Routes to Governance…

…Risks of loss or damage are seldom confined to any one location or function within a corporation. It's imperative that incidents, vulnerabilities and suspected areas – or types – of risk are correctly evaluated by security professionals on a centralised basis ant that the information is then made available to staff in all areas where those risks may impact. Alex Chambers reviews correct procedures for corporate governance.

In recent times, corporate governance has assumed an ever-increasing importance across all those UK companies where stakeholders are requiring more information on the implementation of internal controls.

For their part, Boards of Directors need to maintain a sound system of internal controls in order to safeguard both shareholders' investments and the company's own assets.

Each company must be able to demonstrate that an effective system has been put in place to manage and control risks, whether they be strategic, operational, or financial. It stands to reason that a sound system of internal controls requires regular monitoring, and a regular review of the risk issues involved.

For corporate security professionals, this begs the question as to their ability to ensure that the Board fully understands and appreciates the security risks posed to that company's assets.

In many cases, it's likely that they don't appreciate either the variety or magnitude of the risks they face, nor indeed their personal responsibility for ensuring that "all reasonable steps" are taken to minimise any impact and protect their company, its people, shareholders, customers, assets, and – where applicable – third parties (including members of the public). Members of the Board should be aware that, in a Court of Law, ignorance is no defence.

Keep information channels open

A good place to begin this discourse on corporate governance would be to address the issue of keeping your management team fully informed. Accurate and timely information is seen by many practitioners as being essential to the success of any management system, and security is no exception.

There are a number of clear information channels that should be established to allow managers to manage the risk in their areas of responsibility. Those channels are:

- Clear knowledge of individual and managerial security responsibilities
- The reporting of actual, suspected or potential areas of risk;
- Information on assessed and quantified current or potential risk, and on trends or developments in risk;
- Feedback to measure knowledge and understanding levels.

While security is everybody's business (and responsibility), those in management or supervisory posts have a direct and formal responsibility to actively direct and manage security issues. This means a great deal more than merely being allocated a certain number of security-related functions as part of the role, job description or responsibility statement.

Security effort has to be managed, but it also has to be led. Everyone with responsibility for premises, functions and people needs to show all persons with whom they come into contact that they firmly support the need for secure practices and measures.

In turn, this requires that acceptance of responsibility – as part of the management function – includes the need to communicate (onwards) the acceptance of security in the roles of all their people. The manager and supervisor(s) will have to educate all others within their sphere of influence as to what standards are expected and – above all – will indeed have to demonstrate their own commitment by setting those standards.

'Security effort has to be managed, but it also has to be led. Everyone with responsibility for premises, functions and people needs to show all persons with whom they come into contact that they firmly support the need for secure practices.'

The education of subordinates must take place by way of an ongoing process of formal instruction, written inclusion in procedures and working instructions, and day-to-day direct guidance or counselling. It is only by the process of gaining everyone's acceptance of the need for them to play a personal role in maintaining security defensive levels that effective security will be maintained.

Risks of loss, damage or injury are seldom confined to any one location or function within the corporation. It's imperative that incidents, vulnerabilities and suspected areas – or types – of risk are correctly evaluated on a centralised basis, and that the information is then made available to all areas where risks may impact.

The first stage in this process is the gathering and transmission of the raw information, which will then enable full assessment and evaluation to be carried out. To be successful, all information is required – and should be passed into assessment and quantification system.

Using existing and established communication facilities, it's recommended that the majority of the information be channelled initially to 'screening' points' where any need for additional information or clarification can be established. Two 'screening' points are recommended: and Incident Assessment Team and a Security Collation Desk;

The Incident Assessment Team

It is recommended that a small team be established from safety, security and relevant management to receive initial reports of security or security-related incidents. Their role would be to examine these incident reports and determine whether there's enough information for responsible management to accurately judge the impact and risk level (and consequently direct the need for remedial measures), or whether more information or investigation into causes is necessary.

Of course, any investigation needs identified should be co-ordinated with the manager responsible for the business areas affected.

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

When adequate information is established, the matter will be assessed and – if appropriate – quantified before being passed to the relevant manager for consideration/action as needed.
It is probably best that the incident assessment team should consist of no more than three individuals as this will allow them to get together quickly in a given place when the circumstances surrounding any incident warrant immediate attention.

Security Collation Desks

Reports of factual incidents only offer a small portion on the real picture of risk posed to any given area. For any security incident that actually occurs there are almost certainly others which are 'near misses', or there will be a potential for incidents. For example, employees' suspicions may be raised concerning the actions of people who seem to be monitoring activities where there is a potential for loss or damage (e.g. someone who frequently seems to be in the vicinity of cash collection or movement transactions).

Then there are the recurring errors in handling procedures that appear – to users, at any rate – as offering the possibility of manipulation or likely targeting by criminals.

Consider also the weaknesses, vulnerabilities or omissions in security elements of defensive or protective measures (either physical, electronic or procedural) caused by gaps in planning, changes in methods or about-turns in activity.

And what about suspected attempts made to breach security measures, whether they be an individual seen running away from a slightly damaged door or piece of equipment (but with no real damage caused), or whether it be circumstances like normally locked doors or cabinets being found open?

In addition, individuals who refuse to comply with or follow company procedures and security policies may use other excuses to cover up an attempt to circumvent security checks and avoid detection.

Such information needs to be brought together at a centralised point so that it can be analysed. Persons seen loitering or watching near warehouses may be planning a robbery at that – or a similar – location. If they become alerted to having been seen at one point they will not necessarily abort the operation, but may switch to another location.

Similarly, when doors, etc are discovered to have been tampered with over a number of locations then the trend of impending thefts or damage can be revealed. Even if they all occur at the same location, the knowledge may be spread across a number of different individuals working on different shifts, with the significance being missed as a result.

Information is knowledge

Information or vulnerabilities or security weaknesses discovered may be isolated to one location where the necessary degree of emphasis on controls has lapsed. It's very often the case that the original concepts have omitted to note an 'opportunity' that exists within procedures.

A Security Collation Desk is entrusted with gathering information from both internal and external sources. Criminal and/ or anti-social trends developing elsewhere in the region have to be assessed in order that the security team can determine whether or not there is likely to be an impact on the business. Vulnerability to such trends cannot be measured without sound knowledge of current conditions.

In most cases, the impact will first be felt by front line security staff. If the early symptoms are noted, measures can then be adopted to reduce or prevent any possible consequences.

It's true to say that the collation function proper should be an open process of information gathering and analysis designed to alert management - through the manager responsible for security – to changes that may affect the business.

Information systems have to be two-way to be effective. The collation and analysis elements of the corporation need the raw information to complete their assessments and quantification of risks, while management must be kept fully informed of the risks within their area of responsibility. This can be achieved by using a 'security risk register' where those relevant extracts (of quantified risks) are distributed to managers on a regular schedule. Then you will have the base information needed for line managers to manage security within their own areas of responsibility.

'An effective security cycle of assessments, surveys and reviews requires that managers responsible for the area(s) under analysis be fully briefed on the current or historical levels of risk and the apparent future trends.'

This will also assist managers in working with the security staff or contractors to formulate effective security defensive plans that are compatible with business and operational needs. It will also help them decide on what nature and level of risk they can 'accept'.

Measuring system effectiveness

The effectiveness of any security system has to be measured. Managers and supervisors have the responsibility of ensuring that all employees are aware of their duties – and remain 'aware' at all times. Actual levels of security awareness and activity will be measured as part of regular programmed security reviews, but it's recommended that additional measurement also occurs. In truth, this can take a number of forms.

'While compliance with specific security management standards is not yet a regulatory requirement in the UK, companies that don't actively demonstrate compliance with best practice will open themselves up to legal claims and , increasingly, will be regarded by the markets and stakeholders as bad risks. That is the message that all in-house professionals must impart to their own Board of Directors.

Certainly, any manager or executive visiting a location or function within his/her area of responsibility should actively seek the views and opinions of the staff. It's they who'll be most likely to appreciate any shortcomings in security attitudes or actions, and it's they who'll actually be best placed to comment on any overly restrictive practices.

Alex Chambers is a consultant with IJA, the independent security and risk management consultancy.

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