System Addict…

…John Julian reviews the processes involved in designing-out crime by way of physical and electronic security system provision.

What do we actually mean when we talk about effective or efficient security? In essence, the terms centre on achieving and maintaining a state whereby your people, assets, property, information and corporate image are protected against injury, damage, harm or loss while complimenting and/or note dramatically hindering the business activities carried out by the company in question.

Although this statement is something of a mouthful, it is a useful reminder to the security manager of all those issues that will need to be addressed when it comes to planning and designing security systems for buildings.

In an ideal world, any security measures that you decide to put in place must cover all the risks posed to your organisation by its location, the building (or buildings) and the business realm within which the company operates.

An effective risk management strategy is needed in the early stages of the planning process in order to help the Board decide exactly which risks are priority.

There are several options open to you. You could mitigate the risks (i.e. take measures to limit exposure or the effects of any impact). Another option centres on transferring or sharing the risk – either through insurance or by delegating matters such as Cash-in-Transit to an external contractor. Alternatively, you could choose to spread the risk by dispersing assets over a range of sites, raise reserves or put back-up systems in place to limit any impact. You could always accept the risk of course….

Some risks are straightforward. Criminal threats such as burglary, walk-in-theft, staff / contractor / visitor theft, vandalism and criminal damage are fairly easy to identify from personal knowledge, business records and local police information. The less straightforward threats come from those that may be attracted due to the nature of your company's business, or where the premises are located.

Location, products, image and staff

With this in mind, there are various questions that will need to be asked by the security professional. Where is your business located? Are you in a high crime area? Is your company operating in areas or countries hostile to its type of business? Are you in close proximity to potential terrorist and activist figures? Who are your neighbours? Do their products, assets or activities attract unwanted attention? And what type of boundaries are there at your premises?

The security manager must also consider just how secure the company sites are from neighbouring activities or issues. Is access to your buildings, for example, gained far more readily through a neighbour's property or premises? Are you located in an area where fast access and escape is available due to the road layouts, or is the company situated in an environment where escape is aided by natural or indeed man-made cover?

Do you have the necessary safeguards in place to protect your business and the people working for it against any unwanted attention that might arise?

The fundamental nature of the business is also key. What products or raw materials does the business either create or handle, and does the very nature of those products pose any threat in itself? Here, the security manager will need to think about the personal attractiveness of what it is that the company produces, the ease and value of product re-sale, the ease of contamination and / or destruction of those products and their actual production or use.

Evaluating the nature of what's produced by your company will help the security professional no end in understanding how much effort will be expanded by thieves, activists or terrorists – and to what lengths they will go – in trying to achieve their goal. Similar questions should also be asked with respect to the assets of the business. Will the nature of what's produced on your premises – or the research and testing of those products – attract extremists? Do you have any links with companies whose operations do just that? Does the public's perception of your type of business – or event the company name – provide an association with controversial activities?

Employment within the firm is another important consideration. Security managers must think about whether or not their company's business activities might attract individuals looking for employment who have questionable characters and intentions. Do you operate in an environment where clients and employees, unique products and ideas might be attractive to competitors? In addition, exactly what controls do you have in place with regards to the employment, access and overall treatment of personnel? Such questions demand answers.

Considering the building architecture

There will always be a vast difference between designing security for an existing structure and designing a building with security in mind. Whichever way around this occurs, always look at every actual or proposed feature.

How many windows are there, and what form do they take? Do they provide good, natural lighting or would you need blinds / extra lights to enhance visibility in certain rooms? What are the windows made of, and how might they withstand various types of attack?

What are the building's interior / exterior doors made of, and how safe and secure are they? What sort of access control do they have? Will you offices be open-plan, or will there be restricted access in certain areas? What sort of protection is in place for the staff, especially the 'front of house' people? What sort of protection is there for staff working around and about the building (i.e. car park attendants and the like)? Is there adequate lighting around the building?

When considering possible threats, the security manager must learn to think in broad terms, passing beyond what is normally seen as the 'realm of security'. All-too-often the responsible security professional will consider external criminal, terrorist or activist and vendor / supplier action but will ignore staff theft – internal manipulation, malpractice, fraud and sabotage.

Ian Johnson Associates Limited - Linden Place - Seale - Farnham - Surrey - GU10 1HS.
T: (+44) (0)1252 782664 **F:** (+44) (0)1252 782818. **E:** info@ija.co.uk **W:** www.ija.co.uk

When considering possible threats, the security manager must learn to think in broad terms, passing beyond what is normally seen as the 'realm of security'. All-too-often the responsible security professional will consider external criminal, terrorist or activist and vendor/supplier action but will ignore staff theft – internal manipulation, malpractice, fraud and sabotage.

When designing a new building or moving into an existing one it's usually the case that a given company will look at making a statement about itself. Often, architects are asked to create a look. An atmosphere. A comment on the company. There is no earthly reason why the security elements cannot be designed in keeping with this.

Contrary to popular belief, it is possible to design security systems such that they're discreet. Well-skilled security experts and specialists should be comfortable in recommending systems to fit the circumstance – whether that entails a high, medium or low profile security set-up.

Designing-in security systems

The key to designing-in security lies in ensuring that you are in full view of all the facts on all the important issues that you face, and that you have the best solutions in place to be able to tackle them. As a busy individual manager, it's often difficult to remain up-to-speed with all the latest developments in security technology. Even with good security knowledge in the bank, you may still find certain elements (e.g. determining how to achieve the optimum picture quality from your CCTV cameras) outside the boundaries of your skills.

Good security consultants will be able to offer advice on the risks facing your company, and the best security systems suppliers to use by way of combating them. That said, security managers must ensure that recommendations are based on experience and results rather than any links (financial or otherwise) to particular companies.

The benefit of using security consultants is that, if they are good at what they do, they will be fully aware of the latest technology, crime trends and industry-specific risks. They should also be able to come up with a list of the best systems suppliers. It's often the case that they'll be able to project-manage your entire security design and implementation for you.
Most notably, they may and probably will identify critical cost savings in a specification or proposal without impacting on the systems capability to effectively secure and protect a building.

A good security consultant will be fully aware of the latest technology, crime trends and industry-specific risks.

When initially looking into the design, you should always consider the aims of each and every security arrangement you are about to implement. Do you wish merely to deter and thwart the thief, activist or terrorist, or do you wish to be able to include measures to slow the perpetrators down upon their escape, and provide evidence for criminal proceedings into the bargain? Effective security planning rests on the agreement of a company-wide security strategy that's acceptable to all.

Considering physical security

When considering physical security measures for the building you're mainly looking at perimeter protection methods. It's not always possible to erect fences and deploy gates, barriers, bollards and ramps around your building – you may be hampered by other constructions in the vicinity, local council regulations or the building design itself.

The security manager should always seek to provide as much perimeter protection as is reasonably possible and acceptable. Let's face it, this is your first line of defence.

External lighting is also important for both safety and security reasons. Sensor-activated lighting works well for detecting movement, and will give the impression that the person walking past has been noted. The light often acts as a trigger to analyse an area for movement should you seek to be continually monitoring your office or factory areas. You may choose lighting that simply illuminates the site. This will increase visibility in and around the building(s), and might not only make access in the dark safer for employees but also serve to deter criminals into the bargain.

A good general rule is to adhere to relevant Codes of Practice and regulations whenever you're looking to install perimeter defences such as fences or security lighting. You may find yourself in hot water if your lighting is above the recommended brightness levels, or fittings are badly positioned such they interfere with passing traffic at night, etc.

Indeed many companies have been taken to task for not signposting electric or barbed fencing, and, in certain cases have even been sued by the would-be thief! Be warned.

When attempting to limit access and admittance, do recognise the need for emergency access, or access for those groups with special needs (i.e. wheelchair users and the vertically-challenged).

Security for external elevations

Nearly all security professionals are only-too-aware of the easy access gained through open windows. With most buildings having air conditioning in this day and age, the likelihood of them being left open has been reduced.

A variety of locks, alarms, glass, sensors, screens and grilles can be fitted to make windows more secure, but the use of each will depend on the potential risks faced – and on the local environment. Most companies are also aware of the need for restricting access to their premises, but often the type of access chosen is not suitable for the make-up of the company. Where card-based systems are the order of the day, tailgating or borrowing of passes are likely forms of abuse. Where turnstiles are in place, it's sometimes forgotten that large numbers of people need to get in and out of the building at certain times which can cause problems of congestion.

Where number codes are deployed, they may be easily passed on or overlooked by outsiders. If not changed, they might even be worked out by thieves looking at the wear and tear on the keypad.

Electronic security in context

Integrated electronic security systems can provide the best all-round, all-inclusive security arrangements. You can include a variety of measures to tackle a variety of issues. Internal access control systems, CCTV systems, monitoring and recording devices, lighting systems, public address and alarm systems and even external barriers and/or gates may be added to the security mix.

It is often the case that the access to a building is 'tight', but that movement in and around the building is not. Petty theft, fraud and sabotage of systems are commonplace in most organisations and need to be prevented by internal security systems and access control.

Ian Johnson Associates Limited - Linden Place - Seale - Farnham - Surrey - GU10 1HS.
T: (+44) (0)1252 782664 **F:** (+44) (0)1252 782818. **E:** info@ija.co.uk **W:** www.ija.co.uk

Some companies combine these with employee identification and management via the use of swipe cards and proximity readers.

Flow of staff, working hours, absenteeism, and overtime can all be monitored through systems that will also be able to limit access to certain departments or areas, as well as provide visible identification to staff.

It is often the case that access to a building is tight, but that movement in the interior is not. Petty theft, fraud and the sabotage of systems are commonplace in most organisations. Such occurrences must be prevented at all times by internal security and access control systems.

CCTV and the sabotage syndrome

There are many common mistakes made when choosing a particular type and positioning of a CCTV system (i.e. the positioning, range, clarity and monitoring of pictures, and the lighting needed to ensure effective images).

Security managers also need to bear in mind how easy such systems would be to sabotage, how difficult they might be to get at for repair and maintenance purposes and whether or not they conform to current rules and regulations. Remember to check all maintenance agreements and product guarantees.

Whichever CCTV system you choose will inevitably depend upon what you want from it. The picture quality will need to be excellent if the intention is to use a given set of images in court, thus each camera installed will have to be assigned an 'operational objective'.

You will also have to decide how you intend to manage the CCTV cameras themselves (i.e. whether you are going to feed the pictures through to a central monitoring station for review/action, or whether you merely wish to record the footage for reference should a situation occur). This decision will dictate the types of cameras, recorders and monitors needed, as well as the number of security staff required to administer them.

The management of alarms will also need to be addressed. Intruder alarm systems with movement sensors, static alarms, infrared and microwave sensors and panic attack alarms are all widely available, of course, and may be monitored by either internal or external organisations as dictated by your security plan.

Sometimes, the most practical way of doing things simply involves locking items away or anchoring them to the furniture to avoid them being removed

Asset logging and monitoring

What about asset logging and monitoring? There are a number of software solutions that link to access systems with the purpose of logging and tracking important or expensive items contained within a building. In some instances the security manager may even wish to fit alarms to equipment that is not supposed to be moved or tampered with.

Lighting is often viewed purely from a facilities management point of view (i.e. is it bright enough/too bright for employees to work under safely, and just how costly is it to the company?)

While such matters must be taken into consideration, so must effective lighting for the CCTV systems, and whether the lighting design might make your building more of a target. For example, no lights on at night shows that there is no-one present in the building, and therefore offers thieves a 'window of opportunity' following a break-in before anyone will be able to react. Similarly, some offices where the lights are left on at night are re providing a 'shop window' that illuminates assets like PCs, printers, scanners, laptops and other items.

If you have mirror film on your exterior windows to prevent people from seeing into the offices, check that this also works at night with all the lights switched on (it usually reverses – others can see in and you cannot see out).

We have already touched upon the subject of restricting access to your servers, and this should include the allocation of access levels on all computers to user groups and password-protected files.

Think carefully about how you propose to file or destroy copies of letters, e-mails, faxes and documents on your systems and in the office.

Many companies now recognise the importance of destroying confidential paper documentation, and therefore include the shredding of sensitive information in their security policies. There are plenty of agencies operating a secure collection service that supply lockable bins, and will remove and destroy the shredded materials.

Note that the physical positioning of such items will necessitate much thought (as will the vetting of any disposal agency chosen). Be aware of documents held on machines, and the deletion of records. Items are often stored in a computer's trash folder for many hours or even days after they've been 'erased'.

In all cases, advice may be needed to ensure that Government and system guidelines are observed. There are plenty of industry, Governmental and independent advisers out there to help you should you need it.

At the end of the day, such advice and knowledge is the central key to planning and designing- in your security – and, just as important, designing-out crime.

John Julian CPP is a Senior Consultant at specialist risk and security management consultancy Ian Johnson Associates (IJA).

If you would like further advice on this subject or would like to speak to an advisor, call our consultants on +44 (0) 1252 782664 or alternatively email: info@ija.co.uk

An abridged version of this article appeared in Security Management Today Magazine.