GUIDE TO SRMBOK

EXPLOSIVES INCIDENTS

The Security Risk Management Body of Knowledge (SRMBOK) was developed as an initiative of the Risk Management Institution of Australasia Limited (RMIA) in conjunction with Jakeman Business Solutions Pty Ltd (JBS), which provided the lead authors and financially underwrote its publication.

SRMBOK was written to contribute to the identification and documentation of agreed better practice in Security Risk Management. Copies of SRMBOK can be purchased from www.amazon.com

SRMBOK is also supported by many *Guides to SRMBOK* written by independent security professionals that provide more detailed guidance and examples of how the SRMBOK framework can be applied in practice. Whilst each of these Guides is peer reviewed prior to publication, any opinions and views expressed are those of the authors and do not necessarily reflect the opinion of RMIA or Jakeman Business Solutions Pty Ltd.

Security Risk Management

Body of Knowledge

Abstract

This Guide to SRMBOK is focused on the management of explosives incidents (bombs).

The objective of this 'Guide to SRMBOK' is to help readers understand and mitigate the risks associated with explosives and effectively apply security risk management strategies in an integrated and cohesive fashion.

It has been written in such a way as to stand alone so far as possible, however it is assumed that most readers will be familiar with the concepts and definitions described in the Security Risk Management Body of Knowledge (SRMBOK).

Author

D. S. Williams CPP

Don Williams holds qualifications in Security Management, Security Risk Management as well as Project and Resource Management. He is a Certified Protection Professional (CPP) and a member of ASIS (International) and consults on strategic security analysis.

Based on his security qualifications and over 20 year's experience as a bomb technician in the Australian Army, including three years at the Australian Bomb Data Centre, Don was appointed the Bomb Risk Manager for the Sydney Olympics and Paralympics. He is a member of the Venue Managers' Association and the Institute of Explosive Engineers and is a past Australian Chapter Director of the International Association of Bomb Technicians and Investigators.

Don can be contacted at *donwilliams@grapevine.net.au*

Contents

1. INTRODUCTION

All organisations may experience the fear caused by bombs or the threat of bombs[1]. Security Risk Managers will be involved in defining and implementing bomb protective measures to protect their personnel, information and capability as well as the public.

Bombs are literally “devastating”; large amounts of energy are released in milliseconds creating forces capable of destroying buildings, IT systems, vehicles and equipment and killing and injuring large numbers of staff, clients and the public. The effects of a bomb can be similar to those of an industrial accident or natural disaster but are caused by deliberate human action.

Bomb incidents pose considerable challenges to Security Risk Managers. In many countries, explosives are readily available, or if not, suitable explosive and incendiary compounds can be manufactured from domestic and industrial materials. The initiative will always rest with the bomber who defines: the motive, target, placement, concealment, activation method and the timing of the attack. A bomb does not normally require the perpetrator to be at the scene during the explosion. The effects of a bomb far outweigh the cost of the materials involved. Bomb incidents are newsworthy. The threat of a bomb takes few resources but can have considerable disruptive effect.

All assets can be considered vulnerable to an explosive event. Bombs provide the capability for the offender to do considerable damage with little financial expenditure. The use or threat of, bombs can be used to support a wide range of political, criminal and social motives. The offender can determine the placement and timing of the explosion and, unlike most crimes, does not have to be on site at the time of the event.

Bomb incident management is predominantly a management-level responsibility relying on decisions made with limited information and within a limited time. It is only through the development of appropriate and applicable procedures relevant to the organisation, based on sound security risk analysis that an effective bomb incident management capability can be developed and implemented.

1.1. Applied Methodology

Details of the risk management process are provided elsewhere in the SRMBOK and this document should be read in the context of methodologies such as AS/NZS4360:2004, Hierarchy of Control (ESIEAP), HB167 Security Risk Management Handbook, etc. In outline however, based on information gathered, the likelihood and consequence of each type of bomb incident is assessed and a relative risk rating is defined. Once the risks are identified and rated, specific treatments to reduce their likelihood or consequence can be designed within the available resources and limitations. Security Managers can then apply the appropriate treatment measures to deal with the recognised priority risks.

1 The term ‘bomb’ is used generically throughout this document to include improvised explosive devices (IED’s) whether based on military ordnance, industrial explosives or homemade explosives wherever they are used or intended for use in an unlawful fashion. Ref: Section 2 for details.

To be effective, the risk assessment must be conducted early enough to enable procedures to be developed and practiced. The assessment may need to be revised as related security plans and site surveys are developed. The bomb risk plan should be part of an integrated security risk management process and not conducted in isolation.

The risk of a bomb-related incident can originate from a number of threat sources; telephone threats, vehicle bombs, chemical threats, suicide bombs, incendiaries, pyrotechnics used in pranks, pipe bombs, threats over the internet, mail bombs, hoax devices of all shapes and sizes, booby traps, remotely controlled devices, government sponsored groups, extremists and issue motivated individuals are just a few examples.

1.2. Gathering of information

To be relevant a risk analysis must be based on comprehensive and accurate information. Bomb incident information can be gained from a range of sources including:

- Open source media;
- Historical records;
- Organisational data;
- Professional organisations;
- Intelligence agencies;
- Bomb Data Centres (or equivalents);
- Computer modeling; and,
- Corporate, National and International liaison.

As can be seen, bomb risk analysis cannot happen in isolation, it requires the support and interaction of organisations not often associated with bomb safety. Not all the desired information will be available, which is why an assessment of the risks is required.

1.3. Specific Information Requirements

To enable an effective bomb risk analysis, information is required on topics such as:

- The level and type of “normal” bombing activity within the area of interest;
- Detailed knowledge of the site and activity under review;
- Trends and changes in bomb incidents;
- Political and issue motivated groups and their motives and methods of operations;
- Specific people or sites which are or may be considered targets;
- The availability of explosive materials or their constituents; and,
- Planned or possible changes to the working and political environment.

The following topics are of particular importance when considering bomb risk analysis and security measures.

1.4. Trends

A threat assessment of existing and potential bomb and threat making groups and individuals combined with a review of bomb incident trends in the area of interest and industry, provide the basis for the risk analysis.

1.5. Motives

A review of motives will provide a valid basis for determining what sort of attacks may be expected and why they may be launched. The review can determine the motive, target and desired results of different groups and individuals. For example there are groups whose desired outcome may be the destruction of property, but not the taking of life. Others wish to create confusion and concern via threats, some will intimidate for financial gain, and some will want to kill.

An understanding of the motives will also assist in defining the targets which may be attacked and the method that may be used. This review is likely to be generic, but can provide a solid basis upon which to develop more specific target reviews.

When considering the motives for hoax devices (defined as items manufactured to represent real bombs and to create fear in those that find them), they should be dealt with in a similar manner as bomb threats. Their intent is usually to create disruption without actually causing harm or damage. Consideration of hoax devices when developing treatments is detailed below; it is recommended that hoax devices be dealt with in the same manner as live devices.

1.6. Resources

As part of the information gathering phase an understanding is required of the resources available for use when defining treatments. The resources will include the people, equipment and financial assets. Some will be integral to the organisation conducting the review, possibly including search personnel and equipment.

1.7. Constraints

Constraints that will limit the treatment options are also important. These will normally be in the form of personnel availability, time and finances. Another major constraint is likely to be the need to operate within the ethos or image of the environment or activity of the operation. For example in some cases the security measures may have to be unobtrusive or fit within the requirements of a “friendly and welcoming” atmosphere in others, a visible and declared level of security may be preferred.

1.8. Defending Against Bomb Incidents

The methods described in this Chapter along with the outlined treatments and examples provide an additional tool to defend against bomb incidents.

2. DEFINING BOMB INCIDENTS

Bombings are not a new phenomenon; they have been used by criminal and political offenders for centuries. One of the earliest recorded instances of a sophisticated bomb was the attempt by Felice Orsini to assassinate Emperor Napoleon III in 1858. Experience and statistical analysis show that bombings are still the preferred weapon of terrorists[2] as well as being a common tool for criminals[3].

2.1. Types of Bomb Incidents

Accurate and consistent terminology is essential when defining and assessing risks, threat actors, vulnerability, security events and risk mitigation treatments in relation to bomb incidents. The ill-informed use of terms can prejudice the entire process. As an example, the common use of the term "bomb hoaxes" suggests that the subject item or call is already defined as a hoax before any evaluation has been conducted. The following are definitions of the types of bomb incidents that may be experienced by any organisation. Risk management considerations for each of these types of bomb incidents are provided in this chapter.

- **Bomb.** An explosive or incendiary device designed to create damage and injury.[4] A bomb can be made from commercial, military or improvised/home-made explosives and components. A bomb can be hand-delivered, vehicle-borne, part of a suicide attack, projected by a weapon, or delivered to the target by a range of other means.
- **Unattended Item.** An item whose presence is not readily explained and which could contain a hazard such as a bomb. Unidentified items should be investigated to determine if they are believed to be hazardous or if they are safe.
- **Bomb Threat.** A threat that a bomb has or will be used against the organisation or person.
- **Mail bomb.** An explosive or incendiary device sent through the postal or courier systems. As the delivery, identification, assessment and response options differ from bombs placed on the site by the offender they have different risk mitigation considerations.
- **Post-blast**. If a bomb explodes (i.e. a risk is realised) there will be damage and possibly injuries. The site will probably be a crime scene and business continuity/resumption, staff support and related business plans will be implemented[5].

2 The US Department of State Report for 2003 shows that of international terrorist incidents, 67% were bombings, 27% were armed attacks and less than 1% were hostage takings.

3 The Australian Bomb Data Centre reported 589 bombings (explosions) in Australia in 2003. The US Bureau of Alcohol, Tobacco, Firearms and Explosives reported 220 bombings in the same period. UK statistics are not published in an unclassified form. The ABDC reported 183 bombings in 2005.

4 The Australian Bomb Data Centre defines a bomb as an: "Improvised Explosive Device (IED). A device fabricated in an ad hoc manner which contains explosive components designed to, or capable of, causing unlawful injury or damage." Australian Federal Police ABDC "Bombs Defusing the Threat" 2001.

5 The Australian Bomb Data Centre defines a bombing as "An incident involving the use of one or more improvised explosive devices (IED) which has functioned. Military explosive ordnance which may not be improvised but which has been used in an illegal manner is also included in this definition". http://www.afp.gov.au/services/operational/abdc/abdc_incident_types

- **Hoax**. An item or threat which does not actually represent a hazard. Appropriate and practiced bomb threat analysis and unattended item procedures will help in determining if these types of incidents represent a hazard. If an item is believed to be a bomb it is usually beyond the capability of an organisation to determine if the contents are live explosives or hoax material, this is the role of the investigating emergency services who will examine the contents once the item has been dismantled. The term “Hoax” should not be used until after the incident is concluded and the summary report is being written.

2.2. Elements of a Bombing

In order to apply risk management principles it is necessary to understand the elements required for an offender to conduct a bombing. These are: Motive, Material, Knowledge and Opportunity.

- **Motive**. The motives for using or threatening to use a bomb can be: criminal (murder, extortion, intimidation, vandalism, etc); political (issue motivated/cultural/terrorism, etc); or personal (mental illness, disgruntled employee, domestic problems, etc). As a result, any site could be the target for someone with a motive against the organisation or someone on the site.
- **Material**. A bomb requires certain components: a main charge of explosive or incendiary material, an initiator to detonate or ignite the main charge, a triggering mechanism and a safety switch. The components can be manufactured for the purpose or improvised. The explosive or incendiary material can be commercial, military or home-made. The material to manufacture a bomb exists and is available.
- **Knowledge**. Knowledge is required to build a bomb. This knowledge can be obtained through formal training in the use of explosives provided to the mining, rural and construction industries, pyrotechnical companies, the military and law enforcement agencies. In addition knowledge can be gained through personal research of texts and over the internet. Also, terrorist organisations provide formal training in manufacture and use of bombs. To successfully place a device on site the offender requires knowledge of the organisation, its layout, security and procedures. Little knowledge is required to make a bomb threat.
- **Opportunity**. The offender requires the opportunity to place the bomb on or near the targeted organisation or individual. This is the element which the organisation can utilise as part of its security risk management plan. It is possible to: deny access to the offender to some areas; deny the ability to bring explosive devices onto the site i.e. through the use of detection systems, and to have in place the ability to detect and respond appropriately to the range of bomb incidents.

2.3. Explosive Effects

To effectively plan for bomb incident risks, it is necessary to have an understanding of the effects of an explosion. This section provides a brief overview of explosive effects. The visual effects seen at the cinema do not reflect normal explosive events and may lead to a false sense of the peril faced by the organisation.

In brief, an explosive is a chemical composition where the chemical bonds can be relatively easily broken causing the material to become a gas. What differentiates an explosive is the rate at which the change from solid/liquid to gas occurs. In a fire the solid material is converted to gas at a very slow rate, in an explosion the rate of change is measured in terms of 1000's of metres per second.

The standard measure for explosive comparison is TNT (trinitrotoluene) which has a "detonation rate" i.e. the rate of chemical change over a linear distance of 6900 metres per second and 1 kg of TNT will produce about 730 litres of gas[6].

2.3.1. Blast

The gas released from this chemical breakdown requires considerably more volume than the initial explosive and so it moves away from the site of the explosion. The rapid expansion of gas (the blast wave) is what breaks and destroys the surrounding structures and people. This wave can be thought of as a wall of compressed air travelling at close to the speed of sound. Immediately behind the blast wave is a low pressure area from which the compressed air was drawn, this low pressure area (sometimes incorrectly referred to as a vacuum) further damages structures weakened by the blast wave by causing them to stress in the opposite direction. The exact effects of the explosion depend on the nature and quantity of the explosive, the effectiveness of the initiation system, its location including blast-reflecting surfaces, the casing of the bomb, and numerous other factors[7].

As an example 1 kg of TNT, placed on the ground without any confinement and correctly detonated will apply approximately 43 kPa to a wall 5 meters away about 8 milliseconds after detonation. If, for some reason, the wall did not fail, the pressure would continue to build up to over 100 kPa[8]. It is the speed with which the pressure is applied and the resultant impulse that makes explosive force such an effective mining and demolition tool and a weapon.

Depending on the bombs location, the blast effects may injure and kill people, damage sensitive IT equipment, cause various levels of structural damage, remove sprinkler heads and damage water pipes, disrupt building services including communications and hinder rescue and emergency responses.

The blast wave fades quickly as it passes through the air decreasing in compliance with a cube root rule. The same 1 kg TNT explosion will only apply 8.6 kPa to a wall 15 meters away. Therefore distance is of significant benefit when assessing bomb incident preventative and response measures; the ability to keep the bomb some distance from the asset and the ability to move the assets, particularly people, away from the bomb is a fundamental principle of bomb security and safety.

6 Narayanan T. V., Modern Techniques of Bomb disposal and Detection P36. RA Security System New Delhi 1996

7 The information presented here is a simplistic summary of a complex field of gas and hydro-dynamics. Technical information on blast effects is available from engineering, mining and military texts and from professional organisations such as the International Association of Bomb technicians and Investigators and the Institute of Explosives Engineers.

8 TM 5-855-1 Conventional Weapons Effects. US Army Engineer Waterways Experimental Station. 1992

2.3.2. Fragmentation

The casing of the bomb and anything nearby will be shattered and turned into projected fragments. In some cases the bomb is designed to enhance the fragmentation effect through the addition of nails, etc. Fragments tend to travel in straight lines. Distance, and also something solid between the asset and the bomb, are effective protective measures.

A major factor, when considering blast effects, is the shattering and projection of glass, particularly from windows. The bombings of the US Embassies in Nairobi and Dar es Salaam in August 1998 resulted in 258 killed and over 5000 injured of which approximately 1000 people were blinded by glass fragments[9].

2.3.3. Heat

The detonation process is exothermic and generates considerable heat. The 1 kg of TNT will generate a temperature of approximately 1000 K cal/kg[10]. For many explosives this heat does not last for long and it is unlikely a fire will start unless there are combustibles in the immediate area or the bomb has been designed with added accelerants to enhance the incendiary effect. Some explosive material generates more heat over a longer period and has a greater incendiary capability. Some bombs are specifically designed as incendiaries with the burning of the asset the main aim.

2.3.4. Advantages and Disadvantages to the Offender

The use of a bomb provides the offender with certain advantages compared to other forms of physical attacks. It also offers disadvantages which work to the benefit of the Security Risk Manager.

2.3.5. Advantages to the Offender

Potential advantages, that the use of bombs, offers the offender include:

- Large amount of damage compared to the size of the device.
- Greater level of damage than from an armed assault.
- Degree of anonymity as the offender does not have to be on site at the time of the incident.
- If the asset is on or near the boundary then the offender may be able to attack the asset without having to enter the site. Bombs offer the distinct advantage of creating considerable damage from outside the fence. Noting that the greater the distance of the asset from the fence the larger the bomb that has to be manufactured (e.g. see the Kohbar Towers example at the end of this chapter).

9 http://www.dojgov.net/Clinton_&_Terrorism-01.htm
10 ibid Narayanan 1996.

- The effects of a bomb threat can be considerable including: disruption to the organisation's operation and reputation with little expense by the perpetrator. Hence the term "ten pence terrorism11".
- High media value making it a good means of publicising a cause.

For suicide bombers (political or mental illness) the considerations of detection on site do not apply to the same degree, as the bomber does not need to be as surreptitious or to have an exit plan. Considerations for managing the threat posed by suicide bombers are included in this Chapter.

2.3.6. Disadvantages to the Offender

Disadvantages to the offender which can be advantages to the Security Risk Manager include:

- Risk of the offender blowing him/herself up during construction or transportation.
- Possibility that the bomb may not function as intended or at all.
- Risk to the offender of detection when placing the bomb either on or near the site or into the mail system.
- There is a risk that the device may be detected before it detonates resulting in the safe evacuation of people and information and possibly the rendering safe of the item.
- There is considerable forensic evidence from the construction of the bomb which increases the risk of identification and arrest.

2.4. Risk Considerations

The risks relating to bomb incidents can be assessed and mitigation strategies developed using standard security risk management principles and techniques.

Guidance on defining the risks in relation to the various types of bomb incidents is provided in the next section. An assessment of the likelihood of an organisation or individuals being exposed to the risk is based on a threat and vulnerability assessment that encompasses the changing profile of the organisation and the protective and procedural security measures in place.

The consequences of a bomb incident can be assessed and rated based on knowledge of the assets at peril and the potential effects of the bomb incident under consideration, given the operating environment of the organisation.

While recognising that the initiative rests with the offender, as does the design and placement of a bomb, it is possible to identify and implement appropriate risk mitigation

11 A reference used by UK law enforcement to reflect the cost of a local call.

treatments. These treatments will usually increase the ability to deter a bomb incident and to have appropriate response measures in place to respond to the incident and to minimise the harm to the assets and operation of the organisation.

3. ASSESSING BOMB INCIDENT RISKS

This section provides guidance on defining the risks; the factors that influence the likelihood and consequences; the SRM analysis factors that should be considered; and risk mitigation options for each of the types of bomb incidents (bombs, unattended items, threats, mail bombs and post-blast).

As previously stated, the initiative rests with the offender who has a motive, the material and the knowledge to build and deliver a bomb or to make a bomb threat.

3.1. Risks Relating to Bombs

The principles outlined in this Chapter apply to all types of bombs: hand delivered, vehicle borne, mail bombs, suicide bombs, etc. The detailed application of the principles will vary depending on the threat analysis, exposure and vulnerabilities of the organisation. Separate sections are provided in this Chapter on the specific considerations for mail bombs and suicide bombs.

Most organisations are unlikely to be subjected to a bombing, but as suggested in the previous section, the motive, material and knowledge exists and the Security Risk Manager should assess and monitor the likelihood of the risk occurring.

The likelihood of an offender having the motive and means to build and deploy a bomb is not one the organisation can readily manage, rather the risks related to a bomb being used against the organisation could be defined in terms of:

- “Failure to prevent a bomb from entering the work place …”
- “Failure to protect assets from a bomb (on site/off site/when travelling)…”

These can be further devolved to:

- “Failure to identify a bomb (on site/off site) ...”
- “Failure to respond appropriately to a bomb …

Factors that will influence the likelihood assessment for such a risk will include:

- The existing social, political, workplace and other situations which might make the organisation a more likely target for an act of violence. This could be determined from a specific bomb vulnerability assessment or as part of an enterprise-wide vulnerability assessment. It is essential that bomb incident risks be reviewed as the operating environment, exposure and vulnerabilities change. It is possible that business efforts and relationships elsewhere may alter the likelihood of an attack against an organisation and that the likelihood of a bomb incident will increase and decrease over time.

- Basic access control measures, including adequate boundary protection, personal identification and verification systems ranging from electronic systems to key control processes, restricting the public to public areas, etc.
- “Defence in Depth”, providing additional levels of control and restricted access to higher value assets.
- Good workplace practices such as keeping areas tidy and clean so that any items introduced to the work area will be quickly identified.
- Staff awareness and an ability and awareness to identify items which are out of place and report them to their supervisors/managers.
- Supervisors/managers having the training and knowledge to respond appropriately to a report of a bomb from staff or the public.
- The proximity of assets to the boundary e.g. where the building housing asset forms part of the boundary and the bomb can be placed near the external wall. In such cases the likelihood of detecting such an item and the ability to respond to it should be assessed. CCTV/IPTV and mobile guards may be factors in this assessment.
- Detection equipment. If bomb detection equipment has been deployed it is important that it is: appropriate and capable of the task for which it is employed; that the equipment is deployed as part of a cohesive security plan; that it is maintained; that staff are trained and that processes are in place to respond if they find that which they are looking for i.e. a bomb.

It will be noted that most of these factors are those required to maintain a normal safe and secure work area. Therefore in many respects mitigating the risk of a bomb incident will build on existing security and safety measures.

The consequences of failing to prevent a bomb include:

- An explosion should the bomb detonate. In which case the specific consequences will vary depending on the construction, type and location of the bomb, particularly its proximity to various assets. Response considerations for an explosion are outlined below under “Post-blast”.
- Disruption to operations, should the bomb be identified, while an evacuation is initiated and the incident is managed by the site’s Emergency Control Organisation. As mentioned above, the best protection from a bomb is usually distance provided by an evacuation. The site’s evacuation plan should be reviewed to ensure that the evacuation distances are far enough away from the site to provide adequate protection. Many fire safety evacuation assembly areas are too close for bomb safety considerations.
- Concern by staff, clients and public over the handling of the incident. Documented and rehearsed procedures will assist with this issue.
- Hazards faced by people during an evacuation such as road crossings, handicapped egress, etc, these should be addressed in the site’s emergency procedures.
- Depending on the motive and skill of the offender there is a possibility of other bombs being on or near the site. The emergency procedures should include the requirement for the egress routes and assembly areas to be inspected for

unidentified items prior to or during the evacuation. Such an inspection is good practice as it will also detect blocked exit routes or other barriers and hazards.

Even though the likelihood may be assessed at the lower end of the scale the consequences of an explosion can be catastrophic and appropriate risk mitigation treatments should be considered.

Remember, the bomb can only be classified as a "Hoax" by the responding Emergency Services or forensic team.

The primary treatments for responding to a bomb include the ability to detect the item and to respond appropriately and safely. The organisation's evacuation plans should be reviewed to ensure they provide adequate distances and alternative evacuation routes and assembly areas suitable for explosive hazards as well as fire. The evacuation routes and assembly areas should be inspected by wardens or others (who are trained) to make sure they are free from obstructions and hazards including other bombs. Consideration should also be given to the evacuation of information during an emergency. The specific response plans will vary by site, organisational function, and assets based on the risk assessment.

3.1.1. Suicide Bombers

The management of risks related to suicide bombers requires the same considerations: identifying the hazard and having responses in place. The unique qualities of the suicide bomber mean that traditional deterrents such as CCTV which may lead to being arrested for example are unlikely to be as effective as for other attackers. Equally, although this group is a sub-set of the broader bomber group, this tactic has been popular with insurgents and fanatics for centuries and in some regions will constitute the primary threat vector for attack.

Organisations need to carefully consider if they are likely to be the target of this small sub-set of bombing offenders. The identification and response to suicide bombers may be more difficult as there may be less time to respond and the suicide bomber is the ultimate guided weapon capable of changing its target and timing[12]. The technique for identifying a suicide bomber is the same as for other types of bombs: recognising that which is out of place, that which does not fit the environment. Detecting a suicide bomber may be difficult as they usually disguise or conceal their bombs and can alter their approach if they think they may be detected. If a suspected suicide bomber is identified, usually the best way to minimise the consequences is to immediately begin to move people away and to limit the bombers ability to get closer to the organisation's assets. History shows that once a suicide bomber believes he/she has been detected or is to be thwarted in their attack they will try to detonate the bomb to cause as much effect as

[12] C Williams. Suicide Bombers. Australian Homeland Security Research Centre presentation 2005. Additional information on suicide bombers' motives and techniques can be found in C. Williams C., "Terrorism Explained" P57. New Holland Publishers 2004; Bloom M., "Dying to Kill: The Allure of Suicide Terror", Columbia University Press 2005; Pape R., "Dying to Win: The Strategic Logic of Suicide Terrorism" Subscribe Publications, 2005.

possible. If the risk of "Fail to protect from a suicide bomber …" is realised then there will be a need to have a post-blast plan prepared.

3.2. Risks Relating to Unattended Items

There is a reasonable probability that unattended items will be found at any organisation. It is possible the item may be lost or left goods, workman's tool boxes, tourists' bags, rubbish, courier-deliveries, other non-hazardous items, or a bomb. Such items are more likely in public areas such as foyers, entrance ways and outdoor areas. In most cases there will be doubt as to the nature and origin of the item. If an item found on site obviously appears to be hazardous i.e. visible wires and components that look like explosives, switches, etc or because of its location i.e. strapped to fuel tank, then the item should be considered to be a bomb and the appropriate measures implemented.

The aim is to determine if the unattended item poses a hazard.

The risks related to unidentified items could be defined in terms of:

- "Failure to identify an unattended item …"
- "Failure to respond appropriately to an unattended item …"

The likelihood of detecting unattended items increases if the staff are trained and aware and willing to identify and report such items to supervisors/managers and supervisors/managers know how to action such a report. Staff monitoring CCTV/IPTV systems can also identify and report such items. The public of countries that have suffered from sustained bombing campaigns such as the UK, Spain and Sri Lanka are quick to report unattended items.

The likelihood of finding lost, misplaced, concealed and other unattended items on site is higher than that of finding something that appears to be a bomb. The origin of the item may be confirmed through a review of CCTV/IPTV, access control records, interviewing staff and others, asking for the owner to return, etc. While due care must be taken not to mishandle something that might be hazardous it may be possible to look inside the item (see "Examples" at the end of this Chapter).

Some sites, assessed as being at high risk e.g. international airports, have portable x-ray systems to assist with investigating unattended items, for most organisations this will not be a cost effective capability.

The consequences of failing to respond appropriately to an unidentified item can be considerable. If the process is mismanaged two primary consequences are probable:

- failing to evacuate when there is a real hazard; and,
- unnecessary evacuation and disruption when a simple investigation would have shown that there was no hazard.

The consequences of finding an unidentified item can be mitigated if processes are in place to identify how the item got there, what it contains and if it poses a hazard.

The response procedures for unattended items should include what will be done with the item if it is not hazardous e.g. passed to the lost property office, disposed of, returned to owner, etc.

If there is any suggestion that the item poses a hazard then the risk alters to that of having a bomb on site and the pre-planned procedures implemented.

3.3. Risks Relating to Bomb Threats

An offender need spend little time or other resources in making a bomb threat, or other threat, against an organisation. The organisation has little ability to prevent a threat being made by 'phone, e-mail, SMS, mail, fax or other communication systems. The ability to recognise, evaluate and respond to a threat lies within the capability of all organisations regardless of size or function.

The initial, instinctive reaction whenever a threat is received may be to evacuate although this may not be the safest or most sensible action and does not reflect security risk management principles. Constant evacuation will undermine the employees', clients' and owners' confidence in management's ability to provide a safe, secure and productive work environment. Constant evacuation will also lead to "copy-cat" incidents as staff seek time off work or outsiders enjoy the prospect of disrupting activities. The offender may also learn that the organisation reacts and capitalise on that behaviour. At the other extreme some organisations have an (unofficial) policy of not responding to threats as "they are always hoaxes"; this approach is both negligent and dangerous.

The risks relating to bomb threats (and also for other types of threats against the organisation) could be defined in terms of:

- Failure to respond appropriately to a bomb threat …"

The appropriate response is based on the ability to capture the information about the threat and analyse it. The question is not "is the threat real?" as the threat has been received and is a real threat, the question can be reworded as "is it feasible for the offender to have done that which they claim?". This is a question that the security risk manager, in conjunction with the Security Committee or Emergency Control Committee, should be able to answer based on their knowledge of the site's security and procedures.

For some organisations the number of bomb threats peak at certain times such as in educational institutions where they tend to be more common at exam time than during holidays. Some industry sectors such as the aviation industry receive many threats in a year and deal with them on an almost routine basis. Other organisations are rarely, if ever, threatened, it is these that are at greater risk of failing to evaluate and respond in the safest and most appropriate manner.

The effectiveness of the response to a threat will depend on the organisation's ability to:

- recognise they have been threatened;
- capture and report the information about the threat to the relevant authority within the organization;
- evaluate the threat; and,
- respond appropriately.

Threat evaluation is a management decision and is not a simple matter. It requires procedures, pre-planning, training and rehearsal. It is important that all employees know how to accurately record the wording of any threatening call or to pass on a threatening e-mail or other message. In relation to the evaluation, this is often presented in terms of "specific" or "non-specific"[13] which is a method of indicating the amount of knowledge (and commitment) the offender has when making the threat. If the offender has gone to the effort and personal exposure of making and deploying a bomb and then wants to warn the organisation[14] then it is probable that the offender will provide information that will assist the organisation to evaluate and respond to the threat[15]. Someone with little commitment or knowledge of the site can be expected to provide little specific information about the location, motive or design of the bomb. If someone with knowledge of the site makes a detailed threat then it will be given more credibility as it represents knowledge that may have been gained as the bomb was placed.

As well as reviewing the wording of the threat there are a number of other sources of information that will help the evaluators assess the feasibility that the offender has done that which they claim these can include:

- review of CCTV/IPTV records;
- review of access control records;
- interviews with staff and others; and,
- search of areas, ranging from employee scans of their work areas to formal searches of nominated areas.

If it is determined that the threat is not credible then work may continue, but procedures should be in place to record the evaluation and the basis for the decision and to inform all those that are aware of the threat, of the decision.

If it is believed that the bomb threat is credible, in that the offender may have done that which they claim, then the emergency procedure for responding to a bomb should be implemented. If time permits, a search of the area can be conducted on the basis that if the item is found the bomb squad can be deployed with the aim of rendering the item

13 Refer to the additional sources at the end of this section.

14 It may be that the offender wishes to damage property but not to kill, perhaps there has been a change of heart, possibly there is no bomb and the aim is disruption, panic and a sense of self-gratification by the threat maker.

15 Information provided to the author by various organisations including tapes of actual threats.

safe prior to its exploding and damaging the assets. Again there is a need to record the evaluation and the basis for the decision.

The consequences of failing to respond appropriately will vary from failing to evacuate when there is a real hazard to unnecessary evacuation and disruption when evaluation of the threat may have shown that an evacuation was not necessary.

How the organisation handles bomb and other threats will be reflected in the confidence of staff, clients, owners and the public in the ability of management to deal with such risks while protecting people and productivity.

Remember the bomb threat can only be classified as a hoax after it has been assessed.

3.4. Risks Relating to Mail Bombs

The mail and courier systems offer a degree of anonymity to the offender and the ability to deliver the bomb (or other hazardous material) directly to the targeted individual.

The initiative for constructing and sending a mail bomb rests with the offender and the organisation can do little to modify this. Therefore the risks relating to mail bombs may be defined in a similar manner to other bomb incidents:

- "Failure to identify a mail bomb …"
- "Failure to respond appropriately to a mail bomb …"
- "Failure to prevent a mail bomb from entering the workplace …". (If the mail is received and sorted within the work place this is a difficult risk to manage.)

The likelihood of failing to identify a mail bomb is directly related to the training and awareness of all staff who receive and open mail. Some guidance is provided in AS3745[16] and mail bomb recognition posters and information are provided by the Australian Bomb Data Centre and others. In all cases the guidance needs to be applied to the particular operating environment of the organisation.

The consequences of failing to identify a mail bomb will include injury and possibly death of the person who opens the mail.

The ability to respond appropriately to a mail bomb is dependent upon considered, appropriate procedures relevant to the operating environment of the organisation. The procedures should cover:

- reporting of the suspected mail bomb;
- investigation as to why is it considered suspicious;

16 Australian Standard 3745-2002 "Emergency Control Organisations".

- determining if it is considered hazardous or safe to open;
- if it is considered hazardous, isolation measures appropriate to the site; and,
- evacuation considerations for some or all of the site.

The investigation into the items can include:

- comparing the item to the mail bomb recognition posters and similar guidance;
- asking the recipient if they are expecting the item; and,
- checking information on the sender, if any.

If the item has come through the postal system there should be time to investigate it as it is highly unlikely to have a timed triggering mechanism, rather mail bombs rely on the act of opening the item to it to function (i.e. to explode, ignite, release chemical, biological or other material, or to expose sharps).

If an item is considered hazardous it must not be opened, it should be placed on a flat clear surface, possibly in a pre-selected isolation point, and the area evacuated.

Similar risk considerations can be applied to courier-delivered items with the difference that courier-delivered items could contain a timed triggering mechanism and therefore if a couriered item is suspected of being a bomb an immediate evacuation of the area should be initiated.

3.5. Risks Relating to Post-blast

If a bomb is not detected, despite the best plans and measures, and there is an explosion the risk of a “post blast” situation should be considered. A post-blast plan is usually considered part of the consequence management treatments, but it can be defined as a separate risk in terms of:

- “failure to respond appropriately to a post-blast situation …”

As an explosion is one reason why an organisation my lose access to its site, information or people, the post-blast plan must be aligned with the business continuity and business resumption plans. A post-blast consequence management plan will address the following:

- The main consideration will be a staff support function in that a bombing is a deliberate human act of violence and the psychological and societal effects on the staff and others may be considerable.
- If there are casualties the organisation’s HR support plans will be required.
- The scene of the explosion will be a complex crime scene and may be isolated by the investigating authorities for a considerable period of time.
- Urgent structural assessments of the building may be required.

- The ability to obtain repair services, parts and equipment maybe restricted, particularly if the explosion affected a number of buildings in the area.
- Insurance may not cover the bomb damage depending on the exclusion clauses in the policy, in which case other means of funding repairs and replacements may be needed.
- Legal protection from litigation or claims of negligence may be required. A demonstrated adherence to bomb incident security risk management practices may assist with a legal defence.

It may be that the bomb was not targeted at the organisation and that the organisation suffered “collateral damage”. If the incident is external the organisation should have a “Hold in Place” plan so that people can remain where they are until the nature of the hazard is identified and the most appropriate egress route and time for an evacuation can be determined.

Similar consideration to those above can also be used for planning consequence management for accidental explosions due to industrial accident etc.

4. MITIGATION STRATEGIES

The management of risks associated with bomb threats is a highly specialised field with new technologies, tools and systems being constantly developed. As such, it is worth stating unequivocally that specialist advice although important in all areas of security risk management is essential in the field of bomb mitigation. What follows is provided as merely an insight into the types of risk frameworks and strategies that a manager or security professional might choose to consider when called upon to mitigate risks associated with explosives.

As with any other type of risk the mitigation of explosives incidents should include a layered approach to security-in-depth. It will require a holistic understanding of the threats and risks as well as a concerted application of the Knowledge Areas and Practice Areas outlined in SRMBOK.

These are detailed in SRMBOK, however in summary these include:

- Exposure and threat assessment;
- Risk assessment and management;
- Allocation and application of resources;
- Quality assurance and management;
- Integration with organisational vision, mission, values and business systems;
- Functional design of barriers and systems;
- Application and implementation of security treatments such as blast treatments, training; and,
- Ongoing audit and assurance activities.

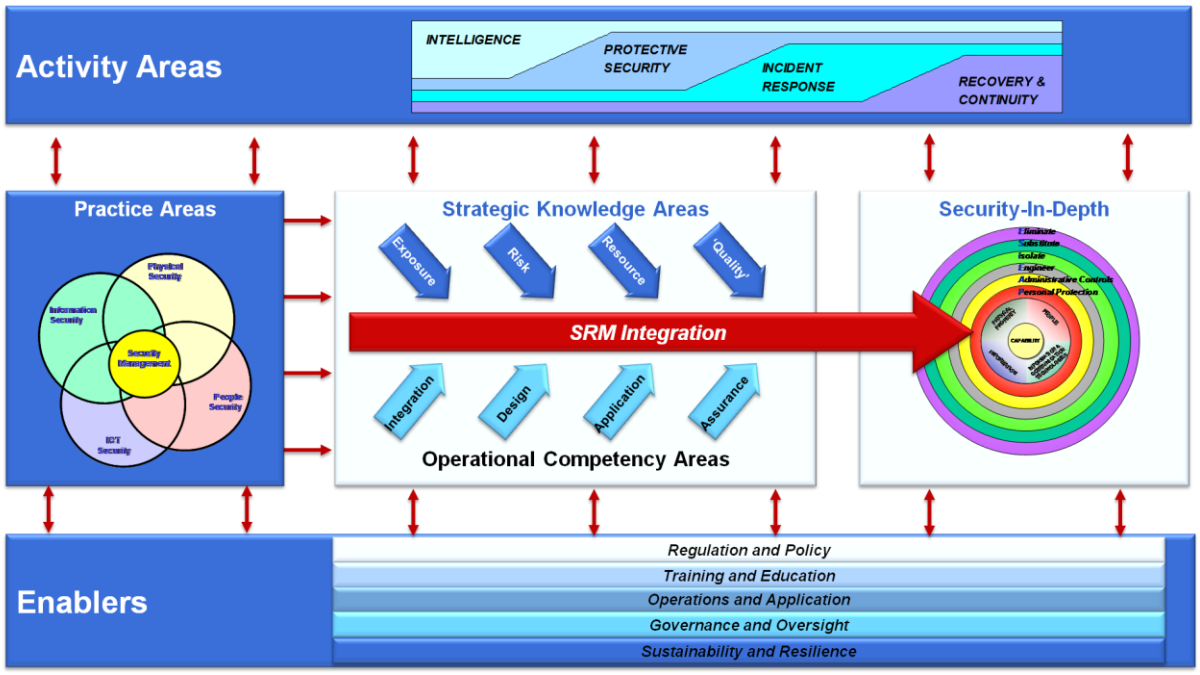

Figure 1: SRMBOK Organisational Resilience Model

The combined interaction of elements illustrated in Figure 1 is one view of how organizations and communities implement security-in-depth to achieve resilience.

An understanding of the Swiss Cheese approach to likelihood and consequence management outlined in the Bow-Tie Model (Figure 2) becomes particularly important when dealing with bomb incidents. In many (but certainly not all) cases there may be little ability to modify the likelihood of a bomb incident and consequence management may be the critical factor. For example, if you are operating a petro-chemical facility in an urban area, there is little (although certainly not nothing) that you can do to prevent an attack with improvised mortars. There is a lot that can be done however post-event. This might include emergency evacuation systems, fire/explosion proof shelters throughout the plant, first aid facilities, fire-fighting, alternative supplier arrangements etc.

The use of Bow Tie analysis is a field of study in its own right which is discussed further in the SRMBOK Guide to Security Risk Assessment and Management. The significance however, of the 'Bow Tie' model is that it allows managers and security professionals to have a discussion within a structured framework regarding options, roles and responsibilities for a given situation.

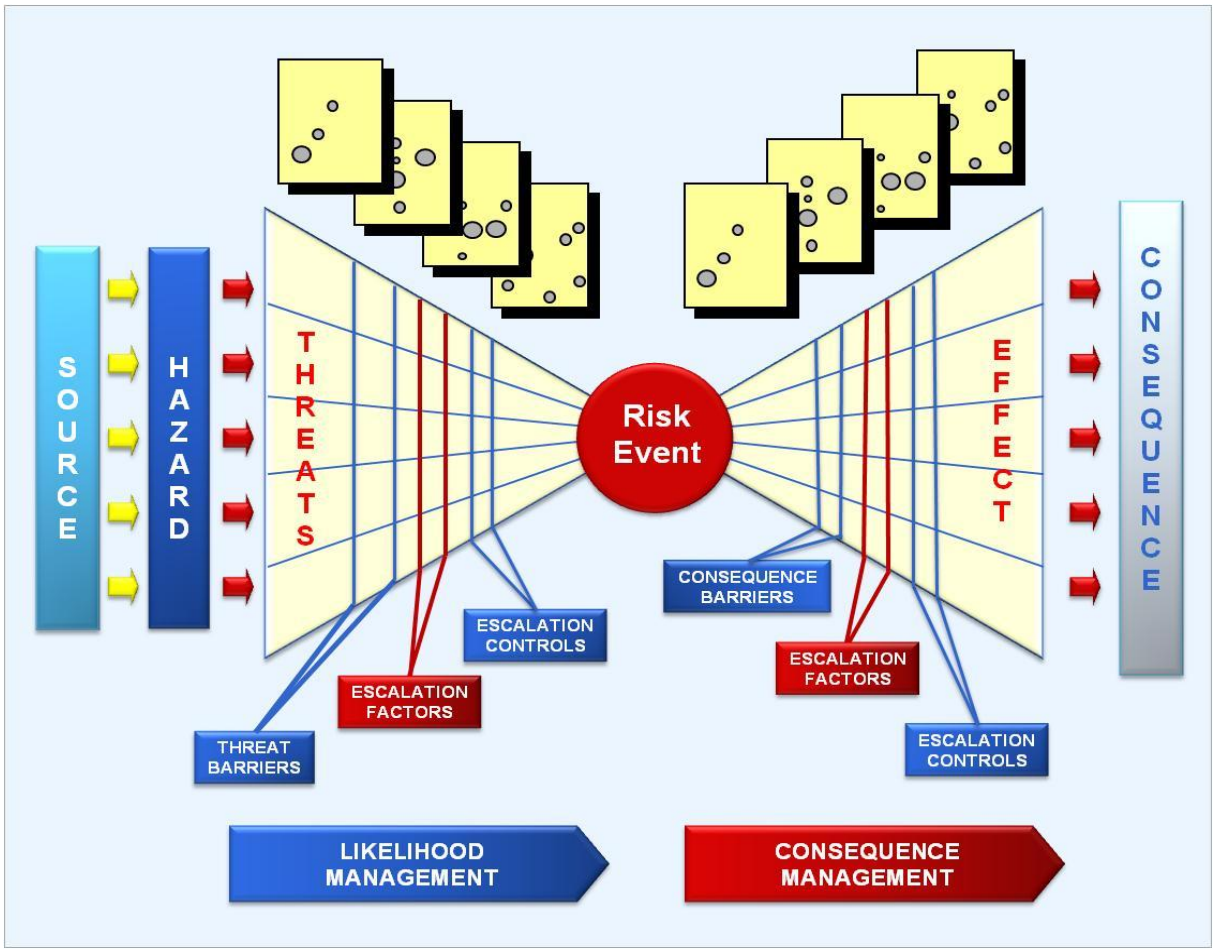

Figure 2: Bow-Tie Likelihood and Consequence Model

It is also useful to understand the concept of escalation factors in terms of how they might impact on existing barriers. A simple example might be the use of blast curtains inside an office[17]. This 'consequence barrier' (Ref: Figure 2) could well be partially or fully negated if for example, the organisation has an escalation factors such as high staff turnover combined with inadequate security training. Thus the blast curtains can be rendered ineffective if the occupants do not use them correctly by pulling them away from the glazing or by moving workstations closer to the windows. In this example, the Escalation Controls might include signage and relevant staff induction training.

Similarly a hierarchy of controls system can provide assistance when arguing the merits of investments in blast treatments. The 'hierarchy of control' categorises control measures in priority order that can be used to select and manage risk exposures. Hierarchy of controls (also referred to by the mnemonic 'ESIEAP') is described in more detail in SRMBOK. The key elements of ESIEAP are:

17 Blast curtains are lightweight see-through curtains attached inside the window and are designed to remain in a closed position at all times to catch the glass fragments produced by a blast wave. They do not eliminate the possibility of glass fragments penetrating the interior of the occupied space, but limits the travel distance of the airborne debris therefore it is essential to keep desks and workstations a slight distance from the curtains.

- **Elimination:** complete removal of the threat, or risk exposure is the ideal control solution where this is practical.
- **Substitution**: involves replacing a hazardous substance, machinery or work process with a non- hazardous or less hazardous one.
- **Isolation:** involves separation of the risk from people by distance or the use of barriers.
- **Engineering controls**: may include modification of tools and equipment, using enclosures, barriers or automation.
- **Administrative Controls:** where a risk cannot be eliminated or controlled by engineering, administrative controls should be used. Administrative controls mean introducing work practices or procedures that reduce risk.
- **Protect the Asset:** as a last resort, where other measures are not practicable it may be necessary to use measures such as Personal Protective Equipment (PPE) such as ballistic body armour or items such as secure briefcases as a last line of defence for sensitive documents in transit.

An example of ESIEAP applied for a bomb risk mitigation for an international bank is provided in Figure 3.

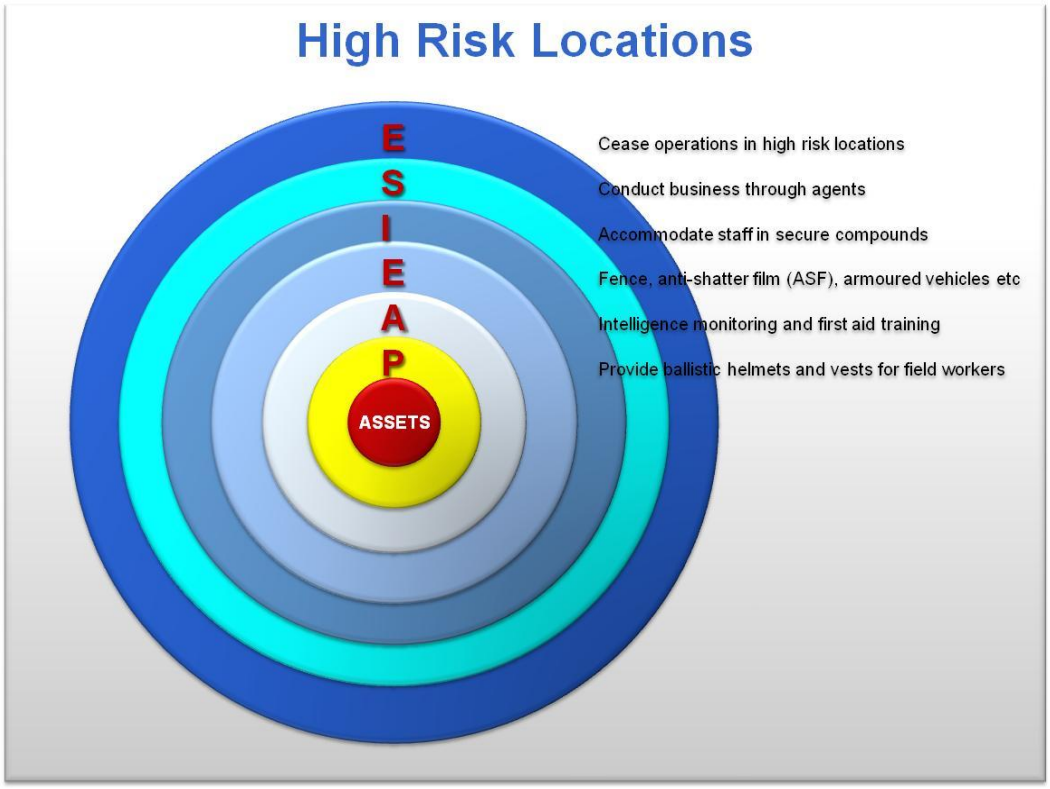

Figure 3: ESIEAP Example for Operations in High Risk Locations

A layered approach to mitigation strategies will offer the best approach. In the following example, the bank may take all or just some of the recommended treatments. Some

countries may be highly dangerous and with insufficient reward to justify retaining a presence. In these locations it may be possible to completely cease business operations. In most high risk locations, it may be possible to use tele-conferencing and local agents who are at lower risk because they are not visibly identified within the target group (eg: as a foreign multi-national organisation). Where it is justified in having a presence but still relatively high risk, perhaps all of the remaining treatments may be adopted.

The approaches outlined above (Bow Tie, ESIEAP, AS/NZS4360, etc) are equally applicable to a school facing bomb hoaxes as to a small business located adjacent to a high profile potential bombing target. The key is to use them in context and ensure that there is some sort of consistent framework to frame discussions and decisions taken.

4.1. Cost of Bomb Risk Mitigation

The cost benefit calculation regarding bomb risk mitigation is something that each organisation will need to decide within their decision making frameworks to reflect risk appetite, et cetera.

It should be noted however that the cost of retrofitting[18] an existing building will in all cases be greater than the cost of including blast mitigation strategies.

18 'Retrofitting Existing Buildings to Resist Explosive Threats' by Robert Smilowitz at http://www.wbdg.org/design/retro_rstexplo.php has some additional US Government and private sector links as well as general commentary on the available options for retrofitting buildings.

5. CONCLUSION

The various types of bomb incidents can be analysed and mitigated using security risk management principles. Knowledge of the motives behind the use of bombs and bomb threats, the effects of explosives, the existing security environment, including the training and awareness of staff, is required to accurately assess and treat bomb incident risks.

The information provided in this guide is by no means a substitute for expert advice however it should assist even non-experts with the engagement of expert advice and support a sound dialogue to apply risk assessment and management systems to this issue.

The threat of bomb incidents in their many guises can often seem overwhelming to even the security risk professional if they are not experienced in this field. It is important to note however that the principles of risk management remain the same. Using sound methodologies to manage the 'risk' rather than the 'threat' will provide a clear basis for decision making to support the allocation of resources in mitigating bomb incident risks.

6. ADDITIONAL READING

Additional sources of information include:

- Australian Bomb Data Centre http://www.afp.gov.au/services/operational/abdc/
- MI5 Security Advice Bomb Protection http://www.mi5.gov.uk/output/Page37.html
- US Bureau of Alcohol, Tobacco, Firearms and Explosives http://www.atf.treas.gov/pub/threat/index.htm
- Indian Bomb Data Centre http://mha.nic.in/nbdc1.htm#dos
- US Federal Emergency Management Agency, (2003), Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (FEMA426), United States Department of Homeland Security, Washington (available for download from http://www.fema.gov/plan/prevent/rms/rmsp426)
- US Government Technical Support Working Group (TSWG) http://www.tswg.gov/index.html

7. EXAMPLES

The following are based on real-life incidents and are offered as examples of bomb incident risk management.

Unattended Item:

At an international airport an unattended bag was found on the secure side (airside) of the passenger screening point. The bag was a shopping bag with the name of one of the clothing and accessory retailers located in the airside concourse. The security supervisor approached the bag and without touching it looked inside and identified a brand new red handbag. He picked up the bag and took it to the retailer to see if they could help identify who purchased it so the owner could be paged or tracked to a flight.

Comment:

Traditional wisdom might suggest that the supervisor should not have touched the bag and should have initiated an evacuation until the owner of the item could be identified. In the incident described, the supervisor made the sound assessment that the item was most probably an item of shopping left behind by a traveller or visitor; there were no indicators to suggest the item posed a hazard. Initiating even a partial evacuation would have disrupted the operations of the airport and airlines. If the supervisor was concerned about moving the item before it had been investigated alternatives might have included: posting a guard near the item while the CCTV footage was reviewed or a staff member from the shop be asked to attend and identify the hand bag as a stock item they sold.

Unattended Item:

At an international airport an unattended briefcase was found in a public area. A call for the owner was made over the public address system. Concurrently an investigative team arrived and x-rayed the item and identified batteries and other items they declared the item “suspicious” and requested the bomb squad attend. A complete evacuation of the area was initiated. During the evacuation a man approached airport staff, claimed ownership of the item and was able to describe it and its contents (which were not hazardous). The man was refused access to the area until the item had been “rendered-safe” by the bomb squad. The period of disruption to the airport and airlines was hours.

Comment:

The risk of the item being hazardous should have been reassessed when the owner made himself known. Once the owner was identified he should have been allowed to claim the item. If the investigating team were concerned they could have checked his details against any name tags or

other marking on the briefcase or questioned him further on the contents. The response process had gained an impetus that was hard to stop.

Bomb Threat:

A manager acting in a senior executive position for a major company received a bomb threat on a private (unlisted) office number. The threat contained specific in-house information and the threat was credible. The company had effective, documented and practiced bomb threat procedures. The manager was not aware of the company procedures and proceeded to apply management analysis techniques to the problem, this resulted in a 15 minute delay before security was informed of the threat and the existing threat assessment procedures were implemented.

Comment:

The ability to respond effectively to the threat was reduced because the manager was not aware of the procedures. There was a company bomb threat card in his desk but he either had not been trained in its existence and use or had ignored the training. The delay may have endangered the lives of staff and visitors and the organisation's operations.

Bomb:

At a hotel, during a major international event, a guest heard a strange beeping noise coming from a rubbish bin. He informed a policeman who approached the bin and recognised the distinctive sound of a low battery alert from a smoke detector (as used in the host country). He searched through the bin found the smoke detector and removed the battery. It is surmised that one of the guests being annoyed by the sound removed the smoke detector from his room and put it in the rubbish.

Comment:

The knowledge and experience of the policeman allowed him to respond appropriately to this incident by identifying the item as non-hazardous. Someone without the same experience may have decided on a different course of action. If the policeman had found a bomb or other item in the rubbish bin then he would have recognised it as hazardous and initiated an evacuation.

Bomb:

At a major public event a member of the public raised the lid of a rubbish bin and saw a brand new sports bag. She identified it as being unusual and not fitting the environment. She notified a policeman who immediately initiated an evacuation away from the bin. A bomb squad which was on stand by at the event investigated and found the bag was torn and empty.

It is surmised that a member of the public had discarded the torn bag.

Comment:

In this case evacuation was appropriate as a new bag is not expected in the rubbish. The likelihood of identifying a potentially hazardous item was increased due to an aware member of the public. The prompt response was possible because: planning for the event had foreseen such an incident; the event was of a nature that could be vulnerable to bomb incidents; and the consequences were assessed as being high enough that a bomb squad was on location to reduce the likelihood of an identified bomb detonating.

Bomb Threat:

In September 2005, over 1000 Iraqis were killed in one incident while on a pilgrimage to the Kadhimiya mosque. They died in a crowd crush which was caused by a rumour of a suicide bomber in the crowd. This is a larger number than may have been killed by a bomb exploding.

Comment:

The rumour was believed because many thought it possible that a suicide bomber could have joined the procession. How the likelihood of a bomber joining the crowd or how the consequences could have been mitigated if the bomber was identified makes an interesting and challenging risk analysis exercise.

Mail Bomb:

During a mail bomb campaign a senior staff member in the targeted industry received a package which was incorrectly addressed and which he did not recognise. As he left the office he jokingly said to his secretary “I will open this outside in case it is a bomb”. He was subsequently killed while opening the parcel as the device proved to be a bomb.

Comment:

It appears the senior staff member was aware that his industry was the target of a mail bomb campaign. While it is possible he identified the item as potentially hazardous, at least sub-consciously, the risk of “failing to respond appropriately to a mail bomb ….” was realised with dire consequences. Once an item is believed to be hazardous staff must know how to implement the appropriate response measures, even if it is only to notify security manager, etc.

Post Blast:

An embassy was the target for a bomb which, because of the security risk assessment and subsequent security measures, exploded outside the fence-line. Although the embassy had an effective “hold in place” procedure the staff were immediately evacuated outside in accordance with the fire drill procedures.

Comment:

All the staff inside the embassy survived the initial blast. By sending them outside they were exposed to hazards resulting from the initial explosion and possibly from other bombs. Although appropriate response procedures for external incidents had been developed it appears that staff, in particular the emergency management organisation, were not aware of these procedures and the consequence mitigation treatments were ignored.

Bomb Threat:

During the build up for the closing ceremony for the 2000 Sydney Olympic Games a threat was received stating that explosives had been placed on the Harbour Bridge and that the closing ceremony should be cancelled. The threat (one of many during the Games) was assessed in accordance with the processes that had been developed. In addition to the heightened security, there were considerable quantities of pyrotechnics mounted to the bridge and all explosives, firing systems and other areas had been carefully checked and rechecked by a number of contractors and agencies.

Comment:

Because of the physical and procedural risk mitigation treatments in place the assessors were able to determine that the likelihood of the perpetrator having done what they claimed was extremely low. As a result there was no requirement to disrupt the event. If required the threat assessment team had additional risk assessment measures available including: reviewing access control systems, reviewing CCTV and sending out search teams trained for that particular environment.

Bomb:

The bombing of the United States military accommodation building at Kohbar towers in Saudi Arabia on the evening of 25 June 1998 was limited in its effect because of the risk management measures put in place. The bomb is estimated to have contained approximately 10 tonnes of explosives. The size of the bomb was a response to the access control measures that denied the offenders the opportunity to get close to the building. There were guards on patrol with visibility of the perimeter; one

noticed the tanker truck and determined that it was out of place and potentially posed a hazard. An evacuation was immediately initiated. 19 service personnel died, but casualties could have been much greater.

Comment:

Without the ability to detect and respond to the bomb the casualties would have been considerably higher, possibly grater than the bombing of the Beirut Marine barracks in September 1983 when 241 service personnel died.

Bomb Threat:

A government storage and logistics facility received a bomb threat at lunchtime every Friday. The management response was to allow all staff to leave the site with their vehicles and close the site until the following Monday. The site lost a half day's productivity every week. When advice was sought, the staff were concerned that their safety could be jeopardised if they were not evacuated. One Friday, after the threat was received all staff were evacuated and assembled in the car park, which had been searched. The entire site was then searched by specialists; this took until late evening at which time it was determined that it was safe for the staff to leave.

Comment:

Initially no threat evaluation was conducted. The risk was assessed as disruption to operations due to poor response to a bomb threat. A bomb threat process was introduced and a method of moving the consequences of the threats to the staff (and probably the offender) was identified. No further bomb threats were received.

Bomb Threat:

A university always received bomb threats when exams were being held. Initially the response was to evacuate the building under threat. The consequences included significant disruption to students and staff, having to reschedule exams, having to rewrite or have prepared alternative exams, alternations to students travel plans periods (including overseas students). Subsequently a bomb threat assessment process was introduced; the exam rooms and surrounds were searched prior to the exams; bags and other items were not permitted in or near the exam rooms making searches by security staff in response to threats quick and simple.

Comment:

As a result of the ability to assess the risk posed by a threat it was determined that it was unlikely that an offender could have done that which they claimed. Thereafter it was rare that an evacuation was called and the threats stopped as the desired results (evacuation and disruption)

were not forthcoming.

Bomb:

During a major international event with large public crowds it was proposed that all rubbish bins should be removed to prevent bombs being hidden in them.

Comment:

A thorough risk review was conducted and the risk of a bomb being concealed in a bin was assessed for its likelihood and consequences given that operating environment. The risk was then expanded to include all locations where a bomb could be concealed including street furniture, gardens, etc and whether these should also be removed. As there was already a high level of overt and covert observation of the area, frequent searches of the site and pre-planned response options these were included in the threat evaluation. A risk analysis was also conducted into the consequences of removing the bins; risks relating to infection, infestation, trip hazards, damage to the environmental image of the event, litigation, etc were identified. As a result it was decided that removing the bins increased other risks to unacceptable levels. Instead of removing the bins, they were emptied more often, the visible security presence in the area was increased, and alternate styles of bins were used in “high risk” areas. It should be noted that by decreasing one risk other risks may be generated or altered.