

Changing Perceptions and the Skills Required by Security Managers

by Michael A Pepper MSc CPP PSP

(First published in *New Zealand Security* – October/November 2006)

Introduction

Mention of security management to the general public is likely to conjure up images of the directors of large security companies such as Chubb or ADT Armourguard. Such a vague perception is perhaps quite valid as members of the public are unlikely to know much about specific aspects of the work of security managers. Often, the perception of security has related to loss prevention through criminal activity or some other event such as fire. Leading European academic Giovanni Manunta has quoted that within commercial enterprises there is a general perception that, *“Security is a non-productive, a highly expensive capital item, extremely costly to install and maintain, always seems to need updating, is forever giving false alarms, and, since we have insurance, who really needs it anyway?”* He has also expressed a rather cynical view of the state of security management in the private sector, *“As professionals, security people tend to be underpaid, under-employed, under-educated and under-trained.”* Such a view is reinforced by others who point to the fact that there is no consistent qualification, title or job specification.

Many commentators have argued that the security function has frequently been regarded as a preserve of former police officers or members of the armed forces. There has been a view that these were the people best equipped because of their ‘experience’, as opposed to any academic or other qualifications, in the protection of assets. Their experience is likely to have been judged to be relevant simply because such individuals were somehow bound to know something about security. After all, is this not something with which the police and military deal every day? Furthermore, the individuals concerned were likely to have held some rank in their previous employment, thereby bestowing ‘management’ or ‘leadership’ experience. Such views do not necessarily imply that security managers have failed to achieve what has been expected of them. Rather, they could mean that businesses have had low expectations of their security managers. The conclusion must be that a rather poor perception of security management has existed and that this can depend upon issues such as context and knowledge. The question arises, “Is such a perception subject to change”?

Other commentators are less pessimistic about security management and see an increase in professionalism occurring. Professionalism can be partly measured by the existence of academic courses and other qualifications. Real progress has been made during the past twenty-five years with the development of degree courses at Foundation, Bachelor and Master levels from a range of universities, particularly in the UK, USA and Australia. Further, the author personally knows of one individual who is pursuing a PhD in the subject. ASIS International has been offering its Certified Protection Professional (CPP) programme since the mid-1970’s, and its Physical Security Professional (PSP) and Professional Certified Investigator (PCI) programmes since 2002. While the police and military influence in the security

industry is still quite strong, the number of those who are choosing security as their first career is growing. There are still plenty of “cowboys” around, however the industry itself is taking steps to eliminate bad practice. The audit system recently introduced by the New Zealand Security Association is a truly positive initiative. There is little doubt that there is an increasing professionalism within the security industry generally and this has come about through security managers learning and applying new skills. So what are these skills and what is their relevance to modern security managers?

Skills

In pursuit of greater professionalism and increased technical competence it has been necessary for security managers to cease being solely concerned with loss prevention. For example, the role of the security manager has broadened to include knowledge of: the law; health and safety; fire prevention; security survey and risk assessment; business continuity planning; and crisis and disaster management. So what is it that makes these skills necessary for the modern security manager? This question is probably best answered by considering the skills themselves.

The security manager is primarily concerned with the protection of the company's assets. These can include premises, plant and money as well as people. Accidents cost money. This not only relates to damage to plant and premises, but also to employees who can suffer injury. Employees who take time off through illness still have to be paid. Others may leave and have to be replaced by others who have to be recruited and trained. A company may well suffer adverse publicity and have to pay, often substantial, compensation to those injured in the course of their work. It is, for example, fairly obvious that security managers should be concerned with loss of property or money due to violent criminal activity such as robbery. However, they should also be concerned about the effect of violence on staff. Violence at work has certainly attracted the attention of trade unions representing workers in the retail and hospitality sectors. There have been warnings that employers could face prosecution for failure to protect staff from violence. Violence in the work-place is only one aspect of health and safety legislation which affects security managers. The legislation now affects so many areas of a company's activities that the consequences of failing to meet its lawful obligations can be very serious. In any event it makes sound economic sense and is good management practice to have a safe working environment. The security manager is not solely concerned with health and safety issues and the risk of harm to employees. There are other risks such as the potential for criminal or terrorist acts against the company. It appears quite obvious that there is a need to know the extent of threat to any asset, however, it could be perceived that existence of a threat, on its own, is sufficient grounds for action and there is no need to bother with any formal assessment. This is a common fallacy.

All of us take risks every day. A simple matter such as crossing a road is informed by judgements such as, how far away is the traffic and how fast is it moving? Similarly, but on a grander scale, the business world takes daily risks. Many of these risks will be concerned with deliberate commercial decisions, an area where, historically, security managers have tended not to be involved. To ensure that the outcome of a commercial decision provides a good return on investment, an analysis of the potential benefits compared to the possibility and consequence of failure is often

used to inform the decision making process. The Australian/New Zealand Risk Management Standard (AS/NZS 4360:2004) states that, *“Risk management involves managing to achieve an appropriate balance between realizing opportunities for gains while minimizing losses. It is an integral part of good management practice and an essential element of good corporate governance.”*

Analytical tools are usually employed in making an assessment of risk. These can be qualitative, quantitative or semi-quantitative. This might imply that risk can actually be measured in some way and therefore eradicated, however, context and culture play as much a part as physical reality. Risk assessment, put simply, is a means of having a degree of certainty about the future. Therefore, as decision makers, security managers have risk assessment available as a tool which allows them to make informed decisions. As with any tool, a degree of skill is required in its use. Apart from the fact that health and safety legislation imposes a requirement to undertake risk assessments, many organisations, including governments, now expect their managers to be familiar with, and apply, the concept of risk assessment to a wide range of disciplines. It is evident that security managers should be no exception. However, it is not sufficient to assess risks and file the findings; some action must be taken to deal with them.

Having identified risks through an assessment process, it is necessary to prioritise them, consider a range of risk treatment options and prepare and implement treatment plans. Some risks may be acceptable due to their low cost even if the frequency is high, whilst others will be unacceptable if the chance of occurrence is low but the result of an actual event represents a catastrophe for the organisation concerned. The actions taken by organisations may depend upon ‘likelihood’ and ‘consequence’. It is argued that whilst something can often be done to reduce the likelihood of an event occurring, for example by protecting some valuable item against theft, organisations should also seek to reduce the impact of an event, through the use of consequence reduction measures. Both these measures are common options in the field of risk management. Guidance manuals, such as the Australian/New Zealand Standard, cover these measures and also list others which are utilised as part of a cyclical process. These include options for treatment of risks with positive outcomes (opportunities) as well as options for treatment of the more usual risks with negative outcomes.

It could be argued that security managers have traditionally tended to focus upon the areas of likelihood and vulnerability. They will have been well used to the application of situational crime prevention measures to reduce the probability of a real event. In the past they may not have been involved with ‘consequence’ reduction measures designed to reduce the impact of an unwanted event. Such measures require planning and there are good examples of how they have been used to good effect in disaster recovery situations. Even though no two accidents or disasters may be the same, much can be learned from the ways in which others have handled them. Following a disaster, it is vital that a company is able to maintain its trading position and contact with its customers and suppliers. Unless there has been detailed contingency planning to deal with issues such as alternative premises, communications and appointment of key personnel, it is quite probable that the company affected will be unable to survive. The UK Home Office has suggested that about 80% of companies which do not have a workable recovery plan will fail within

one year of suffering a major disaster. However, having a contingency or business recovery plan is of little value if no-one knows about it. It is extremely important that staff know the contents of the plan and how to react in an emergency, something which can be achieved through training and the use of simulation exercises. It is argued that because security managers are concerned with the protection of a business, they must therefore be closely involved in, if not responsible for, the development and implementation of plans which deal with 'consequence' reduction measures.

It seems that security managers have little choice but to go beyond the simplistic loss prevention role and develop additional skills. These skills add to the competence of security managers to fulfil their role in the modern world and their relevance must, therefore, be accepted. The question remains. Is it changes in the perception of security management which have impacted upon these skills?

Impact

The traditional perception of security managers was hardly flattering. However, as noted above, changes in this perception have occurred during the past twenty-five years. So what has been the cause? There is evidence that suggests there has been an increasing desire for professionalism amongst security managers and that the main impetus for change appears to be security managers themselves. A range of international security trade magazines regularly feature articles on the need for greater professionalism and the need for greater government regulation of the private security industry. It seems that security managers have become fed up with poor standards and a poor image and are seeking to do something about it. ASIS International and NZSA are keen to rid the marketplace of the "cowboys". The problem is being addressed through the availability of formal qualifications, membership of professional associations such as ASIS International and enforceable audits by trade associations such as the New Zealand Security Association.

Academic input as well as good management practice has helped security managers to identify new skills. These skills can only enhance their capabilities and, therefore, their standing within their organisations. Degree and diploma courses in security add considerably to both skills and knowledge, covering areas of study such as: criminology; law; security risk assessment; research methods; and, management. Some employers are also recognising the need for qualified and highly skilled security managers and encourage their staff to take part in higher education programmes such as the ASIS International Certification Programmes, the New Zealand National Diploma in Security and the degree courses offered by UK, US and Australian universities. Regrettably this is not the case with all. Only two years ago the author had a discussion with the General Manager of a large security company on the subject of security education for his company's management team. The response was that the GM wanted his managers to manage; they did not need to know anything about security. Given that these managers were also providing security advice to clients, this was a damning indictment of the company's sense of professionalism.

Conclusion

Some commentators still perceive security management as rather unprofessional and little more than 'rent-a-cop'. Others see security management increasing in professionalism as security managers acquire new skills. Whilst it is recognised that both perceptions are probably valid, the fact that there is a difference of opinion suggests that perceptions are changing, particularly when these are related to the acquisition of skills.

Although a limited set of additional skills was focused upon in this article, it is evident that other management skills are increasingly being utilised by many security practitioners. The evidence shows that greater demands are being placed upon modern security managers, and rightly so. This requires them to develop new skills through the learning process. The fact that standards are continually improving and that more and more security managers in New Zealand are obtaining professional certifications such as the CPP and PSP through ASIS International as well as degree and diploma qualifications, tends to confirm a view that changes in the perception of security management have been the cause of a real and sizeable increase in the skill level required by security managers. Those who ignore the need for education will be simply be left behind.