

The integration of Risk, Safety and Security - Part 2

In the last issue of Security Oz Magazine, Risk Management consultants Jack Hayes and Jim Truscott looked at the role of senior managers in reducing an organization's overall risk profile. Part two of this article will examine how best to strike a balance between security, risk management and the continuity of daily operations within an organization.

In our last article, we considered the terrorist threat. However, the reality is that terrorism concerns a relatively small percentage of businesses in the marketplace. For the rest, it is the staff and members of the general public who pose a threat to the viability of a business. One of the greatest difficulties one faces when implementing an effective risk management program is to determine exactly how much security, safety and risk management is 'sufficient'.

When the threat to an organization is indeterminate, it is difficult to determine how much security or safety is enough. One must consider the difference between a good level of security and a bad level of security. In simple terms bad security fails to protect to an agreed standard, while good security meets the set standard and provides the senior management team with peace of mind.

When designing a security plan, security professionals must ensure that their 'priorities' align with the priorities of the senior management team. When dealing with an agreed perception of risk, budgeting is simpler.

In order to ascertain exactly what the priorities of the management team may be, a security manager must liaise with the CEO and/or the senior managers and establish what they deem to be acceptable, and more importantly, unacceptable losses.

There is an interesting trend in major hazard facilities towards the use of virtual IT software for process control in emergency situations in place of properly trained crisis and emergency management team.

It has been the authors experience that when a risk management review is conducted at board and senior executive level (with line managers responsible for risk, safety, OH&S and security), middle management are almost always astonished at what the CEO and his/her team are concerned about. Often, middle management, believing that senior managers are more focused on financial outcomes are surprised to hear such comments as:

- "If the chemical plant in Smithville is destroyed – we don't care. We will stop that unprofitable part of our business and focus on the more profitable area over here. The focus is to be on keeping the plant

environment safe so none of our staff are hurt."

- "We will not accept any loss of life by staff at work – any risk or event that could deliver this result is to be immediately reported directly to the CEO and all necessary precautions are to be taken to prevent this outcome."
- "We will accept a 'shrinkage loss' of 8% as our margins can still keep us competitive at that rate of loss."
- "We will not accept any fraud loss of greater than \$10,000 without a full investigation and vigorous legal recovery action. For losses under \$5,000 a local in-house investigation will be enough."
- "We will not accept any OH&S risk that puts the business at threat of any legal action by the authorities. Any threat of a Prohibition Notice is to be immediately reported to the CEO."
- "Line managers have the authority to handle and process emergencies within their local emergency plans. They are to personally report the emergency status to the CEO as it happens. The CEO will activate the corporate crisis team only when and if it is warranted."
- And finally, "I am prepared to accept any loss of property provided I still meet the board requirement for a xyz% EBIT return this financial year"

Cost or Profit Centre?

When allocating budget spending to meet the above needs, it is important to determine

whether security will be a cost centre or a contributor to profit when striving towards zero security and safety incidents. In an organization where safety is treated as an investment one must also work towards making security an investment. To this end, one should ask the following questions:

- What can your current security staff or contractors do that will add value to their activities?

When designing a security plan, security professionals must ensure that their 'priorities' align with the priorities of the senior management team.

- Can the night security officer complete some operational safety checks in the middle of the night rather than having another staff member sitting there all night?
- Do you need to have a receptionist in all sites or is this a function that security staff could perform?
- Can your security officer at the warehouse gate be the receptionist to handle all visitors?
- Can the new access control system be integrated into the CCTV system so that the gate does not have to be manned at all?
- Are there opportunities for your security or safety team to provide services for other contractors working with you or on adjacent sites – and to bill them at a

competitive rate? (This can really change a financial controller's attitude to what is perceived as a security 'cost'.)

Understanding the need for Emergency and Crisis Management Teams.

In today's economically savvy environment, everyone is looking for corners to cut; ways to minimise spending and reduce overheads

There is an interesting trend in major hazard facilities towards the use of virtual IT software for process control in emergency situations in place of properly trained crisis and emergency management teams. However, effective risk management involves the development of a well trained, professional crisis response team. In an emergency situation, it is hard to replace the experience and knowledge of trained professionals. Furthermore, in the absence of such professionals, there is a tendency for staff to automatically respond in a predefined manner because a set process tells them to. It is important to overcome the propensity to not think and just act.

Internationally, there is a growing trend

towards the use of local emergency management teams for the handling of site emergencies such as fires. The incident is then reported to the head office by a senior line manager from the affected site. A corporate crisis management team is only called to the effected site if the incident will produce:

- Substantial asset loss that could damage the long-term viability of the business (Property).
- Adverse publicity or media attention that could damage the business reputation (Reputation).
- Legal action that could prove to be seriously damaging to the reputation, viability or legal compliance status of the business (Legal)

This sort of approach might be okay for small, easily controlled incidents. However, any sort of serious emergency needs to be put under the control of a corporate crisis management team. Such a team may consist of existing members of staff with the necessary relevant experience. Once again, this helps to minimise the cost of employing dedicated specialists or costly contractors. Once appointed, in the event of an emergency, the team will be called together by the CEO or his/her designate and will come together for as long as is needed to determine the strategic direction to be taken. This does not have

to be a 'face to face' meeting as an experienced and well-trained team can easily do this work using conference telephone call facilities.

As soon as the agreed strategy is in place, the corporate crisis management

of skills and experience that can only come from a team. Furthermore, the best solutions often come from the most unexpected players!

Total integration of a wide range of players who will all have an impact on

all of the roles accountable for the components of your business risk and you will be in far better shape when (not if), the unexpected happens. ■

Jim Truscott has been a crisis practitioner for over 20 years. A former member of the Australian SAS Regiment Jim around the world consulting on crisis situations on gas platforms, sub-sea pipelines, kidnappings and threats to gold mining operations. Jim can be contacted at Jim Truscott & Associates on 0421 915 441 or by email at truscott@tower.net.au

Jack Hayes, a former member of the New Zealand SAS Group, became involved in risk management while in the military before moving to insurance industry where he was responsible for a wide range of high hazard sites. Jack's experience includes independent risk management consultancy work in a number of countries and asset protection in Coles Myer Group. Jack can be contacted at Jack Hayes & Associates Ltd, Auckland. 021 771 912 or via email at jackhayes@xtra.co.nz

Build some redundancy into all of the roles accountable for the components of your business risk and you will be in far better shape when (not if), the unexpected happens.

team can stand down turning control of the business back over to the normal vertical line-management. If the situation deteriorates again, for example, there is an adverse TV report on the incident that night on the news, then the crisis management team can be re-convened to plan another strategic response. In an emergency situation, a corporate crisis management team can save an organization from significant financial and physical loss through the deployment of a wide range

of the risk your business faces is an impossible pipe dream- no single person can handle it all alone. However, you can integrate a lot of the functions and processes involved in mitigating risk so the demarcation lines become softer. This approach delivers excellent results with more understanding of each other's roles and priorities in an organization and a team oriented decision-making process.

Remember the golden rule - "no-one is indispensable". Build some redundancy into