Physical Security: Finding the Right Solution…

…Important lessons in security are often missed by the boards of UK companies. Whether or not your own organisation has ever suffered the major effects of a security incident, there should be no excuses for not being prepared for the impact such events may have on your business.

Regrettably the simple fact is that corporate response to security is invariably a knee-jerk reaction after the event. It is for this reason, that attention to security issues is often labelled as a 'disaster or panic sale' – because it is reactive rather than proactive. It seems that there has to be a disaster first before security is taken seriously.

What company boards need to recognise, is that security can be a profit enhancer and motivator built on the ability to protect the company business as well as create a safe and secure environment for employees. This is best achieved by creating a security strategy that analyses all potential risks and identifies appropriate security measures embracing every aspect of the company's business.

Security can be a profit enhancer and motivator built on the ability to protect the company business as well as create a safe and secure environment.

Risk Assessments

The starting point for securing any business has to be the risk assessment. In an ideal world, any security you decide to put into place must cover all the risks posed to your organisation by the location, building and the business you are in. In reality, your budget may not stretch that far, and so a good risk assessment is required in the early stages of planning to help management decide what risks are a priority.

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. A whole series of issues needs to be considered.

Location

Where is your business located? Are you in a high crime area? Are you operating in areas or countries hostile to your type of operation? Are you in close proximity to potential terrorist and activist targets or figures?

Who are your neighbours? Do their products, assets or activities attract unwanted attention? What type of boundaries and defences does your building have?

How secure is your site from neighbouring activities or issues? Is access to your building more easily gained through a neighbour's premises?

Are you located where fast access and escape is available, due to the road layouts? Are you located in an area where escape is aided by natural or man-made cover?

Nature of the business

What products or raw materials does the business create or handle? Does the nature of these products pose any threats in themselves? The management 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 their nature like this also helps to understand how much effort will be expended by thieves, activists or terrorists and to what lengths they will go to achieve their goal. Similar questions should also be asked with respect to the assets and the business.

Business activities

Will the nature of your products or the research and testing of them, attract extremists? Do you have any links with companies that do? Does the public perception of your type of business, or even your name, provide an association with controversial activities?

Image

Do you have high profile personalities promoting or linked to your business? Will they attract adverse attention, due to their image, lifestyle, relationships or beliefs? Have you got the safeguards in place to protect your business and people against any such risks?

Staff

When you think about employment, do your business activities attract individuals with questionable character and intentions? Do you work in an environment where clients and employees, unique products or ideas might be attractive to your competitors? What controls do you have in place with regards to the employment, access and treatment of personnel?

Building Architecture

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

Ian Johnson Associates Limited (IJA) - Linden Place - Seale - Farnham - Surrey - GU10 1HS.
Tel: (+44) (0)1252 782664 **Fax:** (+44) (0)1252 782818. **Email:** info@ija.co.uk **Web:** www.ija.co.uk

Continued from Page 1

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

What are the interior and exterior doors made of? How safe and secure are they? What sort of access control do they have? Will your offices be open plan, or will you have restricted access to certain areas?

What sort of protection do you have for your staff, especially your 'front of hour' people? What sort of protection is there for staff around the building e.g. car parks, entrances and exits? Is there adequate lighting surrounding the building?

What is the overall structure of the building like? Are the main walls (and if adjoining other properties, the interior walls) solid and able to withstand attack?

When considering threats, you need to think broadly and pass beyond what is normally seen as the realm of 'security'. All too often, the responsible manager will consider external criminal, terrorist or activist, and vendor/supplier action but will ignore staff theft, internal manipulation, malpractice, fraud and sabotage.

Grading the risk

Having identified the risks, there are several options open to you. These range from:

- Mitigate the risk; take measures to limit exposure or the effects of impact.
- Transfer/share the risk either through insurance or by delegating to another company (e.g. cash in transit).
- Spreading the risk, by dispersing assets over a range of sites, raise reserves or have back-up systems to limit the impact.
- Accept the risk.

Designing Security

The key to designing in security is 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 to tackle these. As a busy manager, it is very difficult to be up to speed with the latest developments in security technology. Even with good security knowledge, you may find certain things (for example, determining how to achieve the optimum picture quality from your CCTV cameras) outside your area of skills.

The security market is continually expanding and there are now a number of organisations, such as the British Security Industry Association (BSIA) that can offer advice and recommend specialists to help you deal with different security problems. Experienced independent security consultancies will be able to offer advice on the risks your company faces and the best security systems or suppliers to use. However, be careful that recommendations are based on proven knowledge and expertise and not simply because of a link (financial or otherwise) to particular companies.

It pays to get outside help. If they are good at what they do, they will be aware of the latest technology, crime trends and industry specific risks. They should also be able to advise on the best solutions and most cost-effective systems and services.

Most police forces employ an architectural liaison officer, who can also help advise you on security design and may provide knowledge on the types of threats and incidences that occur in your area.

The benefit of using outside help is that if they are good at what they do, they will be aware of the latest technology, crime trends and industry specific risks. They should also be able to advise on the best solutions and most suitable systems and services.

Consider what you want to achieve and set this out in a company security strategy.

When initially looking into the design, you should also look into the objectives of all the security arrangements you propose to implement. Do you wish to just deter the thief, activist to terrorist, or do you wish to be able to include measures to slow the perpetrator down on his escape and provide evidence for criminal proceedings as well? For effective security planning, you need to consider what you want to achieve and set this out in the scope for the security strategy.

THE ELEMENTS OF PHYSICAL SECURITY

PERIMETER PROTECTION

Fences, gates and barriers

It is often not possible to have fences, gates, barriers, bollards and ramps around your building as, you may be restricted by other buildings, council regulations or even your own building design. However, you should seek to provide as much perimeter protection as is possible and acceptable. This is your first line of defence in most cases, so you ought to think of ways to deter the thief as well as prevent him being successful.

Lighting

External lighting is important for safety as well as security reasons, and there are a variety of types on the market. 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 be continually monitoring your security.

Page 2

Continued from Page 2

You may choose lighting that simply illuminates the site, which will increase visibility in and around the buildings and might not only make access in the dark safer for employees but also deter any criminals.

Landscaping

Always take into account any exterior landscaping. Vegetation may act as a screen to stop your business activities being overlooked, but it can often help to conceal would-be muggers or thieves. Make sure it doesn't interfere with any preventative and detective measures.

Codes

Try to adhere to codes of practice and regulations when installing perimeter defences such as fences or security lighting. You may find yourself in hot water if your lighting is above the recommended brightness or badly positioned, affecting passing traffic. Many companies have been taken to task for not sign-posting electric or barbed fencing, and in a few cases have even been sued by the would-be thief, so be aware of guidelines.

When limiting access and admittance, do recognise the need for emergency access, or access for groups with special needs, for example wheelchairs.

EXTERNAL ELEVATIONS

Windows and walls

Nearly all companies are aware of the easy access gained through open windows, and with the introduction of air-conditioning units, the likelihood of windows being left open has been greatly reduced.
A variety of locks, alarms, sensors, specialised glass, screens and grills can be fitted to make windows more secure but the use of each will be dependent on the potential risks faced and on the local environment. Also be aware that the thickness of the walls and windows may have an effect on your overall security. Forced entry or eavesdropping is invariably easier through thinner structures.

Doors

Most companies are aware of the need to restrict access into their premises, but often the type of access chosen is not suitable for the make up of the company. Where card systems are in place for entering a building, tailgating or borrowing of passes are likely forms of abuse.

Where turnstiles are put in place, it is often forgotten that large numbers of people need to get in and out of the building at certain times causing congestion problems. Where number codes are used they can be easily passed on, or overlooked by outsiders. If not changed, they may even be worked out by thieves looking at the wear and tear of the keypad.

Keys and locks

Again, there are many different types of locks and keys on the market designed for a variety of situations. It is important to make sure that when fitting superior quality locks to the doors and windows that they are not undermined by poor quality door and window frames. Hinge bolts or locks should be fitted where needed.

ELECTRONIC SECURITY

Integrated systems

Integrated 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, public address systems, alarms and even the external barriers and gates can be included in the package.

Management also neeed to bear in mind how easy systems would be sabotaged; how difficult it is to remove parts for repair; and whether they conform to British Standard guidelines.

Access/door entry systems

Often, access into a building is tight but movement in and around the building is not. Petty theft, fraud and sabotage of systems are common in many organisations and need to be prevented by internal security systems and access controls. 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 security staff.

Continued from Page 3

CCTV

Over the past few years, there has been a great trend towards installing expensive and sophisticated CCTV systems. However, this is often as more of a deterrent than anything else. Of the thousands of videotapes supplied to the police for evidence, an embarrassingly small percentage are useable in court. Common mistakes concerning the designing of CCTV systems are related to the positioning, range and clarity of cameras, as well as lighting, maintenance and monitoring.

Always ensure that you have a spare hard drive from which to back CCTV footage data on to. In the event of a major incident, Police may request access to the main server or even in extreme cases, remove the hard drive from site for further investigation.

Management also need to bear in mind how easy systems would be to sabotage, how difficult to remover parts for repair, and whether they conform to guidelines. Remember to check all maintenance agreements or guarantees.

You will also have to decide how you intend to manage the CCTV cameras, specifically, whether you feed the pictures through to a central monitoring station for review and action, or whether you merely wish to record the footage for reference should a situation occur. This will indicate the types of cameras, recorders, monitors and staffing you require.

Alarms

Management of alarms will also need to be addressed in the context of what you wish to achieve with your alarm systems. Intruder alarms systems with movement sensors, static alarms, infra-red and microwave sensors, panic attack alarms are all widely available and can be monitored by internal and external organisations, as dictated by your security plan.

Asset logging and monitoring

There a number of software solutions that link to access systems to log and track important or expensive items within a building. In some instances, you may even wish to fit alarms to equipment that is not supposed to be moved or tampered with. Sometimes the most practical solution is just to lock items away or anchor them to the furniture to avoid them being removed.

Lighting

Lighting is often seen purely from a facilities management point of view: is it bright enough/too bright for employees to work in safely? Is it costly to the company?

Asset tracking systems can be an effective way of monitoring the wherabouts of key assets. Don't be afraid however to reinforce common sense procedures. Sometimes the most practical solutions are to just lock items away when not in use.

Whilst these matters need to be taken into consideration, so does effective lighting for the CCTV systems and whether the lighting actually makes you more of a target. For example, no lights on at night shows that there is no one in the building and therefore gives thieves a window of opportunity after a break-in before anyone will react.

Similarly, some offices that leave lights on are providing a 'shop window' that illuminates assets like PCs, printers, scanners and laptops. If you have a mirror film on your exterior windows to prevent people seeing into your offices, check that this works at night with the lights on – it usually reverses, so that others can see in and you cannot see out.

Knowledge is the key to planning and designing security, as well as designing out crime.

An Ounce of Prevention

For each element of physical security, advice may be needed to ensure that relevant guidelines are observed. There are plenty of industry, governmental and independent advisors out there to help you should you need it. Remember that knowledge is the key to planning and designing in security, as well as designing out crime.

If you would like further advice on this subject or would like to speak to an advisor, call our consultants on 01252 782664 or alternatively email info@ija.co.uk

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

Ian Johnson Associates Limited (IJA) - Linden Place - Seale - Farnham - Surrey - GU10 1HS.
Tel: (+44) (0)1252 782664 **Fax:** (+44) (0)1252 782818. **Email:** info@ija.co.uk **Web:** www.ija.co.uk