# Bomb Threat Management Planning Part I

***By Luis Rivera***

In 1998, Osama Bin Ladin declared war on the United States and legitimate targets all US citizens. Since the terrorist attacks of September 11, 2001 our government has managed to deter, and or disrupt other attacks against its citizens and infrastructure such as government buildings and facilities. However, though the government has made necessary adjustments, so have the terrorists, who have redirected their efforts to planning operations against "softer" or vulnerable targets or locations.

**You will be killed just as you kill, and you will be *bombed* just as you bomb. And expect more that make you uneasy … (Usama Bin-Laden)**

The use of *improvised explosive devices,* or IEDs, is one of the terrorists' preferred methods for assassination. These devices are often inexpensive and easy to build. Materials required to build these devices such as fertilizer and other readily available household ingredients are accessible in the open market. In addition to their cost effectiveness, IEDs possess incredible destructive power, making them ideal instruments of terror.

The most common types of attacks are in the form of vehicle bombs. Examples of this is the 1995 truck bomb used in the Oklahoma City bombing by Timothy McVeigh, the 2003 car bomb used by Colombian rebels in the Nogal building in Bogota, Colombia and the 2003 truck bomb attack of Camp Vinnell, Riyadh by Al Qaeda Operatives.

Another type of explosive devices/bombs used by terrorists is hand delivered bombs. These small explosive devices—when emplaced on strategic locations in the building can cause extensive damage. An example in which this type of bomb was utilized was the bombing of a mall in Moscow, the Russian capital, on August 31, 1999—killing one person and wounding 40 others. A note was left saying the bombing was a result of increasing Russian consumerism. Also in Colombia, suspected FARC rebels conducted three attacks in the cities of Medellin, Saravena and Cartagena. The attacks resulted in the killing of 21 people.

Other types of bombs include; incendiary bombs, letter bombs, chemical, radiological devices/dirty bombs, and suicide bombers.

## About Bomb Threats

Bomb threats are utilized by terrorists as well as criminals. Most bomb threats are made over the phone and though the majority of these threats are hoaxes—someone's idea of a cruel joke or terrorists looking to terrorize a specific sector of the population—they shouldn't be taken lightly and should be reported to the police immediately.

Bomb threats are categorized in two types;

- **Hoaxes**: The one in which no explosives have been emplaced
- **Genuine**: The explosives have in fact been emplaced.

**Q**: So, how can I tell one from the other?

**A**: You can't. Even threats that are real can sometimes sound funny or unbelievable.

**Q**: What can we do to prepare for such eventualities?

**A**: Have a plan.

# How to prepare a plan

There are four areas that must be considered during bomb threat management planning:

- Planning and Preparation
- Receiving the Threat
- Evacuation
- Search

The most important factor in managing a bomb threat is having a plan. However, just having a plan for the sake of having one is not worth the piece of paper it is written on. Bottom Line; a plan does not equals a capability, meaning that in order to have a plan that saves lives, it must be exercised, critiqued, and validated. Exercises should be done internally as well as in conjunction with other government agencies—police, firefighters, emergency response teams—as well as private organizations with in the community.

In order to develop an effective bomb management plan it is imperative to have an idea who you are trying to protect against as well as the strengths and vulnerabilities of the building or buildings you are trying to protect. This information can only be gathered by conducting a threat and vulnerability evaluation.

- A threat evaluation is nothing more than information on criminal and or terrorist organizations in the area as well as their methods of operations.


- A vulnerability evaluation provides information regarding specific gaps in physical security that could be exploited by a potential terrorist or criminal.

***It is important to mention, though schools and universities are vulnerable, they are not as vulnerable as hospitals***. The primary reason is, hospitals mostly concentrate their training on how to

respond to a major terrorist incident, rather than planning and or training on what to do if the hospital itself was attacked."

It is important to consider what the terrorists are looking for when casing a location as a potential target. In order to develop a plan or course of action, terrorists must have detail information on the intended target. This information is gathered through surveillance and the use of what is called "The Target Analysis Process." A target analysis is based on the following factors: ***criticality*** (the influence which target destruction or damage will have on the government), ***accessibility*** (the degree to which a target can be penetrated, either physically or with the use of weapons), ***recoverability*** (how long it will take the target to recuperate—measured in time, if the desired damage is less than total destruction), ***vulnerability*** (the extent to which the target is vulnerable if the terrorists have the means, ability, or expertise to destroy it), and ***effect*** (what type of reaction the act or attack will provoke from the population).

## C2

Command and control or C2 is the key to success in responding to any emergency—these are the people in-charge with making the necessary decisions. Therefore, the plan must delineate a clear ***chain of command***, the ***command relationship*** with other agencies as well as ***task organization*** (who is responsible for what). Additionally, the plan must identify the ***locations of the command post*** (Primary and alternate). The command post should have available an ***up to date alert roster*** (procedures for notification of emergency personnel and agencies as well as Points of Contact telephone numbers, and services i.e. fire department, police, FBI, explosives and ordinance, ATF, etc.). It must also include a copy of the ***communications plan*** (Very important, as "You may be able to command all you want, however, without communications; you would not be able to control anything") as well as sketches, photographs and blue prints of the building. In addition, the command post must also have copies of the ***evacuation and search procedures*** with a list of the key personnel assigned to supervising and performing said tasks.

## Logistics

The next item to consider is emergency equipment. Things like fire extinguishers, and first aid materials. It is also as important to conduct sporadic inspections to ensure the equipment is in working order and in enough quantities.

## Preparation

As most threats happen over the phone, it is essential to have ***bomb threats checklist*** by all telephones. A signal of some kind (known by all) should be developed in order for the person that's handling the call to alert others without breaking contact with the caller. The person receiving the call must remain calm and objective at all times. Remember not to hang up the phone when the call has been terminated, as it is still possible to trace the call. However, if the threat is written, it is important to handle with much care to avoid disturbing anything that can be used as evidence (the best thing to do is to place note inside a document protector).

**Upon receiving the threat**, the first thing that has to take place is the notification of key personnel (personnel responsible for executing the bomb threat plan) and pertinent agencies.

**Evaluation of the threat** will follow notification. It is here the decision makers make their money. They will attempt to determine if the threat is in fact real. Nevertheless, all threats will be treated as real until it is determined otherwise. Historical data seem to indicate the more specific the threat the better the chance it is the real thing. However, even threats which information seem to be hazy, should not be underestimated. Again, it should continue to be handled as the real thing until it has been investigated and evaluated. Personnel that received the information must be made available to law-enforcement personnel/authorities (not people that received information second hand) as well as personnel that are familiar with the building (such as maintenance personnel) as they are the ones that can better determine if something looks out of place or doesn't belong.

## Considerations for Evacuation

Once the threat has been evaluated a determination must be made as to what course of action (COA) would be the most desirable given the situation—this is where the Big Dawgs really earn their money. COAs available are as follows;

- Do nothing
- Conduct a search without evacuating personnel from the building
- Conduct a partial evacuation of the building
- Conduct complete evacuation of the building and conduct a search of the building

## Planning Considerations

- **Evacuation routes**: As a rule the key word ***PACE*** should be applied when determining evacuation routes—PACE stands for **P**rimary, **A**lternate, **C**ontingency and **E**mergency. The primary reason for having these many routes is that the suspected IED may be located along or in the vicinity of one of the routes. In addition, if the device should detonate during evacuation, one or more of the routes may become inaccessible.

- **Evacuation Signal**: Signals may vary from one location to the other. However, it is not advisable to use signals all ready designated for other emergencies. For example; A fire alarm, though effective in alerting everyone at the same time, may not be the best signal to use as in the event of a fire, doors and windows are closed in an attempt to prevent the fire from spreading. However, in a bomb/IED situation the actions required are the opposite. In a bomb/IED incident, windows and doors are left open to minimize fragmentation. Other means of signaling are telephonic notification and word of mouth (Key words). Whichever method is utilized for initial alarm, it most be accompanied by voice commands. These commands must be **C**lear **C**alm and **C**oncise (the intent of these commands is to provide reassurance and keep positive control of the personnel during evacuation).

- **Identify and train evacuation control teams**: these personnel must be knowledgeable of the routes (PACE), any and all dangers or hazards along the routes, as well as have the ability to control and direct the evacuees.

- **Identify personnel holding areas/points**: These locations should be at a safe minimum distance from the building with the IED (no less than 300m). If all possible, it should be a terrain feature between the building/IED and the holding point. The location of the holding areas should also provide protection from the elements.

Again, hospitals have different considerations when dealing with evacuating patients and personnel. They prefer to use ***"horizontal evacuation"*** procedures or moving patients to other parts of the building. The reason for this is; some patients are not easy to move or evacuate as they may be on life support systems or their condition would not allow it. The assumption is that emergency services will arrive in time and evacuate them if necessary. However, the reality is that emergency response agencies and personnel may not be able to intervene as timely as expected—as was the case in areas affected by Hurricane Katrina. Therefore, it is imperative to plan to continue to operate without outside help for a period of 48-72 hours.

The last of the tasks to consider when developing a plan is the ***SEARCH*** of the building. However, this task will be addressed separately in a Power Point Presentation—the second part of this article—in an effort to better illustrate some of the tactics, techniques and procedures (TTP's) involved.