The architects of security…

…With the threat to company security greater now than ever before, managers will need to seek objective advice on strategic planning – an investment that requires careful research. In this article, Alex Chambers examines ways in which security professionals might create a working environment that minimises risk and maximises corporate well-being.

Important security lessons arising from disasters are often missed by the Boards of UK companies. Whether or not your own organisation has been involved there is a very strong case for reflecting on what impact such dramatic incidents as bomb blasts might have on your company business - and whether more thought and energy could be given at senior level to creating an environment that minimises risk and maximises corporate well being.

The simple fact is that whether the incident is a terrorist bomb, fraud, intrusion or industrial espionage, corporate response to security is invariably a knee-jerk reaction. It is for this reason that attention to security issues is often labelled as a 'disaster sale'. Why? - Because it is reactive when it should be proactive.

For too long now businesses have paid scant attention to anticipating security problems before they occur. For the most part, confusion wedded to ignorance pervades the world of corporate security. Clearly, there is a need for greater understanding about the subject itself, and the risks involved. The objective is clear: it is the creation of a safe, secure, efficient corporate environment that contributes to any company's success and corporate image.

For this reason everything – including the company building(s), the security systems installed and the staff employed must be carefully planned beforehand.

The 1992 amendments to the Health and Safety at Work Act 1974 requires employers to safeguard their staff against everything from a cut finger, to canteen fist-fights, and protection from terrorism. Equally corporate governance codes of practice such as Turnbull, requires that companies formally address operational as well as financial risk. The first message the Board should understand is that security is now an integral part of corporate planning and vital to staff welfare, morale and ultimately profits. The second message is that is covers a complex range of issues, which need careful consideration.

RISK ASSESSMENT

The starting point for securing your business has to be the risk assessment. How can you address all subsequent security issues without this valuable document? The effectiveness of strategic security planning, policy provision and introduction of workable, targeted security systems are all diminished if they are not responding to identifiable threats and the risks. Why then do some businesses, particularly those with no dedicated security manager, ignore the risk-based approach to security? We are used to doing Health & Safety risk assessments, so why not security risk assessments?

Without the latter, the result is likely to be an ineffective security system, inefficient targeting of resources, additional and unnecessary cost, plus exposure to intangibles such as corporate reputation and litigation.

BUILDING SECURITY

Over the past few years, companies have taken protection of assets like equipment, staff and information more seriously. Most companies have now installed CCTV on their premises; however, this is often in a hope of preventing security incidents arising. When they do occur, they find that they do not have the procedures, policy and equipment in place to respond effectively, which proper planning would have provided.

An example of ill-considered security is the current tendency to purchase expensive and sophisticated CCTV systems but without the expert advice on how best to install them. A state-of-the-art mission control bank of monitors may look impressive but how effective is it? Of the thousands of videotapes which are supplied to the police for evidence, only an embarrassingly small percentage are useable in court. After installation, rarely is sufficient attention given to Home Office guidelines for the management of video evidence, maintenance of the hardware or even re-alignment of cameras, should this be necessary. Where expert advice has not been sought, the tapes are invariably unusable due to poor pictures resulting from lighting problems, incorrect positioning of cameras or wrong lens selection. Another tendency is to fill the control room with monitors but only employ one person to keep an eye on all of them. If this is the case, expect crimes to go un-noticed and certainly do not expect to obtain a successful prosecution.

When planning building security, people will always certainly think of CCTV, a good access control system and perimeter protection. Try thinking of security issues that don't just involve the breaking and entering style thief, but other types of crimes. Think insider as well as outsider and your planning will start to take shape. Involve your HR department, health and safety executives, IT managers and facilities managers in the assessing stages so that you can begin to see the weak areas of your current security and what you might need to improve.

MONEY WELL SPENT?

"An example of ill-considered security is the current tendency for managers to purchase expensive and sophisticated CCTV without seeking expert advice on methods of installation. Very rarely is enough attention given to Home Office guidance on managing video evidence."

Where possible get expert advice on security systems and design. Watch out for the legal pitfalls: when restricting or controlling access, monitoring public areas, or installing systems remember to follow the current codes of practice and laws such as the Data Protection Act 1998 for CCTV systems which became effective on 24th October 2001.

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

Continued from page 1

DETERMINING A SECURITY POLICY

The company security policy must be clearly communicated to all staff as every individual has a part to play in its successful implementation. Where necessary staff should be given the necessary training commensurate with their security responsibilities.

Security policies extend in various forms to all members of staff: whether through IT security, post room procedures, or visitor access. A member of staff innocently loading a virus-infected disk on their PC can cause as much damage to a business as a terrorist. Clear policies on behaviour in the work place, as well as procedures covering purchases and sales can aid in the preventing and discovering of internal fraud and violence in the workplace.

There is a need to raise the level of security awareness throughout a company's organisation and this demands the involvement of the Board. Ultimately it is the Board who must set and agree security policy and it is to them that security issues should be routinely reported.

Many companies make one fundamental error. Having installed their physical security systems, firewalls and various detection software, written their security policy and determined reporting procedures, they feel they're adequately covered against most serious threats. If companies do give a second thought to the enemy within, it's usually only based on how much they feel they can trust an employee – very rarely is it based on research.

Very few of the larger blue chip organisations check the background and experience of those they are about to hire. Why not? If you were about to hire a nanny or a home help to come into your home you'd want some authentication, proof of suitable training and references to substantiate the reputation of that given individual. How is it, then that most companies will invite people into their offices, offer access to their company information, supplies and staff solely on the strength of how they performed in a 30 – minute interview or what they may have said about themselves on a Curriculum Vitae? In most cases, your business cannot afford to hire the 'wrong people'.

PROVING THE POINT

In May 2001, it was reported that the troubled Marks & Spencer retail chain hired a security advisor to investigate the leaking of sensitive documents and sales figures on account. A process that was harming staff morale throughout the company, at the same time leading to another sharp fall in profits. The investigation demanded that all staff at the company's head office in London's Baker Street be interviewed to find the rogue employee.

Also in 2001, foods giant Kraft sued over an attempt by a rival to steel trade secrets about a new pizza base recipe. The $1.75 billion market for frozen pizza bases was the matter at issue, Kraft alleging that Schwan's Sales Enterprises had hired a double agent and a freelance corporate intelligence agent to discover the secret of Kraft's rising crust frozen pizzas. According to Kraft, the freelance agent posed as a reporter, a food researcher and then subsequently as a manager in order to solicit the necessary information.

This strategy apparently worked. The company then argued in court that even a "slight advantage" in the marketplace could mean millions of dollars of lost sales.

Third, a report by the Computer Security Institute in San Francisco blames disgruntled employees for $378 million (£259 million) in damage to property or fraudulent claims identified by US firms in 2000/2001.

Security managers should never fall into the trap of thinking about fraud purely in terms of individuals siphoning off millions of pounds out of others' accounts, or selling on trade secrets to their company's competitors.

Think of all those thefts from the supply cupboard, missing laptops secretly taken home and those employees pretending to work when they're actually doing other things. Often we think of moonlighters, but all those handing in worksheets for hours spent surfing the net for private use are committing fraud. All of those hours are effectively stolen company time, and should be seen as a theft of manpower as much as they are bad for morale.

Who wants to work alongside someone who is being paid the same salary but does nothing all day, especially when the security manager turns a blind eye?

Jack Welch – the retired chief executive of General Electric, and the man credited with turning the $12 billion per year turnover outfit into a $530 billion worldwide conglomerate – thinks that a happy and efficient workforce was the key to his success.

Welch recently addressed selected managers at an Institute of Directors seminar, and said "Your employees know more about what's going on in your company than you do. The day you learn to understand that will be the day that you cross the great divide. Employees know who is shirking, and they hate it if management looks the other way."

This policy of vetting all employees should extend to suppliers and, in some cases, the clients as well. Since those you have dealings with are not governed by your own internal company policies, you should be aware that they also not be as reliable or trustworthy as your own members of the security team.

Always remember that good policies provide the checks and balances, which could be an early warning system to much bigger crimes.

CARRYING OUT SECURITY ASSESSMENTS

Vital to any security plans should be regular audits and reviews. After all, how do you know that you have the right security design in place?

When drawing up your objectives of improving security, always factor in assessments. Most companies carry out appraisals for employees, and most will also conduct fire and evacuation test procedures. How many, though, conduct security penetration tests and assessments? It's often only when a security alert occurs that companies realise there are gaps in the security arrangements and procedures, or indeed a lack of any company policy to cover them.

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

Continued from page 2

PENETRATION TESTS – WHAT ARE THE BENEFITS?

Penetration testing is a useful assessment to determine the security measures you currently have in place are effective. A penetration test will;

- **Detect procedural and physical flaws in your security systems before an intruder exploits them.**
- **Measure staff security awareness and highlight complacency.**
- **Demonstrate to staff and security personnel that security is taken seriously, keeping all involved persons alert.**
- **Measure guarding and reception performance; critical in ensuring contracted service is maintained at the right t standard.**

The other common mistake to make involves warning everyone that a test will take place! By example, a scheduled evacuation of One Canada Square (more popularly known, of course as Canary Wharf Tower), many people used the lifts as a means of escape because they knew it wasn't a real danger situation, while others chose to be 'out of the office' for the whole time.

Tests and audits must be carried out in a natural environment. People will usually react differently when they're put under pressure, as indeed will the building equipment.

For those enlightened company directors who realise the importance and seriousness of good security management, well qualified advice can significantly reduce the harm that may be done to a business and its reputation.

Many also view the need for an annual company security audit in much the same way as a financial audit. There is much to be gained by a regular review of security measures. At the very least, the assets and future of the company will then be properly safeguarded.

In light of the tragic events that unfolded stateside on 11 September, no-one should remain naïve about the environment in which we now live. The threat to security is greater than ever before. Protecting your company's assets against the myriad risks out there requires expertise, sound knowledge and experience. Any advice you make use of must be objective and totally independent of internal management pressures, while still taking into account the security needs specific to each individual department within the firm.

The overall solution, however, is not to be found in the Yellow Pages or at your local crime prevention office. Obtaining qualified and professional advice is an investment requiring nothing less than careful research.

A sad comment on today's world though it may be, security is an ever-present issue that affects us all. Get it right and there is no need to panic, even in the face of terrorist activity. With well-established, sensible security measures and contingency plans in place, your company can protect its business and continue to operate with the minimum of disruption.

If you would like further advice on conducting a security assessment of your working environment and 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 Magazine.

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