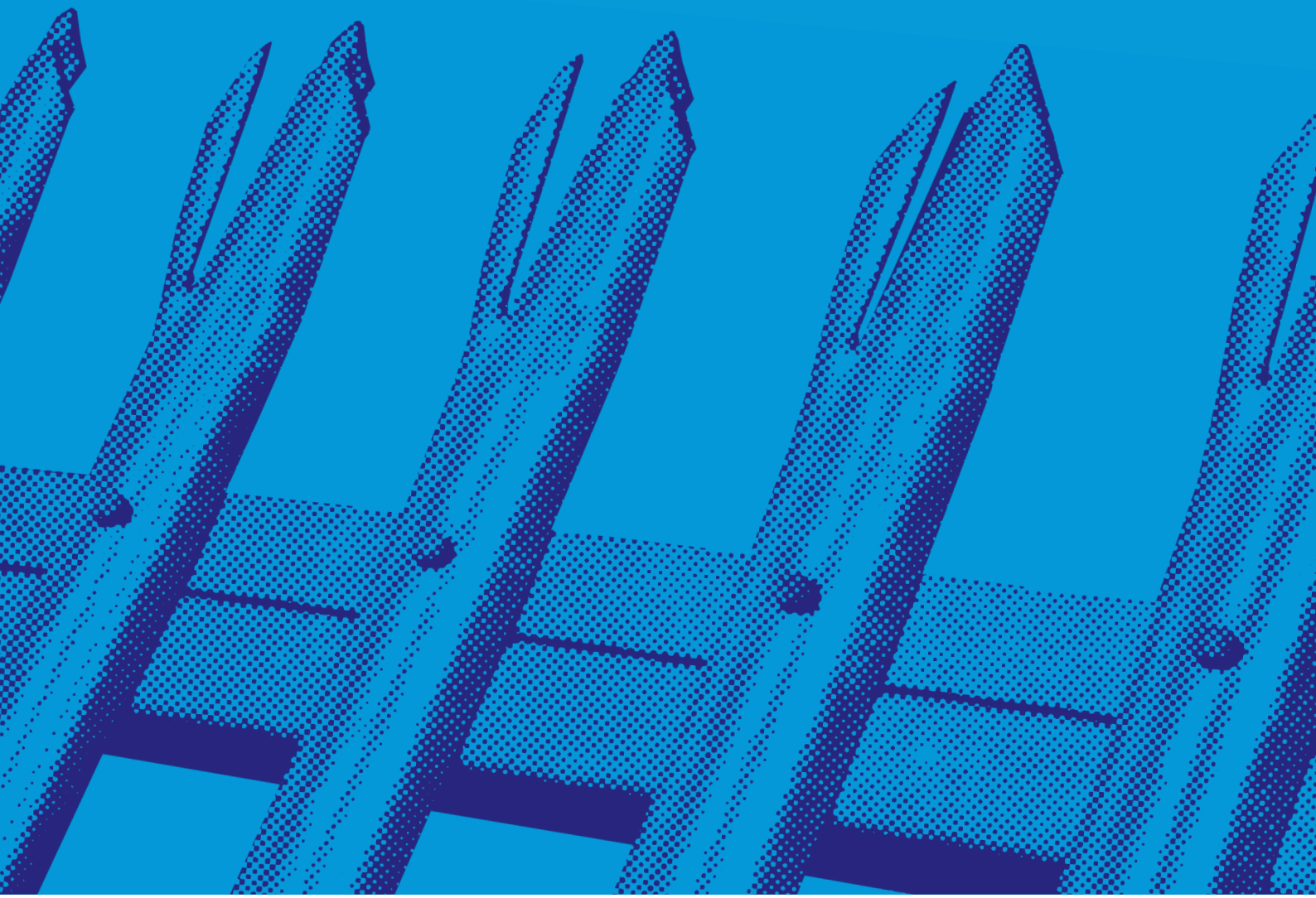
S20
First published 2012
Version 01

Security

Essential principles for the security of property



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

INTRODUCTION

There are generally no specific requirements made of people to adopt set levels/types of security at their premises (whether buildings or land); any mention of security in legislation/regulations, eg Building Regulations, usually being in the context of what one is not allowed to do, eg not fit certain types of key locks to emergency escape doors/windows, etc.

That said, there may be an implied need to have in place adequate security by virtue of a duty of care, eg to prevent access to premises where danger may exist, and in addition there are some voluntary schemes that might require particular levels of security, for example the Secured By Design (SBD) scheme or National House Builders Council (NHBC) guidance.

Security measures are often considered in terms of these three broad categories:

- *physical security;*
- *electronic security; and*
- *human security.*

Whilst much of the available security guidance tends to concentrate on the first of these – passive (physical) security, which indeed is often a fundamental measure – security may sometimes need to rely upon active security measures, eg electronic and/or human surveillance. In fact, passive and active measures are generally complementary, and in that spirit extending security planning to consider many other basic principles is usually also necessary to help achieve in-depth security.

RISCAuthority publishes a range of documents on the security of physical assets, with this document identifying the basic ten protection principles underlying many of the recommendations contained within them.

SCOPE

This document has been prepared to outline the basic steps that should be considered when planning new, or reviewing existing, security measures and is intended to assist those designing, specifying, purchasing and implementing security measures intended to manage the risks to physical property of theft and malicious damage (including arson). For the most part the principles can also be applied to the security of intangible assets such as intellectual property.

PRINCIPLE 1

A security risk assessment should be undertaken.

This should take account of all factors likely to have an impact on security, and will therefore need to consider the following:

- *what property (target assets) could attract criminals;*
- *what are the target asset values, typical and maximum, eg seasonal;*
- *when are they present, eg permanently or temporarily;*
- *where are they located;*
- *what are the high/low risk periods, eg during or after trading hours/site occupancy;*
- *the likelihood/nature of the expected crime, for example*
  - *theft;*
  - *burglary;*
  - *robbery;*
  - *vandalism;*
  - *arson;*
  - *fraud; or*
  - *unauthorised IT systems access – 'hacking';*
- *the likely monetary, commercial and personal impact of crime; and*
- *the nature, depth and adequacy of existing precautions.*

Only once this systematic assessment has been completed can relevant and cost-effective measures to improve security be realistically considered.

PRINCIPLE 2

The need for and/or benefit of liaison with others should be considered.

There may be other people/organisations that have a legitimate interest in your security arrangements and will wish to influence, or otherwise advise upon, them. For example, they may have a financial stake in the situation, eg as an insurer; because of public policy, eg a neighbourhood crime initiative or large site policing/emergency response duty; or because of safety considerations of personnel who may be called to site as a result of a criminal activity, eg police or security response personnel.

PRINCIPLE 3

Reduction or elimination of intrinsic risk should be considered early in the process.

Before money is spent on improving security, it is sensible to ask if it needs to be spent at all as the need for security may be reduced by either, or a combination of, risk removal or risk reduction measures.

Removing items of attraction

Where practical, eliminating target assets can be a cost-effective option, eg not accepting cash payments, removing vehicles etc.

Risk reduction

Where target assets have to remain, the exposure to loss can be lessened by reducing the amount/value of those assets, eg holding lower stocks or arranging for more frequent cash banking, etc. Another strategy might be to split target assets between several locations, for example keeping cash in several safes.

If risk removal/reduction has only limited success in removing/reducing risk, that which remains should be managed by other means.

PRINCIPLE 4

A security strategy, tailored to the circumstances, should be adopted.

Using a recognised security strategy to plan your security measures is likely to encourage a rational, integrated approach, and is thus more likely to result in an effective outcome.

The selected security strategy should be supported by documented policies/procedures and an appropriate level of management control.

There are several security strategies mentioned below that can be adopted and, whilst they may be considered in isolation, they are often used to best effect if considered alongside each other. For example, if using a 'layered approach' consider to what extent each security measure provides one or more of the 'Four Ds'.

Layered security

This is an approach whereby amplification of the overall value of individual security measures is achieved by ensuring a succession of barriers to crime exists, eg from the perimeter of a premises inwards. This is sometimes also referred to as the 'onion skin' principle.

Within this approach if assets vary widely in their likely appeal to criminals and relatively few high risk items exist, it can sometimes be a more cost-effective option to locate the assets most at risk within a high security envelope, sometimes referred to as a 'strongpoint', and concentrate security measures at that point.

Four Ds

With this approach you need to consider whether a particular security measure, or several working in combination, help to:

- *deter;*
- *detect;*
- *delay; and*
- *defend.*

***Deterrence** affects all criminals, and typically results from measures that are clearly visible (overt), eg a perimeter fence, well constructed/secure buildings, a guard presence or an electronic security system. However, measures that are not readily visible (covert), eg forensic marking, disguised CCTV cameras, etc. can be still be effective, but ideally such measures need to be 'advertised' eg using notices such as 'staff do not have access to the safe'. In fact, in the case of covert CCTV, warning notices will almost certainly be mandatory (see the Information Commissioner's CCTV Code of Practice).*

***Detection** of criminals can be achieved through use of site personnel, security guards or an electronic detection system. The aim always being to recognise an incident requiring intervention early on, to prevent or otherwise minimise loss or damage.*

***Delay** of criminals typically occurs when a series of measures increases the amount of time taken for them to reach their objective. For example, the use of several strong physical barriers, requiring criminals to penetrate deep inside premises, and/or storing assets in a way that demands time and effort in removal.*

***Defence** against criminal activity is initiated in response to its detection, ie the active steps taken to prevent or limit a loss once an incident is recognised. This usually occurs at the time, eg through prompt intervention but may come later through steps taken to prevent a repeat attack using the same criminal method.*

PRINCIPLE 5

The potential benefits of both passive and active security measures should be considered.

A passive security measure can be regarded as something that is permanently in place during any particular risk period, most typically being a physical security measure. This may be part of the site itself (eg a fence or the building shell), an item used to secure part of it (eg a door lock) or an item securing an individual asset (eg a computer entrapment device).

An active security measure can be regarded as one that either provides or otherwise enables a real time response to be made to a criminal act. It might take the form of a human presence on the site, eg staff or a security guard, and/or electronic security system(s) such as access control, intruder alarm or CCTV installation(s).

Assuming the security risk assessment concludes that remedial action is necessary to improve security, there will be some circumstances in which either only passive, or only active, security measures are appropriate. However, in many situations there is likely to be a case for adopting a mix of both passive and active measures. Where this applies, security needs to be based on an optimum (complementary) balance of passive and active security measures as, failing this, there is a danger that deficiencies in one type of measure will critically undermine the other and devalue the investment made. For example it is often the case that a minimum standard of physical protection (ie passive measure) is essential in supporting the design and reliable operation of an electronic detection system (ie active measure).

PRINCIPLE 6

Security products and services, and their providers, should be selected with care.

Security products should be selected that not only match the intended application but also have evidence of conformity with a relevant standard – ideally supported by a suitable scheme for third party certification/approval.

Various standards/codes of practice exist, designed to help determine an appropriate use and/or ascribe a security value to particular types of security product, for example:

- *European/British Standards;*
- *Loss Prevention Certification Board Loss Prevention Standards;*
- *Secured by Design scheme; and*
- *Sold Secure scheme.*

Suitable product selection can be assisted by use of competent providers.

A wide range of bodies/schemes exists by which a security provider can demonstrate their credentials, perhaps by adherence to recognised standards/codes of practice, training regimes and/or Criminal Records Bureau (CRB) checks, etc. For example:

- *Association of Security Consultants (ASC) membership;*
- *British Security Industry Association (BSIA) membership;*
- *Master Locksmith Association (MLA) membership;*
- *LPCB approved contractors;*
- *National Security Inspectorate (NSI) approval;*
- *Security Systems and Alarms Inspection Board (SSAIB) approval; and*
- *Security Industry Authority (SIA) Approved Contractor Scheme (ACS).*

Use of such providers should help ensure appropriate product/service selection, design, fitting/implementation and, as appropriate, maintenance.

PRINCIPLE 7

Users of security products and services should be suitably trained.

The best security measures can fail if those charged with adopting/using them do not have an appropriate level of understanding of their purpose, correct operation and use. To prevent this, users require a suitable level of initial and ongoing training/awareness.

PRINCIPLE 8

Adequate maintenance should be provided.

Certain security measures require routine or periodic maintenance to preserve their effectiveness in terms of ease of use, reliability and credibility. This may take the form of physical or remote inspection/servicing and/or testing of products/services.

PRINCIPLE 9

Security should be continuously reviewed.

The adequacy of security should be subject to continuous review, eg as the nature or value of the protected premises/target assets change, as external factors alter, eg an increase in crime in the area or values increase (eg scrap metal), or, in particular, after any security breach/loss.

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.

PRINCIPLE 10

Adequate records should be maintained.

The creation/retention of suitable records of the design, commissioning/installation and maintenance of security products and services, and any related training, is an important starting point for evaluating implemented security measures, providing evidence of them to interested parties, eg an insurer, and for any future security review.

APPENDIX 1: SUMMARY OF THE TEN SECURITY PRINCIPLES

Principle 1

A security risk assessment should be undertaken.

Principle 2

The need for and/or benefit of liaison with others should be considered.

Principle 3

Reduction or elimination of intrinsic risk should be considered early in the process.

Principle 4

A security strategy, tailored to the circumstances, should be adopted.

Principle 5

The potential benefits of both passive and active security measures should be considered.

Principle 6

Security products and services, and their providers, should be selected with care.

Principle 7

Users of security products and services should be suitably trained.

Principle 8

Adequate maintenance should be provided.

Principle 9

Security should be continuously reviewed.

Principle 10

Adequate records should be maintained.

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