

## SECURITY MANAGEMENT – WILL YOU SEE IT THROUGH TO THE END?

Phil Wood MBE  
December 2009

JCSSM  
Vol.1, No.2

Page 81

Organisational assets, which support business objectives, require protection. This, I argue, calls for security management procedures based on linking together crisis management, risk assessment management, and business continuity plan in an overarching Risk Management Plan. Risk assessment management is driven by what the business objectives are, prioritisation of potential threats, and the probability and impact of their occurrence. Once risk assessment has been made, a way forward can be found on how to deal with potential risk. Risk treatment process requires research, thought, and detailed planning and, if carried out properly, will allow security management to be incorporated into corporate planning, and influence the corporate direction.

Other articles,  
research  
notes, and  
commentaries

The potential loss to an organisation from a threat occurring can be incalculable. For example; the incidence of fire may cause a loss of network IT capability and inability to communicate; this is a direct loss. However, there will also be other consequential losses. These might include: loss of business, investigation costs, salaries for staff who cannot work, loss of customers and customer confidence, increase in insurance premiums, cost of replacement equipment, loss of data, reprogramming costs, reinstatement costs, loss of reputation, loss of market share. The list is long and mostly avoidable if risk management process had been carried out to protect the organisation's IT facilities.

Staying with the theme of fire; it is a requirement that fire prevention measures are in place in the workplace. Most fire risk assessment measures are designed to ensure that all boxes are ticked as far as possible; that does not, however, prevent fire from starting and businesses burning down. Normally, during fire, crisis management procedures in the form of evacuation and other measures are activated. However, in most cases, little thought is given to the organisation's ability to continue doing business – i.e. business continuity. In this article, I draw attention to the importance of thinking of crisis management, risk assessment management, and business continuity management as interlinked, complementary and synergistic; their successful combination in an overall Risk Management Plan is, in my view, essential for the organisation's survival and continuing operation. This proactive and cyclical risk management approach, I posit, allows an organisation to be as well prepared as possible for a risk event to occur.

Once a risk event (e.g. fire) has happened, and whilst it continues, a crisis management plan will alleviate the impact of the event.



Journal of Crowd  
Safety and Security  
Management  
*An online journal*

The focus of the plan will be to survive the progressing crisis and to ease its effects. It is essential that the risk management process has clearly identified the risks, that the crisis management plan is changed and amended to reflect changes in the business management process and associated risk factors, and that it is tested regularly to ensure its currency and efficacy. The crisis management plan will include measures such as evacuation procedures, and the establishment and maintenance of information flow as the crisis unfolds. Dealing with the consequences of the risk impacts is what links the crisis management plan to the Risk Management Plan.

Business continuity planning is the third phase of the security management plan. Its focus is to maintain the delivery of services to ensure the organisation's survival. As with the other plans, the business continuity plan encompasses policies, procedures, protocols and information to allow rapid response and to prevent service interruption. The business continuity plan follows a similar path to risk management planning; typically consisting of analysis, implementation and testing, and maintenance and review.

The business continuity plan requires analysis, assessing the impact of an event and providing scenarios allowing an appropriate solution to be chosen. It looks at critical and non-critical functions and provide for the continued provision of the critical ones. The solution may, for example, involve relocation to alternate facilities, provision of additional personnel and the establishment of secondary communications with contacts and other agencies. In the case of IT services, data back up systems may be put in place and equipment replicated at a secondary location if necessary. The ideal business continuity plan allows the organisation to continue to operate as seamlessly as possible in as short a time as possible following a crisis.

The plan should be implemented and tested. Testing may include the practice call-out of personnel, physical and technical transfer to alternative facilities, and testing of the organisation's core business processes under business continuity arrangements.

As with both crisis and risk management, the business continuity plan must be kept under constant review and updating. Linkage to the Risk Management Plan must be maintained to ensure that the hub activities initially identified can continue in the event of disaster or disruption.



The cyclical nature of the Risk Management Plan is reflected in both crisis management and business continuity plans. The effectiveness of all three depends on their flexibility and anticipation of changes in either the organisation itself or the threats to it. All the three plans must be linked with the Risk Management Plan at the centre, informing changes to the other two plans and influencing their development.

This synergistic linkage can be illustrated by the following scenario, focusing on a risk identified within an organization, using the annotations: R (risk), C (crisis) or B (business continuity), as they apply to the appropriate security plan.

*'A corporate insurance company's claims processing department is responsible for a turnover of £50 million each year. Located in the City of London, it has 30 staff and is IT reliant. The company deals with many high profile clients around the world who rely on it solely for the provision of this service. The Corporate Security Manager has anticipated all eventualities and has ensured that the plans have been cleared and put in place. He has consulted widely and assessed the company's business priorities (R, B) and has ensured that the plans to deal with an event (C, B), emergency response (C) and recovery and continued service (B) have been widely disseminated, tested and exercised. The Manager has been made aware that there is a high terrorist threat to financial centres in London and has assessed the risk of a bomb explosion and the impact that it will have upon the business (R,C,B). His planning has accepted that the business will inevitably be disrupted in such an attack (R, B) and having made his assessment has ensured that:*

*The risk can be accepted. A conventional non-hardened building cannot withstand an explosion and the cost of relocation or upgrading the building is prohibitive. The threat can be mitigated by the provision of a cleared zone around the building and by a strict access control system. The threat has been balanced against the company's need to continue to operate in this location and the risk to personal safety. It is essential that this continuity is maintained and that service to the company's customers is not disrupted. (R, C, B).*

*Unfortunately, the worst happens and a large truck bomb is detonated some 100 metres away from the building. There are some minor injuries to personnel and the IT systems are damaged or disrupted. Immediately the Manager puts into operation his well rehearsed plans and a team of 4 designated first aiders begin to treat the casualties after a rapid evacuation of the building to a designated assembly point well away from the point of explosion under the direction of nominated marshals (identified by dayglo vests). His designated Emergency Assistant (the Company Secretary) has contacted the emergency services on a telephone issued to him for that purpose (C).*

*Concurrently the Manager has used his own dedicated mobile telephone to contact a subsidiary company based in Pimlico. He has activated the plan to open a small office within their building which is fitted with IT equipment and has a back-up server to that in the main office.*



*The office is basic but suitable for interim operation. Staff in the subsidiary company have been trained in the procedures for continuing the parent company's business, albeit in a reduced role. Within 30 minutes, a basic, but functioning business is again operating (B).*

*Recovery from the incident takes several weeks and the Security Manager has de-briefed and consulted at all levels to check the efficacy of his plans. He discovers that his Risk Management Plan functioned as required and that the measures that he put in place did mitigate against more extensive damage to the Company's operations (R). The evacuation and first aid treatment of casualties went well, however, the use of mobile telephones proved to be difficult after the explosion and plans (R, C, B) will need to be reviewed to identify a more robust system. Finally, the alternative office arrangements did allow work to continue, however, there was a need to further develop working rosters and cross-pollination of staff between the two companies to ensure a smoother transition (B). The company has allocated funding to upgrade and extend the alternative office to further reduce the impact of similar incidents in the future (R, B)*

The above scenario shows how the Risk Management Planning function is at the core of the company's survivability, and crisis management and business continuity are complementary to it. All three planning processes underpin the company's ability to conduct its business and to provide a physically secure environment for its staff. The cyclical nature of the planning process is illustrated by the actions taken by the Corporate Security Manager after the company has recovered from the effects of the attack; Seeing it through to the end (note the title), looking at all aspects of the business and the threat to it. Success depends on accurate identification and assessment of risk impact, backed up by a maintained Risk Management Plan, along with well thought out and detailed Crisis and Business Continuity plans. There are some similarities between these planning processes, and whilst interdependent, their aims are fundamentally different. Whilst all plans must be formulated and implemented separately, their linkage and review processes must be maintained and monitored in order to ensure that when the anticipated risk becomes a reality business can continue, security can be maintained and improved; and more importantly, human life is protected. This 'belt, 2 pairs of braces' approach involves a hell of a lot of work - but if you keep everything tight you won't be 'caught with your pants down'.



