Terrorism preparedness of building facilities managers

Then and Loosemore present first-line research on risk, crisis and continuity management practices of facilities managers

Abstract

Many of the new security threats we face today, revolve around the apparent exposure and vulnerability of buildings and infrastructure to terrorist attacks. Yet little is known about the level of preparedness to deal with changes in terrorist strategies away from secured "hard" targets towards "soft" unsecured targets in the urban environment such as buildings, infrastructure and public spaces. This paper presents the findings of preliminary research into the risk management, crisis management and business continuity management practices of Facilities Managers responsible for a range of major public and private buildings in Sydney, Australia. The results suggest that Facilities Managers may underestimate the vulnerability of their buildings towards terrorist attack. They also point to a possible misconception about likely targets and inadequate systems for preventing and managing the occurrence and aftermath of a terrorist incident.

Introduction

For some time, there has been evidence to indicate that terrorists have shifted their interests towards the public by focusing on soft unsecured targets such as buildings, businesses, public spaces and public infrastructure (Fischer and Green, 1992, Decker 2001, Gilbert *et al* 2003, Nathwani 2004). Although there has been a considerable amount of technical research and development to design more terrorist resistant buildings (Holtorp 1994, Vesilind 2003), the state of facility management preparedness has been largely ignored. The aim of this paper is to help address this problem by exploring current facilities management strategies to prevent, cope with and recover from terrorist attack.

Terrorism and the built environment

Terrorism is the systematic use of violence for the purpose of achieving a political objective (ADSC 1996, Pizam and Smith 2000, ASIO 2004). In countries like Australia, which have received specific threats of terrorist attack, protecting critical infrastructure and buildings from terrorism has become a high priority, prompting nationwide reviews of security (ASIO 2004, Vermeer 2004). These reviews have identified a range of facilities which are considered to be at particularly high risk of attack, including iconic buildings such as the Sydney Opera House, major bridges and public rail networks in major cities. Nevertheless, recent changes in terrorist strategies make it more likely that the focus of future attacks will be on soft unsecured targets where large crowds congregate such as transport facilities, large businesses, shopping malls, public spaces, schools, libraries and hospitals (Lorch 2001, ADSC 2004, Nicholls 2004, Nathwani 2004, Connolly 2004). Recent examples are September 11th bombings, the Chechnya school siege, the Moscow theatre siege, the Bali bombing, the Oklahoma bombing, the Aum Shinrikyo cult gas attack in Japan, the Madrid train bombings, the embassy bombings in Jakarta, Indonesia and the recent underground bombings in London.

Terrorism and facilities management

Most organisations are exposed to six main areas of security risk, namely: premises; personnel; equipment; data, information and knowledge; information systems and; public relations (BWA 1994). Facilities management is involved with the management of an organisation's premises risks and in simple terms involves planning, providing and managing a workplace environment to enable an organisation to achieve its core business objectives (Alexander 1996). Facilities management is a rapidly growing discipline which is in the process of defining itself and responsibilities taken by facilities managers can range from a simple traditional maintenance contract for building fabric and services to project management and space planning and more commonly, responsibility for a wide range of non-core business support services such as cleaning, catering, landscaping, parking, energy management, waste disposal and of course, security (McGregor and Then 1999, Barrett 2000, FMA 2004).

In recent years, security has understandably become a more important dimension of a facilities management function, since the security of an organisation's premises are is clearly central to the protection of an organisation's human, intellectual and physical capital and thus its

business continuity. However, in most organisations the importance of facility-related issues has gone unrecognised; security traditionally being restricted to issues such as theft, computer crimes, drugs and workplace violence (Baen 2002). This is a trend which has driven by a general belief that it is the government's responsibility to deal with terrorism in the built environment (NEI 2003). Nevertheless, recent changes in building procurement processes towards private-public-partnerships have ensured that over 90% of Australia's critical infrastructure and buildings are now privately owned. In this new privatised environment, effective protection against all forms of hazard, including terrorism, now depends on an effective partnership between the business community and government (Rothery 2005). While governments and authorities may do much to prevent the likelihood of terrorist attack through intelligence agencies, information networks and emergency services, it is also the responsibility of property owners and their facilities managers to manage this risk.

However, buildings represent a complex security challenge since the physical location, design, construction and operation of a building can represent both a risk and opportunity to security objectives. Nevertheless, it is important to recognise that most buildings and infrastructure were conceived and designed before recent terrorist attacks rose to prominence in peoples' minds, have not been designed with security in mind and therefore represent a logistical problem in controlling access and visibility. For example, many buildings have numerous access points which require a greater degree of security to prevent physical infiltration. Many buildings are located in busy inner-city areas where large numbers of people and buildings in the surrounding urban environment may afford protection for potential threats and risks for effective prevention and response. Furthermore, the majority of buildings we occupy have many spaces in which explosive devices can be easily concealed and which are difficult to monitor, control and evacuate. Indeed, with new high efficiency ventilation and water supply systems, very large buildings containing many thousands of people could be completely contaminated by a biological attack in a few minutes (CIS 2002, Perinotto 2002). The materials used in buildings can also hinder effective security. For example, contemporary cladding materials such as glass present a higher degree of visibility to outside elements, a high level of fragmentation in an explosion and modern sprinkler systems to deal with fire can cause enormous collateral damage to electronic information systems and security systems and can destroy physical data records. All of these risks are amplified when an organisation's facilities cover more than one building or site and where the facility envelope may include a range of areas for non-core services including catering, entertainment, recreation, relaxation, parking, refreshment etc. There may also be hazardous materials stored in the buildings such as compressed gasses, flammables, corrosive materials, explosives and even radioactive materials. And in some businesses, the number of people using a facility can run into many thousands per day and the access needs of all these people and the interrelationships between the many different functions which operate within it must be considered in any effective security strategy.

Clearly, with increased terrorist risks, it is now more important than ever, for building owners to think carefully about the design of their buildings and whom they share information with during the planning, design, construction and operational phases of a facility's life. It is also important that any response is commensurate with critical security threat factors such as: the significance of the business as a target; the proximity to such organisations; the history of terrorist attack in the building's proximity; the ease and extent of public access to the building and its surrounding urban environment and; existing security measures in the building and its surrounding environment. In response to these risks a range of preventative and coping design strategies should be employed to reduce the probability of terrorist attack and the impact of such an attack on physical assets and people, should it occur. For example, preventative measures may include: cladding or re-cladding a building in blast absorbing, non-fragmenting materials such as reinforced concrete or laminated/ reinforced glass; installing physical barriers to entry such as screens, turnstiles or landscaping; locating cellular offices on the perimeters of open plan offices; locating car parks away from highly occupied areas; locating important areas (with many employees, hazardous materials and critical systems) away from vulnerable disaster zones; simplifying perimeter shape and reducing perimeter area to minimise access and reduce blast waves reflection; floodlighting and; installing electronic alarms, detectors, surveillance cameras, close circuit TV and centralised control systems etc. (BWA 1994). The role of the facilities manager with responsibility for security is to ensure that such measures are incorporated into a business's facilities, that they are commensurate with levels of risk, that they are maintained effectively and updated in response to changes in critical risk factors and, that they are tested frequently. It is also their responsibility to liaise with emergency services, devise and document and implement emergency response procedures, to ensure that in the event of a crisis an organisation's assets and personnel are afforded maximum protection and to ensure that a business can recover from an attack as rapidly as possible. These dimensions of a facility manager's security responsibilities are discussed in more detail below.

A comprehensive terrorism management strategy

A complete strategy to deal with terrorism should incorporate a *preventative* (risk management), *coping* (crisis management) and *recovery* (business continuity management) dimension.

Prevention

Risk management is a proactive process to help mitigate risk which has a number of simple steps. First, the organisational assets which can be affected by an act of terrorism must be clearly understood to identify the potential impact of a terrorist act. These assets can include people, buildings, technologies, raw materials, data, reputation etc. Having identified assets and vulnerabilities, the next step is to identify ways in which they can be exploited and to measure the likelihood and consequences of this. The final stage of the risk management process is to develop, implement and monitor countermeasures to minimise the risks identified.

Crisis management

The steps involved in managing a crisis are: take charge; understand the circumstances; define the problem; identify solutions; move decisively to eliminate causes and; prevent recurrence (Loosemore 2000). Security and public relations are also important issues since interference from unwanted elements can exacerbate a crisis or, at the very least, interfere with its management. After a crisis, attention must be given to recovery and rectifying the long-term consequences of a crisis such as damage to the environment, or dealing with government or legal investigations.

Business continuity management (BCM)

BCM is concerned with how an organisation plans to re-establish key business processes in the aftermath of a crisis to ensure survival in the longer-term. The first stage in developing a BCM program is to develop a clear plan for development and implementation with key objectives and milestones. The next step is to ensure that managers understand their business and undertake a business impact analysis, which involves asking questions which revolve around "outage". Having identified maximum outages, a treatment plan should be developed to mitigate potential outage losses. The penultimate step is to document them in a BCM plan and to implement them and the final step is to regularly audit, test, refine and maintain it.

Method

A survey was conducted to investigate the risk management, crisis management and BCM strategies of facilities managers responsible for twenty seven potentially vulnerable buildings in the Sydney metropolitan area, Australia. A vulnerability assessment using FEMA (2004a) revealed that the sample consisted of no low risk buildings, 93% medium risk buildings and 7% high risk buildings. 74% of the buildings had a high visibility and 44% a high asset value, indicating that these buildings were important to their local constituencies. An accessibility assessment indicated that the sample buildings had unprotected entry and open access. Population capacities indicated that 85% of the sample buildings had a daily population rate of over 500 (19% over 5000, 44% over 1000 and 22% over 500) and 70% of the sample buildings had a local urban population within a one mile radius of over 5000 people.

Perceptions of vulnerability

Perceptions of vulnerability are illustrated in Figures 1 and 2.

Figure 1. Perceptions of vulnerability

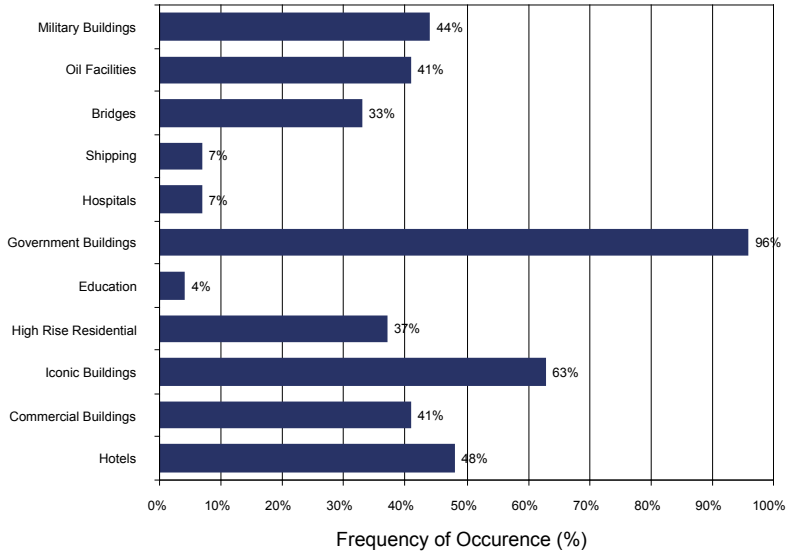
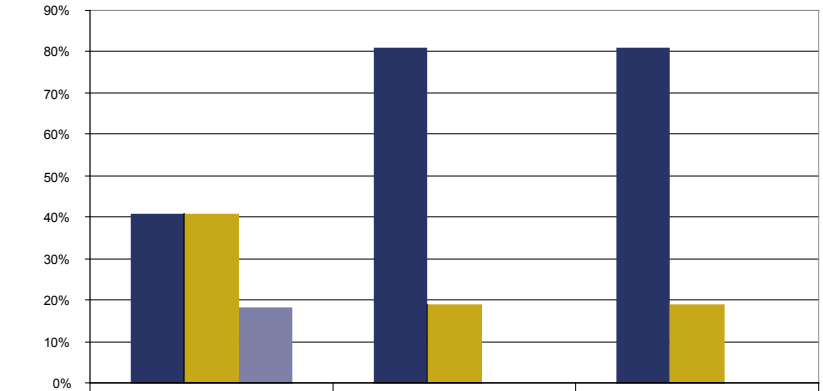


Figure 2. Perceptions of threat



	Australia	Respondents' Buildings	Respondents' Neighbourhood
LOW	41%	81%	81%
MEDIUM	41%	19%	19%
HIGH	18%	0%	0%

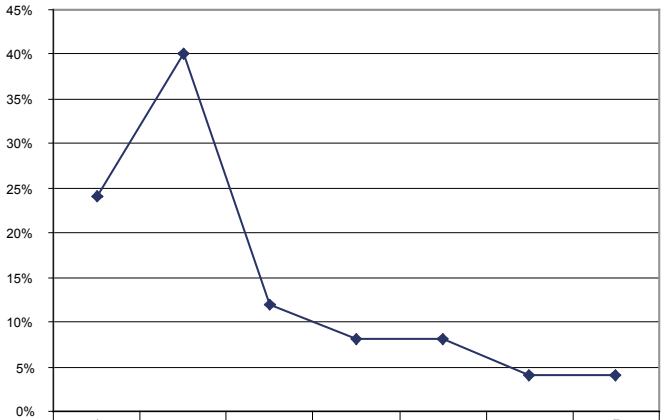
Threat Level

Predictably, government buildings were perceived as most vulnerable (96%), followed by iconic buildings (63%) and then hotels (48%). 41% of our respondents in Figure 2 considered the general possibility of attack to be low. 81% of our respondents also perceived the possibility of a specific attack on their building as low. These perceptions contrast with recent intelligence and research which identifies a medium level of risk and unsecured soft targets being at greatest risk. Further evidence of risk underestimation is found in a comparison of our respondents' perceptions of threat (Figure 2) with our initial vulnerability assessment which indicated that 100% of our sampled buildings were of medium or high vulnerability. Finally, the identical results relating to specific buildings and neighbourhoods are also interesting given the range of vulnerabilities identified in Figure 1. This may indicate that our respondents have difficulty in distinguishing between the two and understanding the relationship between their building and the wider urban environment. It also implies a lack of collective responsibility in the built environment towards dealing with terrorist threats, which could inhibit coordinated responses to such events.

Risk management

Figure 3 illustrates the perceived state of preparedness for terrorist attack in our sample.

Figure 3. Perceived state of risk management preparedness



	1 Totally unprepared	2	3	4	5	6	7 Very well prepared
Frequency of occurrence (%)	24%	40%	12%	8%	8%	4%	4%

Rating

76% of our respondents considered their buildings as being unprepared for an attack (24% being totally unprepared). 48% of respondents had a formal risk management system to deal with terrorism, while 41% did not and 11% did not know. 64% of those who did not have a system in place cited the low risk of terrorism as the reason. The other 36% provided a range of reasons such as "not applicable", "the tenant has a program in place", "considered necessary but not yet implemented", "currently looking at a program" etc. Of those programs that did exist, 69% had been developed in the last five years, in reaction to the September 11th and Bali bombings.

Figure 4 shows that risk management systems typically focussed on the protection of employees, premises and plant and equipment. The protection of IT systems and business processes are given relatively low priority.

Figure 4. Scope of risk management systems

	Respondent												
Activities	4	5	8	10	11	12	14	20	21	22	23	24	25
IT / Communication Systems		✓	✓										
Premises / Facilities		✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Processes		✓	✓	✓									
Plant and equipment		✓	✓		✓			✓	✓	✓	✓	✓	✓
Employees / tenants		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Other													
Don't know	✓												

Crisis management

74% of our respondents had a crisis management plan for terrorism, a higher response than the 48% for risk management systems, indicating a reactive approach to the problem. Perceptions of crisis preparedness are illustrated in Figure 5.

Figure 5 does not reflect that 74% of our respondents had a crisis management plan and would suggest a relatively low level of confidence in them. Only 55% of our respondents had updated their plans, 20% had never been updated and 25% of our respondents did not know. The channel used most widely to communicate those plans were evacuation drills (95% of respondents) and training (75% of respondents) and the stakeholders involved are illustrated in Figure 6.

Figure 5. Perceptions of crisis preparedness

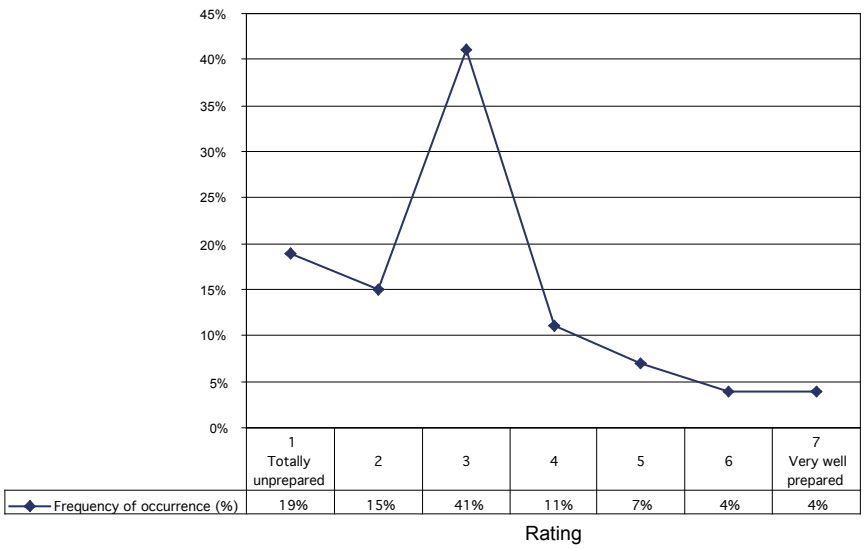


Figure 6 indicates that crisis management planning is internally focussed on workers and employees. The complete exclusion of the unions is somewhat surprising given their strong emphasis on health and safety but may reflect a non unionised white collar workforce. It is also surprising that 40% of our respondents did not consider clients as a key stakeholder and that 70% did not see the media as an important stakeholder. These findings are reflected in the perceptions of communication illustrated in Figure 7.

Figure 6. Stakeholders in crisis management planning

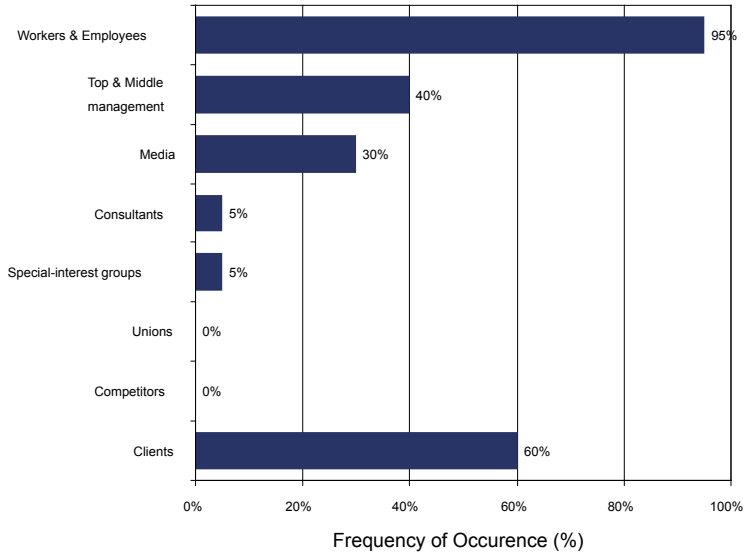
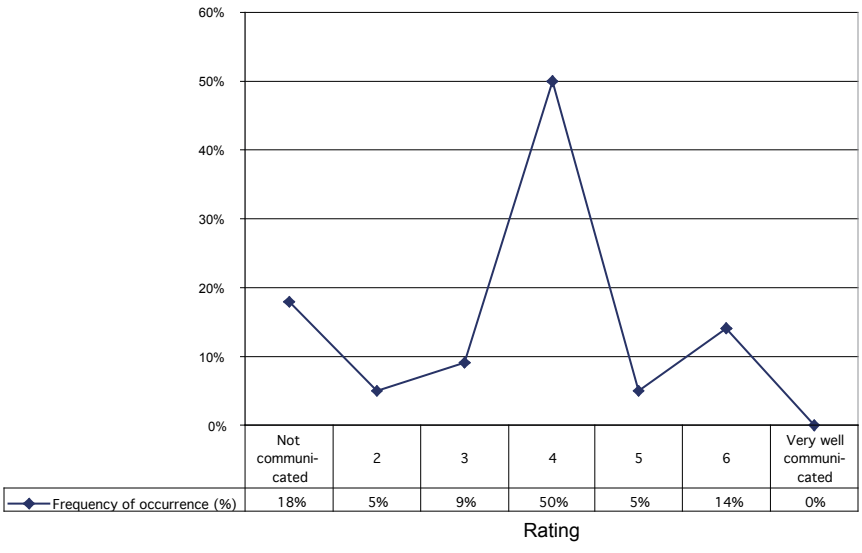


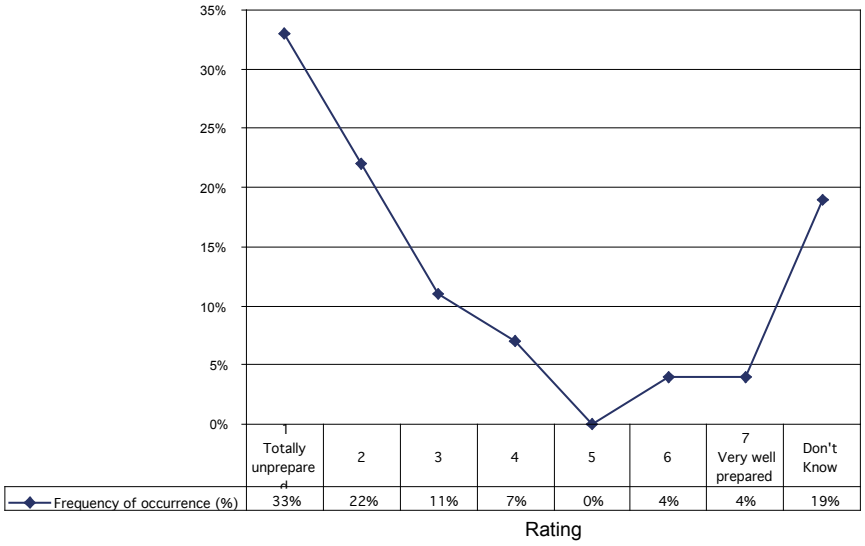
Figure 7. Perceived communication effectiveness of crisis management plans



Business continuity management

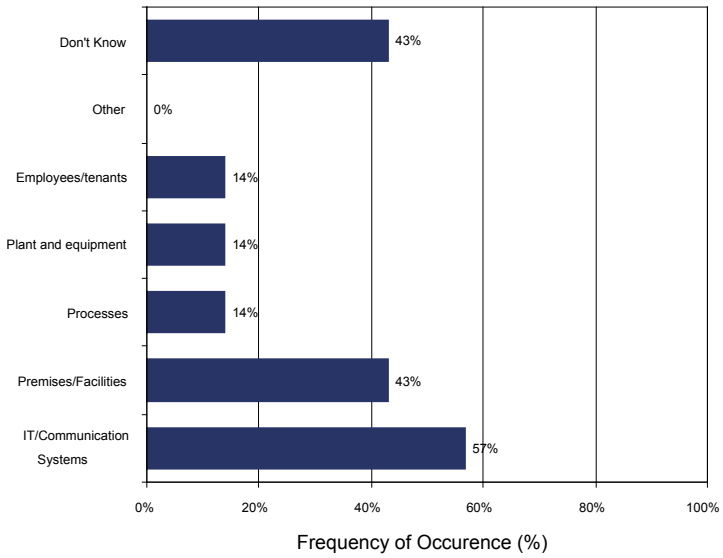
The overall rating of BCM preparedness given by our respondents is illustrated in Figure 8.

Figure 8. Perceptions of BCM preparedness



The rather poor state of preparedness portrayed in Figure 8 is reflected by the fact that only 26% of our respondents had a BCM plan in place, that 52% did not and that 22% did not know. Reasons for this revolved around a perceived lack of responsibility for clients' business operations. Other reasons were terrorism being a low risk (31%) and BCM planning being a low priority (56%). To most of our respondents, BCM was seen as the responsibility of individual tenants reflecting an ignorance of the relationships between buildings and tenant business objectives. Of the 26% of respondents who did have a BCM plan in place, only 57% had undertaken a criticality assessment. This is not surprising given that tenants were rarely regarded as key stakeholders in BCM planning. The most widely involved stakeholder was the IT department which reflects the common problem associated with BCM plans to focus on IT activities, as illustrated in Figure 9.

Figure 9. Stakeholders in BCM planning



Conclusion

Given the exploratory nature of this research, it was inevitable that our survey was general in nature and fairly limited in scope. There is undoubtedly a need for more extensive and detailed investigations of the risk management, crisis management and BCM practices of facilities managers in a range of different building contexts. Furthermore, this research was conducted before the London underground bombings which are likely to have changed perceptions of terrorist risk, at least in the short-term. Nevertheless, the picture which has emerged from this research is quite disappointing. Not only is there a general lack of preparedness for terrorist attack but there is a worrying level of ignorance and a lack of confidence in the limited plans that do exist. Furthermore, the limited measures that have been taken to deal with this threat are largely reactive in nature and our respondents seemed to underestimate the level of risk in a general and specific building context. There was also a general misconception about likely targets.

References

Alexander, K (ed) (1996) *Facilities Management* – Theory and Practice, E & FN Spon, London.

ASIO, (2004) *The Year In Review 2002/2003* [Online] Available: http://www.asio.gov.au/Review/Contents/review.htm [14th March 2004].

Australian Defence Studies Centre (1996) *Terrorism and the 2000 Olympics*, ADSC, Canberra.

BWA (1994) *Facilities economics*, Bernard Williams Associates, Building Economics Bureau Limited, London.

Baen, J.S. (2002) *The implications of September 2001 and terrorism on international urban form and various classes of real estate*, University of North Texas, USA.

Barrett, P. (2000) 'The role of real estate assets in supporting the fulfilment of corporate business plans: key organizational variables for an integrated resource management framework', *Facilities*, Vol.18, No.10/11/12, pp. 421–426.

CIS (2002) *The infrastructure security partnership* (TISP), Congress on infrastructure and security for the built environment, First congress, , Nov 5–7, Washingston DC.

Connolly, E. (2004) *Businesses ignoring possibility of attacks, says security adviser*, Sydney Morning Herald, 16 July 2004.

Decker, R.J. (2001) *Key elements of a risk management approach*, [Online] Available: www.gao.gov/new.items/d02150t.pdf [3 April 2004].

FMA (2004), *What is Facilities Management*, Facilities Management Association of Australia [Online] Available: http://www.fma.com.au/content.cfm?infopageID=12, [8th May 2004].

FEMA, (2004) *Emergency management guide for business and industry*, [Online] Available: http://www.fema.gov/library/prepandprev.shtm#terrorprev [28 March 2004].

FEMA, (2004a) *Reference manual to mitigate potential terrorist attacks against buildings*, [Online] Available: http://www.fema.gov/fima/rmsp426.shtm [28 March 2004].

Fischer, R.J. & Green, G. (1992) *Introduction to Security*, 5th ed., Butterworth-Heinemann, USA.

Gilbert, P.H. *et al*. (2003) Infrastructure issues for cities – countering terrorist threat, *Journal of Information Systems*, ASCE, March 2003; pp.44–54.

Holtorp, P. (1994) In response to the terrorist threat: the security plan, *Facilities*, Vol. 12, Iss 5; pp 16–19.

Loosemore, M. (2000) *Crisis Management in Construction Projects*, ASCE Press, Virginia.

Lorch, R. (2001) Tall buildings, high density and terrorism, *Building Research* and Information, 29(6), pp. 415–416

McGregor, W. and Then, D.S. (1999) *Facilities management and the business of space*, John Wiley and Sons, New York.

Nathwani, A. (2004) *Impact of extraordinary incidents on buildings & building services*, Norman Disney & Young, Sydney.

Nicholls, S. (2004) *ASIO lends its expertise for state's anti-terror shield*, Sydney Morning Herald, 29 April 2004.

NEI (2003), *Nuclear Plant Security*, Nuclear Energy Institute, [Online] Available: http://www.nei.org/index.asp?catnum=3&catid=48 [8 May 2004].

Perinotto T (2002) *Designing for a post-September 11 world*. Australian Financial review News , 5th April 2002, p 45.

Pizam, A. and Smith, G. (2000) Tourism and terrorism: a quantitative analysis of major terrorist acts and their impact on tourism destinations, *Tourism Economics*, Vol. 6 (2); pp 123 – 138.

Rothery, M (2005) Critical infrastructure protection and the role of emergency services, *The Australian Journal of Emergency Management*, 20 (2), 45–50.

Vermeer, T. (2004) *Security barriers for Opera House*, The Sunday Telegraph, 21 March 2004

Vesilind, P.A. (2003) Engineering and the threat of terrorism, *Journal of Professional Issues in Engineering Education and Practice*, ASCE, April 2003; pp.70–74.

Author

Siaw Khiun Then is a Research Assistant and Martin Loosemore is Professor and Associate Dean of Research at the Faculty of the Built Environment, University of New South Wales, Sydney, 2052.
Email: mloosemore@unsw.edu.au