

The integration of Risk, Safety and Security

A Supreme Court judge, in passing judgement on a recently failed Australian business deal worth millions of dollars, said that the deal was “a frantic, unsightly and ungainly late evening that can only be described as a madhouse by all who participated under the most considerable time pressure imaginable”. Of course this could equally be a description of any crisis or emergency, anywhere in the world. Even with the best management track record imaginable, events of this nature can and still do happen. However, as failure is generally not an option in business, what can two former SAS operatives now trapped in the bodies of businessmen advise about reducing risk profiles?

A recent benchmark study of 260 of Australia's top public and private sector companies revealed a mixed response in attitudes toward and practices of risk management. While 87% of companies surveyed saw identification, assessment and management of risks as important, only 50% of companies outside the banking and finance sectors were confident that their risks are being effectively managed. That said, risk management and safety are becoming components of corporate reporting worldwide, with a plethora of government codes on corporate governance, requiring compliance statements by the Board of Directors on internal controls and risk management in annual reports.

Is safety, security and risk management a cost centre in your business or a contributor to profit? At the ESSO plant in Longford

Victoria, safety had clearly become enmeshed with engineering cost centre cutbacks – a move which had dire consequences for the company. The explosion at the Longford ESSO plant is a clear demonstration of what happens when senior management fails to budget for proper risk assessment processes. Systems are not enough. Hazard and operability studies are also not enough, as the reality of any ‘emergency’ is that you need to demonstrate that you can deliver an effective ‘on the ground’ response. Both of these need to be supported by an overarching corporate culture. This leads to the issue of behaviour modification techniques

There is strong research evidence to show that behaviour modification techniques can be effective in promoting critical safety behaviour provided such techniques are implemented effectively. While these techniques are rightly focused on frontline staff, a recent National Safety Council of Australia report notes that senior management commitment to behaviour modification programs is essential. This report boldly states that senior management commitment is the single most important factor in the success or failure of any risk management program.

In an Indonesian head office in Jakarta, they have signs on all floors which say “Don't even think about smoking!” It sends a powerful meta-message to employees in a culture where smoking is rampant in the workplace and non-smokers are very much the minority.

You may well be doing this sort of neuro-linguistic persuasion already. It is our

experience that many oil companies are adopting the aphorism “You become what you are labelled”. Woodside Energy, for example, has a “talent manager”, which tells us that Woodside believes that managers become what they are labelled. Therefore, the trick is to find the appropriate title that you wish the manager to adopt.

However, it would seem that as social responsibilities increase and the nature of protective challenges evolve, the current demarcations in corporate responsibilities tend to blur. Operations, finance, information technology, human resources, property, purchasing and security departments all have a stake in creating and maintaining the best possible risk reduction and mitigation plans. Many companies have already turned their Health, Safety and Emergency (HSE) managers into HSE and Quality (HSEQ) managers.

Other companies have turned theirs into HSE and Security (HSES) managers. One company in Singapore even has a CRASHES (C.R.A.S.H.E.S) manager responsible for Community Relations, Auditing, Security, and Health, Emergency Response and Safety responsibilities!

Whatever title is used, there has to be a very robust partnership of leadership and co-ordination across all disciplines. Protecting individual turf does not contribute to effective risk management planning in the brave new corporate world.

Next, we need to lay out some risk integration concepts:

• Coping with the Terrorist Threat

Despite the intense media hype that currently surrounds this area, we can give some insight into how a terrorist thinks and acts. There is always an element of unpredictability in dealing with terrorists. In general terms, it is safe to act on the basis that terrorists are beyond conventional thought whether fighting for their liberation, their God or their anti-establishment beliefs. Unlike the normal risk assessment process that focuses on likelihood and consequence, with any tenable

To achieve the best results you need to humanise security as you would with safety. In the absence of strategic information, every employee must watch out for and actively report suspicious activity. It is necessary to ensure that there is a system of collecting security-related information as intelligence. This is the only chance to obtain an early warning against terrorist attack. The reality is that government agencies are seldom able to deliver early information of any specific value for the protection of business facilities.

...it is safe to act on the basis that terrorists are beyond conventional thought whether fighting for their liberation, their God or their anti-establishment beliefs.

terrorist threat it is necessary to examine one's business a little differently.

Here one needs to think in terms of intent and capability. This can be difficult to do when the threat source is unpredictable at best. However, assets can be viewed as through the eyes of a terrorist who is selecting a target. This also means the impact of any terrorist action will cross the traditional security boundaries as the terrorist will aim to inflict the most damage possible with the least effort. The limitations of what most people would consider to be 'normal' do not apply as (in their eyes at least) they are at war and you are the enemy.

• The CARVER Acronym

Many terrorists are trained to use the CARVER acronym. You may also find it useful in assessing threats to assets within your own responsibility. This is how it is applied:

Criticality. What asset is the most critical?

A terrorist organization could attack the supplier of an organization's spare parts warehouse or the local fire station in addition to the critical machinery in an organization's production area. How would one handle no water being available for fire fighting because explosives destroyed the street main?

Accessibility. Could a stranger find his way around key sites and be able to identify the critical equipment and buildings? Ignore security suppliers who claim that their latest access control system will stop an offender. Many access control systems can be defeated by a determined terrorist. For example:

- How do you stop a determined terrorist who will steal a valid access card?
- How can you protect against the committed terrorist who will deliberately kill the on site security officer in the entry to walk through the site with the security 'master access card' that opens virtually everything?

Recognition. This includes the ability to actually identify the local milk factory as opposed to a critical chemical processing plant. Even the Americans can make a mistake here despite spending millions on satellites and other space age technology. How obvious is it to a stranger what process or products are produced in any plant? Can you adopt a low profile with critical plants and buildings? Is it easy to identify the CEO and other key senior managers because they always park in the same space? How easy is it for someone in a suit to walk into an executive suite? (After all, everyone knows that terrorists are male of Middle Eastern descent and wear white headdress things, don't they?)

Changes in this area can be made at low cost and little inconvenience.

Vulnerability. This refers to the ease with which things can be put out of action. Terrorist groups using substantial force in unexpected areas often obtain the best results. The World Trade Centre in New York, for example, had a very sophisticated access control system and plenty of security staff available to control entry – there was nothing that could have prevented the terrorists from flying an aircraft into the side of it. In the Bali bombing incident, it already appears clear from the court evidence reported in Australia that the alleged offenders had no comprehension of just how much damage would be done to the light building structures by the volume of explosive that they used. Their only concern was that they used ‘plenty’. They did so to devastating effect on all tourists unfortunate enough to be in the wrong place at the wrong time, and the equally innocent Balinese staff.

Effect. How would the local population perceive the “rightness” of the action?

Sometimes the destruction caused by the attack can be counter-productive to the purpose of the terrorist as it damages the terrorist’s psychological objective of winning hearts and minds for ‘the cause’. Thus, it is important to win widespread support from the community. Perhaps this can be achieved through an annual sponsorship program of some description. There may be needs in the community that could be met with a view to improving a company’s business profile.

Recoverability. This refers to the ability, effort, key people, time and money required to bring the asset back on line. Look for anything that is a ‘one off or an import’, that you cannot quickly bypass or contract out – that is a critical component.

In the next issue, we will look at how the security and safety professionals can work together to lower the risk levels a company faces. ■

Jim Truscott has been a crisis practitioner for over 20 years. As a former member of the Australian SAS Regiment, Jim was intimately involved in sorting out problems in Papua New Guinea, Cambodia, Iraq, Indonesia, East Timor, Homebush Bay, the Solomon Islands, Bougainville and the Southern Ocean. Jim now consults as a trouble shooter for a variety of industries including nursing homes, gas platforms, sub-sea pipelines, kidnappings, gold mining and shipping. Jim can be contacted at Truscott & Associates, Perth. 0421915441 truscott@tower.net.au

Jack Hayes became involved in risk assessment while in the New Zealand SAS Group before moving to the insurance industry where he deals with a wide range of high hazard sites. His experience over the last 25 years includes independent risk management consultancy work in a number of countries and asset protection for the Coles Myer group. He is currently working in Auckland as a risk assessor for insurance underwriters. He can be contacted on 021 771 912. jackhayes@xtra.co.nz