

# Safeguarding your physical and virtual assets

**From: Facilities Management, October 2009**

Steve Garton outlines the key security issues facing facilities managers and summarises the standards with which they need to comply.

*Steve Garton is a Director at security consultancy Advent IM ([www.advent-im.co.uk](http://www.advent-im.co.uk))*

The facilities manager's role is continually evolving into a more complex and diverse position, with responsibilities encompassing multidisciplinary activities across several different environments. Within this fast-growing discipline, facilities managers have extensive responsibilities for providing, maintaining and developing myriad services. These range from property strategy, space management and communications infrastructure to building maintenance, administration and contract management.

In addition, particularly in the current climate as companies tighten their budgets and look to restructure their manpower, the facilities manager is increasingly being pulled in to assist other offices and senior management. One area where cross-departmental cooperation is particularly important in the implementation of security measures to safeguard the organisation physically and virtually. This is an area requiring greater attention than ever, with facilities managers needing to keep track of a growing range of legislative requirements, standards and guidance (see '**Legislation and Guidance**' below).

## **INFORMATION TECHNOLOGY**

With the advent of enhanced technology, businesses work in different ways and this raises the issue of whether it should be the IT manager or the facilities manager who is responsible for IT and physical security. It is important to reduce the blurring of territory as this can leave employees confused, and clear lines of responsibility will encourage a better work culture, with security raised higher up the business agenda. However, regardless of which department the security function is based in, facilities and IT managers need to work jointly on security measures.

Threats to an organisation can occur from both internal and external sources. The risk of insiders stealing information of assets has always been significant, and this threat is increasing due to the economic climate and growing numbers of staff being made redundant.

Working together with the IT team, facilities managers should ensure that there are procedures in place to restrict disgruntled former employees from entering buildings and knowing shortcuts or passwords. Although new technology is an enabler of safer systems, it is not the complete solution. Facilities managers therefore need to manage the working environment to control how technology, information and physical assets are shared and kept safe. This involves them working closely with the IT manager to control systems that protect information security. There also needs to be a back-up plan to ensure business continuity, so that if a disaster or major disruption occurs that could affect virtual and physical assets, the organisation will be able to recover and restore partially or completely interrupted critical functions in a timely fashion.

## **PHYSICAL SECURITY**

The building's physical security is another important part of the facilities manager's role. The environment and the building itself often dictate the style of the security solution. For example, organisations located in areas of environmental importance or in listed buildings will be restricted in what they can implement.

Many aesthetically pleasing buildings are seen as problematic in terms of security. However, security measures do not have to be obtrusive or costly if approached in the correct manner. Facilities managers should therefore not be deterred by the fear of a precautionary measure looking out of place as security components can be delivered to integrate aesthetically with a building profile and offer the protection required.

The first step a facilities manager should take when considering the physical security of a building is to conduct a threat assessment. This process is a relatively standard procedure, enabling the assessor to study the actual threat in the vicinity and

consider the modus operandi of the person or group that could impose a threat. This analysis then feeds into the risk assessment process, making it more defined and ensuring informed decision making.

The facilities manager should also consider where the risk lies – is it with an outsider looking to force entry or an inside worker with authorised access to the building? A thorough threat assessment will weigh up genuine risks, enabling the security solution to be based upon analytical findings and not on perception or rumour. This will pay dividends in the long term and achieve significant savings during the design phase of any security plan.

### **EXPERT ADVICE**

Those facilities managers who are lucky enough to have a source of security expertise in-house should have the capacity to address the physical security issues that affect their building. This is, however, not always the case and many facilities managers will be seeking expertise in this field on a consultancy basis. It is important that they choose a professional working for an independent security consultancy to guarantee that their findings are not biased towards any particular products and that the advice offered is impartial and directly for the organisation's benefit.

Many security companies are keen to offer a plethora of security products, including CCTV and alarms for example, when in reality fewer products are needed. Carrying out a comprehensive threat and risk assessment will make clear the type and volume of products required.

Facilities managers should ask their consultant to mentor them throughout the process, keeping them abreast of the assessment and giving suggestions to permit a useful and feasible plan of protection. Regular independent reviews are also important, which should highlight both the strengths and weaknesses of the building. A rolling review means that should threats to the organisation change or increase, the facilities manager is equipped with responses that are both cost effective and proportionate to the risk.

### **HELP NOT HINDRANCE**

A well-structured security plan contributes to the delivery of strategic and operational objectives. The right solution will be viewed as a business enabler rather than an expensive hindrance installed as an afterthought,

**FM**

## LEGISLATION AND GUIDANCE

There are a number of laws, compliance documents and guidelines that facilities managers should be aware of in a security context, including the following:

### **BS7858: personnel screening**

The British Standards Institution code of practice for security screening of personnel now urges employers to screen all individuals who have unescorted access to their premises. Originally intended for security firms, the standard is now used more widely as the benchmark for good screening procedures. In the current economic climate, fraud and crime are on the rise from both inside and outside the organisation. An employee screening process should therefore be conducted for all prospective workers, regardless of their position, in an attempt to confirm legitimacy. According to BS7858, this process should include:

- current address validation;
- a credit check and County Court judgment, insolvency and bankruptcy search;
- a five-year written employment verification;
- a Criminal Records Bureau check; and
- personal references.

[www.lexisurl.com/FM4](http://www.lexisurl.com/FM4) 7

### **BS25999: business continuity**

To ensure business continuity after a disaster or extended disruption, organisations need to create and validate a practised logistical plan for how they will recover and restore partially or completely interrupted critical functions within a predetermined time. BS25999 is the British Standard for Business Continuity Management that companies can refer to and work towards achieving.

[www.lexisurl.com/FM339](http://www.lexisurl.com/FM339)

### **ISO 27001: information security**

Information security involves protecting and defending information and information systems by managing their confidentiality, integrity, authentication and availability. ISO 27001, the International

Standard for Information Security Management, can be referred to and worked towards.

[www.lexisurl.com/FM278](http://www.lexisurl.com/FM278)

### **Security Policy Framework**

The government's Security Policy Framework contains the most recent guidance on security and risk management for government departments and associated bodies. Although security policies will differ depending on the type of business and the risks it faces, this is the source of all local security policies, so acts as a useful reference point for facilities managers.

[www.cabinetoffice.gov.uk/spf.aspx](http://www.cabinetoffice.gov.uk/spf.aspx)

### **Corporate Manslaughter Act 2007**

This Act imposes a duty on employers to protect their employees and lone workers.

[www.justice.gov.uk/guidance/manslaughteractguidance.htm](http://www.justice.gov.uk/guidance/manslaughteractguidance.htm)

### **Data Protection Act 1998 (DPA)**

The DPA regulates the processing of information about individuals, including the obtaining, holding, use or disclosure of such data.

[www.ico.gov.uk/for\\_organisations/data\\_protection\\_guide.aspx](http://www.ico.gov.uk/for_organisations/data_protection_guide.aspx)

### **CCTV**

Two documents are worth noting. First, there is the *National CCTV Strategy*, a 2007 report that reviews the use of CCTV and the legal requirements on CCTV footage, should it be needed as evidence in court for prosecution purposes.

Second, there is the *CCTV Code of Practice*, issued by the Information Commissioner's Office. This code provides best practice advice for those involved in operating CCTV and other devices that view or record images of individuals. It also covers other information derived from those images that relates to individuals (for example, vehicle-registration marks). Information on individuals held by organisations is covered by the DPA, and the guidance in this code will help them comply with their legal obligations under the DPA,

*National CCTV Strategy*. [www.lexisurl.com/FM343](http://www.lexisurl.com/FM343)

*CCTV Code of Practice*: [www.lexisurl.com/FM3752](http://www.lexisurl.com/FM3752).