ALEXANDER BONHILL

Security

Risk Management Guide

INTRODUCTION

When planning security for any commercial premises, consideration should be given to securing the external areas of the site first, followed by further levels of defence built-up depending on location, nature of the business enterprise and the values at risk. The following security provisions should be considered:

PERIMETER SITE SECURITY

- Is it practical to fence the site with security gates at entrance points? There is a wide variety of fencing systems available. Any system considered should confirm to BS 1722.

- Should external CCTV be considered (together with appropriate lighting)? Camera systems that are remotely monitored can provide a useful means of confirming criminal activity and alert keyholders or the Police. If a monitored CCTV system is required, this should be designed, installed and maintained by a company that is ISO9002 certificated and approved by a UKAS accredited inspectorate. The installation should comply with BS8418:2015.

- Alternatively, manned security of the premises may be preferable. If so, National Security Inspectorate (NSI) minimum Silver Standard companies should be appointed. The company should also comply with BS7872:2011, standard for manned guarding services in the UK.

For more help and advice, please visit www.nsi.org.uk

PHYSICAL SECURITY PROTECTIONS

The type and standard of physical security should be appropriate for the location and nature of the business. As a minimum, this should comprise:

- Key operated window locks to all ground floor and accessible windows;

- Security bars or grilles fitted to vulnerable windows in areas containing valuable goods;

- Timber personnel doors secured by mortise deadlocks conforming to BS3621:2017 or fitted with heavy-duty locking bars and padlocks. Where there is a requirement for means of escape (from fire) from the inside without the use of a key while maintaining security from the outside, lock assemblies to BS8621:2017 keyless egress should be fitted. An alternative lock, BS10621:2017, provides a function whereby the operating mode can be switched between the normal BS8621 operating mode and a secure mode in which no egress is possible – this is useful in a situation where a person is the last to leave and is responsible for closing down the building.

- Access control systems to prevent a 'walk-in theft';

- Roller shutter, folding or sliding doors secured by a heavy-duty locking bar and padlock, shutter guide bolts or padlocked operating chain. If there are translucent plastic viewing panels within the sectional shutter door, additional grilles or bars should be fitted.

INTRUDER ALARM PROTECTIONS

Unless occupied 24 hours per day, all commercial/business premises should be fitted with a form of intruder alarm protection. There are various standards in the UK for the design, installation, maintenance and signalling of alarm systems and further information is available at **hmlgroup.com**.

OTHER SECURITY CONSIDERATIONS
COMPUTER SECURITY

Fixed and portable computer equipment is highly theft attractive and certain items such as servers, CAD systems are particularly vulnerable. Consideration should be given to securing such equipment to the workstations or the fabric of the building using proprietary encasement security devices conforming to test standard LPS 1214, installed by the manufacturer or an accredited representative. Laptop computers should be removed from the premises outside business hours or alternatively secured within a suitable locked drawer or cabinet.

SECURITY CABINETS

Small, high value stock, plant or equipment (such as portable power tools) should be stored in a suitable secure cabinet or vault whenever the premises is unattended. If tool chests are to be used, be aware that these are often targeted by thieves who know they are likely to contain valuable equipment. Consideration should therefore be given to chaining and padlocking these to a suitable, fixed, anchored point of the premises using a chain approved to 'Sold Secure' Gold Standard and padlock satisfying the requirements of BS EN 12320 CEN Security Grade 4 or higher.

SMOKE GENERATING DEVICES

Areas such as computer server rooms or shop front window displays are particularly vulnerable to theft and the installation of a suitable smoke generating security system should be considered. Any system is to be designed, installed and maintained in accordance with BS EN 50131-8:2019 Alarm Systems; Intrusion and Hold-Up Systems; Security Fog Devices.

SECURITY MARKING

Permanently marking valuable or business critical equipment with your business name and postcode may deter theft or aid the Police and potential recovery of stolen assets. A number of security marking products are available ranging from security etching to sophisticated concealed marking.

KEY SECURITY

Many businesses live to regret leaving keys where they are easy to steal or copy. Keys that cannot be kept on your person should be stored in a locked security safe or proprietary metal key cabinet. Access to this safe should be restricted and it should be located in a concealed position within the premises, preferably within an alarm protected area.

MONEY & CASH HANDLING

If you handle large volumes of cash as part of your business operation, a specific Cash Handling Policy should be provided and communicated to staff on a signed receipt basis. This should include:

- Cash handling procedures;
- Till management;
- Banking/cash collections;
- The use of Personal Attack/Hold-Up alarms linked to the premises intruder alarm system

In most instances, a suitable, proprietary cash/security safe will be required to store cash before it is deposited in the bank or collected by a professional security company. Safes have a specific 'rating' determining the maximum amount of cash that can be safely deposited and this rating should be adequate for business needs and not be exceeded.

Where a safe is provided, insurers normally require keys to be removed from the business premises when the premises is unattended.