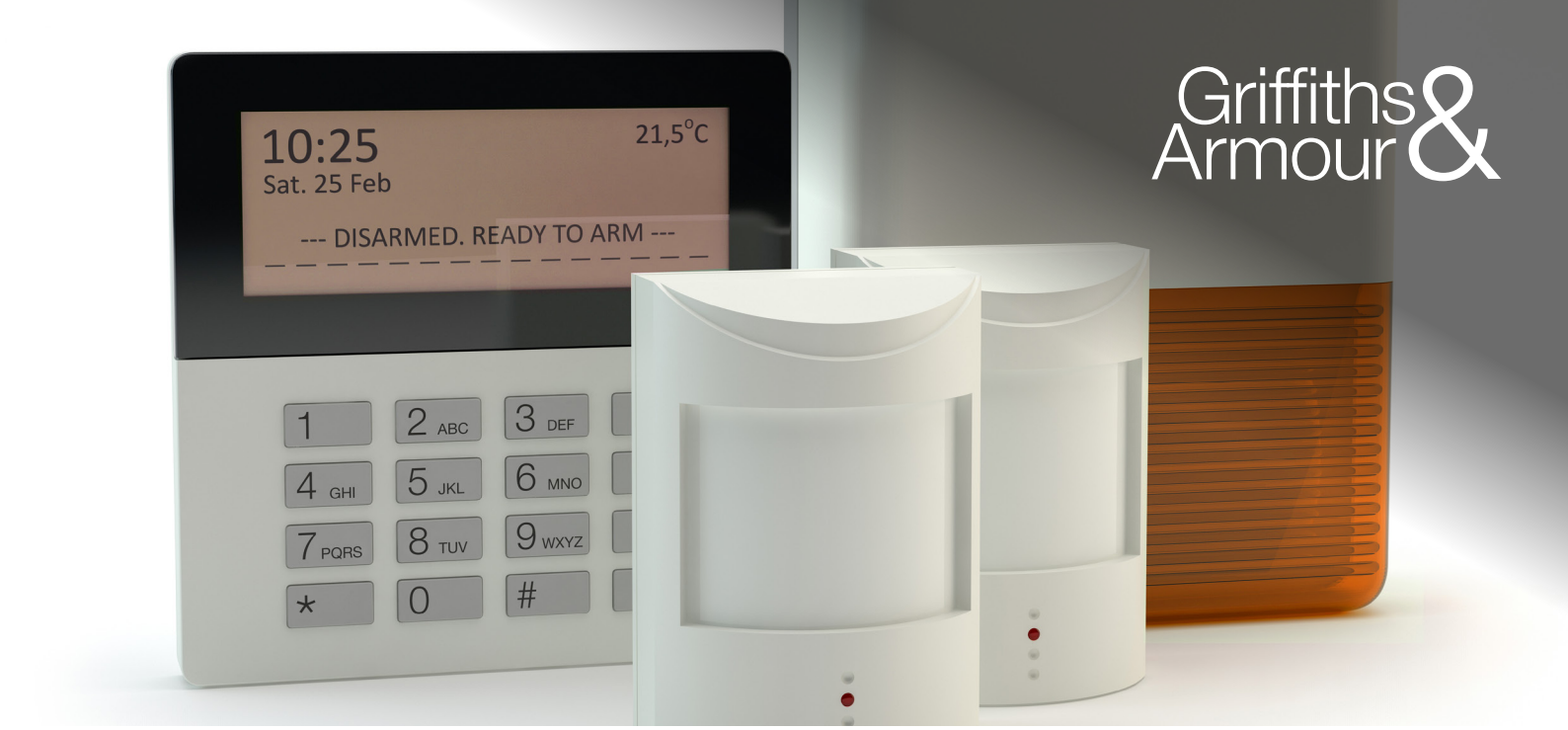
GATES

These should always be considered as a continuation of the fence and, as such, should be of similar strength, security and height. Ideally, the width of gates should fill as much of the opening as possible. Hinge pins should be either reversed, or another means of protection devised, to prevent gates being lifted off their hinges. They should be secured by heavy-duty, close shackle padlocks (with a minimum 5-lever or 6-pin tumbler mechanism) on permanent hasp and staple. The use of chains should be avoided whenever possible. Where large or double gates are used, locking bolts should be installed on the first closing leaf of the gates.

BOLLARDS

Largely used to restrict or protect against vehicle access and ram raids. Bollards come in a variety of forms and these include fixed, removable, hinged or telescopic. Where bollards are required to be locked in place, this should be either by a minimum 5-lever or 6-pin tumbler, close shackle padlock fitted to permanent hasp and staple.

42% OF REPORTED BUSINESS CRIME IS ROBBERY AND BURGLARY



ELECTRONIC PROTECTIONS

INTRUDER ALARM SYSTEMS

All new Intruder and Hold Up Alarms (HUA) have to be designed and installed to the European Standard BS EN 50131: standard in accordance with PD 6662:2017 and BS8243 for monitored systems. The Standard defines four grades of alarm system, which determine the performance and resilience of the equipment and the degree of protection afforded. Whilst, for detailed information, reference should be made to the Standards themselves, in layman's terms, individual grades can be summarised as follows:

Grade 1: Only suitable for very low-risk situations.

Grade 2: A reasonable quality system, suitable for most residential property and lower risk commercial or industrial application.

Grade 3: A system suitable for some higher risk residential properties and mainstream commercial or industrial application.

Grade 4: A system suitable for very high-risk situations, such as a bank or a jewellers.

It is also recommended that systems should be installed by companies approved by insurers and a relevant accreditation body, such as the NSI (National Security Inspectorate) or SSAIB (Security Systems and Alarms Inspection Board). Detection should normally, as a minimum, comprise of magnetic contacts to all external doors and movement detection to main thoroughfares and higher risk areas. Movement detection is typically provided by passive infrared, microwave or dual technology detectors (combining two forms of detection so as to minimise the incidence of false alarms). Other forms of intruder alarm detection include break glass detectors, window foil, tube or lace wiring, vibration sensors, infrared beams and personal attack buttons.

In all but very low-risk situations, intruder alarms should signal to an Alarm Receiving Centre (ARC), which again should be approved by Insurers and an accreditation body.

A variety of methods of remote signalling are available and a summary of some of these is provided as follows:

- **Autodialler and/or SMS Sender**

  Plays and/or sends a voice or text message to a pre-programmed number upon alarm activation. Potential weaknesses include the message quality becoming distorted over time and, if the telephone line is cut, the signal will not be transmitted.

- **Digital Communicator**

  Transmits digital information over the telephone line to an ARC. Potential weaknesses include that, as the line is not continuously monitored, the ARC will not be notified if the telephone line is cut.

- **BT Redcare**

  Operates on a similar basis to a digital communicator with the exception that, as the line is continuously monitored, should it be cut, the alarm-receiving centre is alerted. Potential weaknesses include that, for confirmable systems (see overleaf), the telephone line being cut would only be considered as a preliminary activation with no remaining means to communicate full activation.

- **GSM and GPRS**

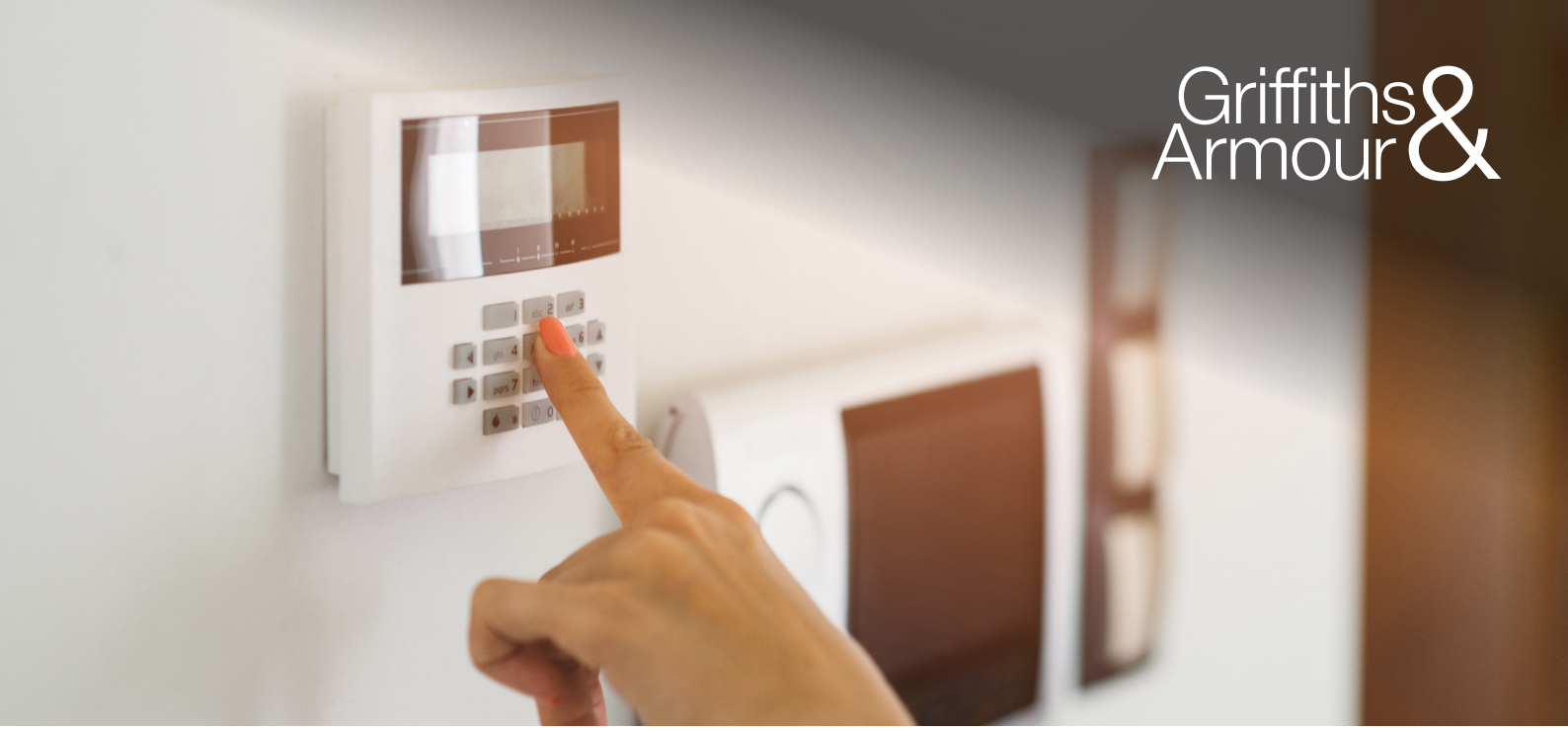
  Provides a similar service to that of Redcare, but via a mobile phone network. Potential weaknesses include that, whilst the line is polled (i.e. a signal is periodically sent to check communication is still in place), the checking process is not continuous. The potential also exists for the system to be jammed and coverage or signal strength may be limited in more remote locations. It should be noted that GPRS systems can be more complex and provide greater flexibility over GSM.

- **Dualcom**

  Utilises two signalling paths (otherwise referred to as 'confirmed signalling') combining a digital communicator and mobile network signalling. Limitations include mobile phone coverage or signal strength may be limited in more remote locations and the lines are not continuously monitored (although the provision of a secondary communication link can reduce the impact of this). Recent improvements in 'polling' frequency (i.e. how often checks are made to ensure that communication lines are intact) has led to the introduction of a new service referred to as Dualcom Plus and DualCom GPRS G4, which is generally considered by insurers as an acceptable alternative to Redcare GSM or Redcare Secure (see below).

- **Redcare GSM and Redcare Secure (GPRS)**

  Another form of confirmed signalling, this time combining BT's Redcare system with GSM or GPRS mobile network signalling. These forms of signalling are generally considered to be the most secure forms of signalling.



Griffiths & Armour

Any newly installed intruder alarm systems, or existing alarm systems with false alarm activation problems are required to meet certain criteria for Police response. Such systems will only qualify for a Police Unique Reference Number (URN), and thus Police response, if they include confirmable detection technology. Confirmable technology is when alarm systems are required to be 'confirmed', be it by either sequential, audio or visual verification. This is when more than one separate detector, camera and/or microphone is activated to determine whether a break-in is in progress. Two activations received within a short period of time confirm the high probability of a genuine or attempted break-in. For example, the first alarm signal (unconfirmed alarm) is generated when an intruder enters the building and activates a detector. If another detector or device is activated, a second (confirmed alarm) signal is sent to the ARC. Only then are the response authorities notified.

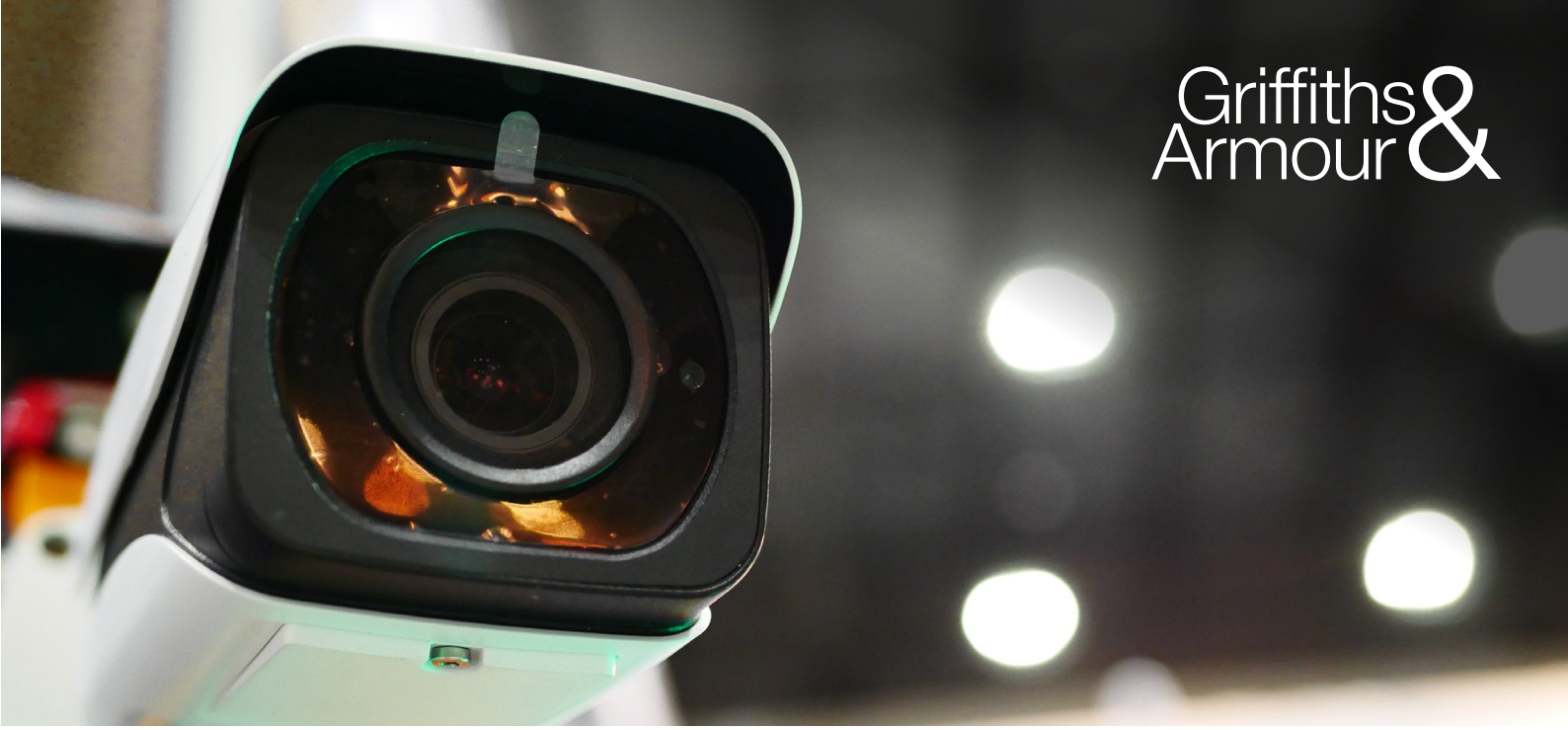
Alternatives are:

Sequential: Where more than one alarm detector is activated.

Audio: Using microphones placed around the premises enabling the alarm-receiving centre to listen to confirm the presence of an intruder.

Visual: Using cameras allowing the alarm-receiving centre to visually confirm the presence of an intruder.

Whilst not forming part of the Police requirements, it is strongly recommended that such systems be utilised in conjunction with confirmed signalling methods so that, should the primary signalling line be cut, alternative means of communicating the required second/full activation is available.



CLOSED CIRCUIT TELEVISION SYSTEMS (CCTV)

Where closed circuit television systems are monitored by on-site guards, staff or an Alarm Receiving Centre, these can provide a particularly effective deterrent. When specifying such a system, it is recommended that this be in accordance with relevant standards, such BS 8418 and/or BS EN 50132, and be installed by an approved installer, such as one recognised by the NSI (National Security Inspectorate). It is strongly recommended that such systems incorporate 24-hour recording, ideally via digital means. Where such provision is made, it is further suggested that recorders be located in a secure area.

The requirements of the Data Protection Act 2018 should also be considered and further information in this regard is available here:

READ MORE

ACCESS CONTROL

Controlling access to the main entrance doors of buildings and to strategic internal areas, can minimise the risk of loss of assets as well as safeguarding staff. Access control solutions range from basic mechanical door locks to intelligent fingerprint and eye scanners and various technologies in between.

SECURITY LIGHTING

Security lighting can be a useful deterrent, particularly in areas where surveillance is possible from neighbouring property or passers-by. To ensure that the system operates effectively, it is recommended that it be automatically activated by means of, for example, a photoelectric cell, time switch or passive infrared movement detector.

SECURITY STAFFING

Security staffing is often considered expensive, however for higher risk establishments this can still be the most cost-effective way of properly managing security risks. Normally the duties of such guards principally revolve around controlling access and egress, conducting site patrols, monitoring and responding to electronic security systems (such as CCTV cameras and intruder alarm systems).

When considering the use of security staff, it is suggested that companies be recognised and registered with an appropriate body, such as the NSI, and individuals meet any necessary licensing requirements. Further information on approved contractors is available here:

READ MORE

The following are also put forward as areas for consideration:

- Patrols should be undertaken at minimum hourly intervals, ideally recorded by some mechanical or electronic means as, unfortunately, the use of logbooks can be open to abuse.
- Guards should be provided with a means of communication, so as to allow them to summon assistance or an emergency response.
- Where guards are based within the area they are employed to protect, it is recommended that, should this area be protected by an intruder alarm system, this be zoned so as to keep other parts of the system live. It is further recommended that, where an intruder alarm is installed, the alarm-receiving centre be provided with the guard's contact details to facilitate an immediate response.

PROTECTIONS TO HIGHER RISK ITEMS OR AREAS

Examples of higher risk items include: cash; electronic office equipment (for example, computers, laptops, projectors, video and digital cameras); flat screen televisions; commercially sensitive documents; non-ferrous metals (for example, copper or lead); power tools; spirits; cigarettes; and objet d'art. Any area containing or providing access to high values or concentrations of such items may be considered higher risk.

Where higher risk items or areas are identified, the following are recommended for consideration:

- Limit the extent of higher risk items or areas as far as possible.
- Store higher risk items in relatively inaccessible areas. Whenever possible, avoid storage on accessible floors, for example basements and ground floors, or in areas in close proximity to accessible external windows.
- 'Out of sight is out of mind' – higher risk items or areas should be sited so as not to be visible to visitors and passers-by. The use of window blinds or mirrored glazing may assist in this regard.
- Install a security enclosure, such as a high security cabinet, safe, or a specific internal strong room into which access is restricted.
- Locate higher risk items in areas that are constantly attended or monitored by responsible members of staff.
- Establish property-marking systems to render any stolen goods readily identifiable.
- Enhance general security protections in the immediate vicinity, such as doors, locking devices, the intruder alarm system, CCTV coverage and access control systems. The installation of panic buttons and staff security training should also be considered for high-risk situations.

GRIFFITHS & ARMOUR RISK MANAGEMENT SERVICES

Risk management is a cornerstone of Griffiths & Armour's proposition. Simply put, good quality risk management practices lead to fewer incidents and claims, which in turn help minimise premium spend and retained costs. Our guiding principles for risk management are innovation, practicality and focus on your desired end result, which can be anything from premium reduction to legal compliance. This, coupled with our core belief that you should get the very best we have on offer from day one, ensures a strong partnership based on communication, trust and transparency. Specialisms include:

- STRATEGIC RISKS
- BUSINESS CONTINUITY AND SUPPLY CHAIN
- CYBER RISKS
- ONLINE RISK MANAGEMENT SYSTEMS
- LIABILITY CLAIMS DEFENSIBILITY
- HEALTH, SAFETY AND ENVIRONMENT
- MOTOR FLEET RISK MANAGEMENT
- PROPERTY RISKS

If you would like to discuss any of these risk management services please contact us on 0151 236 5656 or by **email**.

ACKNOWLEDGEMENTS, REFERENCES AND RECOMMENDED FURTHER READING

- A Specifier's Guide to the Security Classification of Access Control Systems - BSIA
- Users' Basic Guide to Access Control - BSIA
- Windows and Doors: Security of Windows and Door Products - Glazing Manual Data Sheet - The Glass and Glazing Federation
- The NSI and SSAIB Directories of Approved Companies and Recognised Installers
- Code of Practice for Digital Recording Systems for the Purpose of Image Export to be used as Evidence - BSIA
- Security Systems: Police Response to Security Systems 2014 - ACPO
- Audible-Only Intruder Alarm Systems - Summary of Insurers' Typical Requirements - S13 - RISC Authority
- Police Response Intruder Alarm Systems - Summary of Insurers' Typical Requirements - S14 - RISC Authority
- CCTV Code of Practice - The Data Protection Commissioner

LEGAL NOTICE

Insurance Brokers and Professional Risks are divisions of Griffiths & Armour, a partnership which is authorised and regulated by the Financial Conduct Authority.

Risk management services are not regulated by the Financial Conduct Authority.

This document does not provide legal advice and is not a substitute for obtaining specific legal advice in order to protect the interest of your business. Should you require legal advice on any of these matters, please contact your legal adviser. It is intended only to highlight issues that might be of interest to Griffiths & Armour clients. The contents of this document are based primarily on the legal position under English law and may be subject to change. Further, more detailed advice may be appropriate in relation to other jurisdictions in which you work. Where links to third party websites are provided, we accept no responsibility for their content.

Griffiths & Armour

OUR VALUES:

SUPPORTIVE

PERSONAL

PROACTIVE

RELIABLE

& that's the difference

griffithsandarmour.com

Assurex GLOBAL

Insurance Brokers Chartered

IB0175