From the BRMA Committee on Terrorism:

# Bomb Incident Management

**Eugene Tucker, CPP, CFE**

February 2002

The days since September 11 has shown us that terrorists are capable of using 'non-conventional' means to carry out their objectives. Although many experts believe that terrorists have not yet solved the technical and logistical difficulties to 'effectively' launch such weapons, others believe that even their failures can cause unacceptable losses. In spite of the difficulties they need to get lucky just once. The very real threat of the use of weapons of mass destruction has caused many in our government to use our resources in ways that return little value. In our rush to protect against these 'new' forms of attack, we have lost our focus and have not done a better job of either mitigating or preparing for the conventional-the simple, tried and true tool of both domestic and international terrorism: bombings.

One of the aims of terrorist groups is to cause severe damage to our economy and infrastructure. The FBI is concerned that oil refineries, business with hazardous materials, or other operations that could cause collateral or synergistic damage are prime targets. Although all of our domestic bombings are rather small scale (with a few, very notable exceptions), we can expect the devices they use to greatly increase in size.

As continuity planners, what can we do to protect ourselves and help our businesses recover? From the recovery view, there is not much, if any, that we would do differently after a bombing except for an understanding that the area may be considered a crime scene and that public perception and employee fear may leave a lasting effect. This is assuming that you have done worst-case scenario planning that assumes the complete loss of the target location. We can, however, have a very direct effect in the prevention of losses from bombings or more commonly, from bomb threats.

## Brief Scope of the Problem

Throughout history and throughout the world, bombings are a prime tool used by terrorists. In 1996 there were 1,685 bombings and attempted bombings in the Untied States that caused $2,260,362 in damage and 24 fatalities. In the same year, incendiary incidents totaled 533 and $7,058,368 in damage. 7 people died from these firebombs. Between 1993 and 1997, bombing and incendiary incidents totaled 13,560, killed 478, and caused $645,947,792 in damage. Letter bombs, depending on the year examined, typically represent less than one percent of the above totals.

The Alcohol, Tobacco, and Firearms (ATF) reports that in 1996, 2,983 pounds and between 1992 –1996 27,562 pounds of high explosives were stolen. Interestingly, they report that 27,562 pounds (1996) and 93,278 pounds (1992-1996) were recovered. California consistently ranks as one of the top three states with stolen explosives and leads the other states in the number of bombings.

Vandalism consistently leads as the motivation of bombers (mailboxes are a common target), followed by revenge (sour love affairs, ex-employees, and 'messages' to our beloved Internal Revenue Service, for example). Homicide, suicide, protest, extortion / insurance fraud and labor disputes are near the bottom of the list.

The Oklahoma City bombing consisted of a 4,800-pound ammonium nitrate/fuel oil mixture that generated a blast pressure of almost 6,000 pounds per square inch, created a 30-foot wide, 8 foot deep hole, and the winds spawned to replace the vacuum caused by the explosion exceeded 1000 times hurricane force. Windows were blown out 1,000 feet away. Even in a small-scale explosion, structural damage is possible. Non-structural damage can include: fire and smoke damage, water damage, soot and dust, glass and debris. Electronic equipment and circuit boards can be damaged from the blast, and the psychological effects can be significant. A bombing or the discovery of a devise can put the firm on legal 'notice' that such incidents are foreseeable and thus increase future liability.

**Prevention**

Is it possible to prevent bombings? Yes. The difficulty in carrying out an operation and the increased chance of intervention or capture has made even international terrorists (Ramzi Yousef, for example) to change their targets and plans. Although the government shares a large responsibility in developing and implementing regulations and oversight in the control of explosives and materials used to make explosives; security, risk managers and business continuity planners can directly affect the exposure of their facilities. The level of physical security, and the degree in which it is enforced, is a primary consideration when it comes time to evaluate the credibility of, and the response to a bomb threat.

- Good physical security is an effective step in preventing bombings. Glare lighting, clear zones and good natural surveillance of the site and facilities, fences, high visibility security officers and alarm systems are basic elements to consider. If the site is at a high risk, structural design and mitigation to strengthen the buildings and make them more resistant to blast effects can be employed. Moving roadways and parking lots away from the facility or critical infrastructure may become part of the plan. See the BRMA Reporter article on Physical Security in the October 2000 issue for more information. If there is no in-house expertise, select a security consultant who is a Certified Protection Professional (CPP) to complete a physical security survey.

- Access Control is another important element. Develop a method to allow entry into the building to only those who have business inside. This can be achieved through restricting the number of entrances and exits to the absolute minimum, checking in and escorting visitors, issuing employee badges, and using cameras and other access control devices. Pre-employment background investigations and the identification and clearance of vendors and contractors prior to admission to the site should also be considered for high-risk operations.

- The incoming inspection of packages, purses and briefcases, while seemingly a draconian measure in most cases, may be routine in high-risk facilities. Companies that produce materials that can be used to construct bombs or add a synergistic effect to a devise, should develop internal controls to prevent and identify the sale of these materials to illicit sources. Likewise, companies that buy and use these materials in their production should take steps to prevent their theft.

- An intelligence program that tracks the people and activities of certain groups that may pose a threat can be an invaluable tool. Some antiabortion, environmental, animal rights, and militia extremists are known to use explosives and incendiary devices. Often members of these groups can be identified casing the facility or attempting entry beforehand. Observe for suspicious activity and train employees to report suspicious unattended vehicles. A close liaison with local law enforcement may assist in these efforts.

- Finally, develop a policy and capability to fully investigate and prosecute all threats. Any overt action by management to identify the perpetrator will have a powerful deterrent effect if the threats are generated internally.

**Threat Evaluation**

Threats can be emailed, snail mailed, or most commonly, telephoned into the business. It is important to remember that the great majority of telephoned threats are hoaxes. Only 2 – 6 percent or less of bombings are preceded by a threat or warning. There is some variation in these numbers but some experts put the probability at 0.5% (1 in 200 chance), while others such as the San Jose Police bomb squad put the odds at 'infinitesimal.' I have responded to two actual explosive bombings, two incendiary incidents, and one attempted arson case using an incendiary device. There was no prior warning in any of these cases. I have received and evaluated countless threats while failing to ever find a device.

Generally, the purpose of a valid threat is to prevent injury or to prove intent in an extortion case. In these cases, familiarity of the site and the increased detail provided by the caller adds credibility. The caller may provide the exact location, time of detonation, and a detailed description of the explosive. Although 'Bomb Threat Checklists' are found at may reception stations, it is important for someone in your organization to develop the capability to evaluate the credibility of any threats received. This capability can reside with the security director, risk manager, crisis management team, or other responsible person who can be reached quickly and has the ability to make rapid decisions. The great majority of police officers and police dispatchers are not trained to evaluate threats. Many are restricted by policy to not offer advice to the business owner. The person or persons who evaluate the threat must have some training in threat evaluation that includes an understanding of the firm's threat risk profile. Basic components of the profile are:

- Level of security (see above);
- Evaluation of the visibility of the company or controversial business activity;
- Recent events (product recall, pending labor actions, reduction in force);

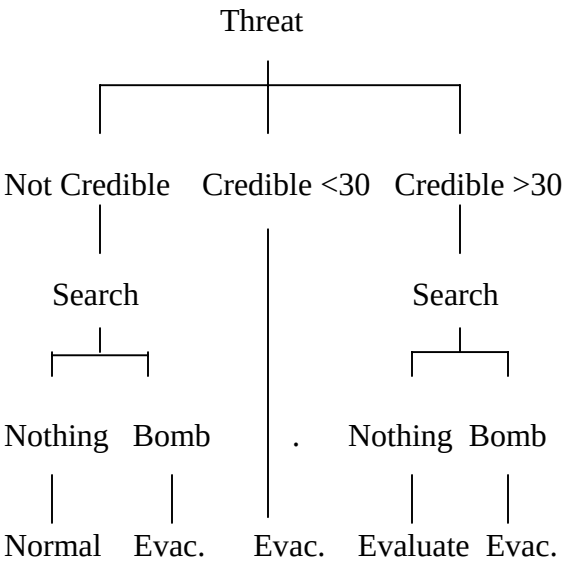
- History of bombings and threats;
- Activity of individuals and groups (intelligence).

The wording of the thereat is examined for key words ('device' as opposed to 'bomb,' terms that describe the firing train, etc.), conditions and circumstances (background noise of a party –low credibility or day in history that is significant to a suspect group – higher credibility), detail of the threat, ability to carry out the threat (security level and profile), and motivation. The results of the evaluation will guide the decision to evacuate, shelter in place, close the business, or other action as appropriate.

**Evacuation**

The decision to evacuate the building or site after a bomb threat is still a controversial and difficult action although many security managers now follow the philosophy of avoiding evacuations unless a devise is actually found. There is good reason for this approach: since most threats are false, evacuation will cause needless loss of productivity, decrease employee morale, increase the possibility of injury from the evacuation, and most often, satisfy the intent of the caller. Once a threat had been communicated to employees through an evacuation, expect additional threats generated internally. Most bombs in business settings are placed in the parking lot, building perimeter, or 'public' areas such as the lobby, hallway, and lockers. Evacuating employees will send them though and to these areas.

Consider the following guide when deciding to evacuate:




| ATF | VEHICLE DESCRIPTION | MAXIMUM EXPLOSIVES CAPACITY | LETHAL AIR BLAST RANGE | MINIMUM EVACUATION DISTANCE | FALLING GLASS HAZARD |
|---|---|---|---|---|---|
| | COMPACT SEDAN | 500 Pounds 227 Kilos *(In Trunk)* | 100 Feet 30 Meters | 1,500 Feet 457 Meters | 1,250 Feet 381 Meters |
| | FULL SIZE SEDAN | 1,000 Pounds 455 Kilos *(In Trunk)* | 125 Feet 38 Meters | 1,750 Feet 534 Meters | 1,750 Feet 534 Meters |
| | PASSENGER VAN OR CARGO VAN | 4,000 Pounds 1,818 Kilos | 200 Feet 61 Meters | 2,750 Feet 838 Meters | 2,750 Feet 838 Meters |
| | SMALL BOX VAN *(14 FT BOX)* | 10,000 Pounds 4,545 Kilos | 300 Feet 91 Meters | 3,750 Feet 1,143 Meters | 3,750 Feet 1,143 Meters |
| | BOX VAN OR WATER/FUEL TRUCK | 30,000 Pounds 13,636 Kilos | 450 Feet 137 Meters | 6,500 Feet 1,982 Meters | 6,500 Feet 1,982 Meters |
| | SEMI-TRAILER | 60,000 Pounds 27,273 Kilos | 600 Feet 183 Meters | 7,000 Feet 2,134 Meters | 7,000 Feet 2,134 Meters |

If the threat is not credible, begin a search. If nothing is found, return to normal operations. If a device is found, evacuate a safe distance away from blast effects or send employees home. If the threat is credible and a detonation time of less than 30 minutes is given, you may want to delay the search and evacuate if the employees can be cleared from the building and placed in a safe location before detonation. If the threat is credible and a detonation time is greater than 30

minutes, initiate a search if it can be completed in time to safely evacuate after the search is completed. These times are somewhat arbitrary and should be adjusted according to your circumstances. This criterion applies only to threats received in the United States. The characteristics of threats and groups overseas may require a different approach.

**Search**

Although you should rarely evacuate after a threat is received, you should almost always begin a search for a bomb, even if the threat is obviously a hoax. Searches should be conducted internally as most police officers are not trained in search methods or are not allowed to conduct a search of your premises. Calling the police to report a threat or to conduct a search will often result in the incident becoming part of the public record, open to publication by the media.

Searches can be conducted by the security force, Emergency Response Team, the Facilities Department in conjunction with department managers, or by a combination of these methods. Bomb sniffing dogs are very effective, but their extended response time makes their utilization often impractical. Training in search methods and bomb recognition is desired but not overly important as a bomb can look like anything – any object that is out of place such as an unidentified, unclaimed briefcase, a package next to the gas main, or a small pipe sitting outside the data center is suspect. It is most important to identify search methods and searchers ahead of time.

Any search must be systematic, rapid, and thorough. Sectionalize portions of the site and building and prioritize the order these sections are searched. Assign specific search areas if they can be searched concurrently or assign the sections as personnel become available. A good starting place is any area mentioned in the threat (I always check the bottom of my chair first). Search next the most common, accessible areas bombs are found (building perimeter, 'public' areas), then areas that could provide a synergistic effect (hydrogen tank, gas main), and then areas critical to the business operation (backup electrical generator or data center). Search last the non-critical areas or areas difficult to reach. Assign these sections to teams most familiar with the area such as a department manager. This carries the advantage of increased search speed, a greater likelihood to recognize objects out of place, and a better knowledge of critical equipment and hiding places.

If a suspicious object is located, try to find its owner. Isolate (secure) the area from entry. Evacuate people away from the area (see table above) or send them home (the facility may be closed for 24-36 hours or more). Inform the appropriate jurisdiction (dial 911). If safe, open doors and windows around the blast area and shut off hazardous processes in the area. Consider shutting off utilities. If safe, continue to search for other devices. Do not touch or move the object (even if it is a 'dud'). Do not cover the object or cut any wires. Do not put the object in water or pour water on it. Activate your Crisis Management Plan.

**Package (Mail) Bombs**

Mail bombs can be envelopes, boxes, or packages and may have one or more of the following characteristics:

- Unusual postmarks or places of origin;
- Excessive postage;
- Incorrect addresses or titles of recipients;
- Excessive handling, wrapping, taping, or inappropriate bulkiness;
- Excess weight, stiffness, bulges or uneven balance and feel;
- Smudges and greasy looking spots or areas;
- An order of almonds or a chemical odor;
- Protruding wire or string;
- Pinholes from which a safety pin arming device may have been withdrawn.

The use of non-metallic letter openers can help to prevent a detonation, but if there is any doubt, isolate the letter and have it examined. Inexpensive sprays exist to quickly identify any explosive residue on the package.

**Summary**

An effective program to prevent, mitigate, and respond to a bomb incident involves many more elements and knowledge than outlined here. As continuity planners we can take steps to understand the risks and effects of these incidents and to help influence company policy and procedures.

Evaluate your risk exposure, improve physical security, establish how and by whom a threat will be evaluated and decide what procedures will be followed when a threat is received or a device is discovered.