Terrorism prevention measures for office buildings – a new layering approach

S. Dermisi
Walter E. Heller College of Business Administration, Roosevelt University, U.S.A.

Abstract

Terrorist targets have changed through time from specific individuals, aircrafts and government or military related installations to office buildings. Considering recent terrorism attacks targeting office buildings the one that tops the number of victims is the September 11, 2001 World Trade Center attacks in New York. This terrorism incident along with the threat of other attacks towards office buildings has modified the perspective of owners and management companies towards security of office buildings in a post September 11, 2001 context in the U.S. The initial reaction, of general security measures with an unclear prevention role, should be replaced by improved and more thorough decision-making process of prevention measures targeting specific types of threats for specific buildings. This paper proposes the development of a layered approach in terrorism prevention through the formation of Building Security Task Forces (BSTF), which will utilize a number of security measures outlined in the paper. The main role of a BSTF is the protection of their property by the implementation of existing security measures as well as cross-collaboration with law enforcement and emergency management agencies allowing the development of contingency plans to address terrorism most effectively. In addition, the city of Chicago is used as a case study, because of the several corporate headquarters, high-rise and trophy buildings.

Keywords: office building security measures, office buildings, office property management, terrorism.

1 Introduction

Terrorism has been used at an international level as a means of protest by politically, ideologically or religiously motivated groups, since the early nineteen
hundreds. Considering the number of international terrorism incidents and their casualties, there is clear evidence of a decrease in incidents after 1988, with an increase however of the number of casualties with significant spikes from 1995 until 2003 (Figure 1). Enders and Sandler [8] highlight, in their study of terrorism patterns, that in recent years a terrorism act is 17% more likely to result in casualties than in the 1970s. In addition, focusing on the type of facility targeted through time, businesses are hit the hardest after 1988 (Figure 2). The significant decrease in number of businesses targeted by terrorists after 2001 can be attributed to the increase of protection measures taken by office building owners and managers after the terrorist attacks of September 11, 2001. Although a variety of security measures were initially used, their significant cost made them quickly obsolete and property owners and managers have been seeking for the appropriate measures, which balance security and cost.

Figure 1: Number of terrorist incidents and casualties, 1968-2002. (Data source: U.S. Department of State [15] and Sandler [13]).

Figure 2: Type of facilities struck by international terrorist attacks. (Data Source: U.S. Department of State [15]).
This paper highlights both the physical and decision-making measures to be taken by private office owners and managers in cities or areas where an elevated-high threat level exists. It also proposes the formation of a Building Security Task Force (BSTF), with specific goals and strategy. BSTF will be both an up-to-date Task Force on security issues and will also enhance the communication among property personnel, investigative and emergency personnel improving the on-site human intelligence and response time.

2 Building security in the US: before and after 9/11/01

A survey of more than 200 BOMA and ULI members [5] indicated that the most widely employed security measures before September 11 included building alarm monitors, lobby security, surveillance cameras, partial employee background checks and in very limited cases perimeter barriers. The most frequent upgrade after 9/11 was tighter vendor security including vendor identification, check-in and request for vendors to conduct employee background checks. Another survey of 300 office tenants conducted by DEGW and IDRC [5], from 12/01 through 1/02, highlighted the importance of planning for emergency escape and some preference towards low-rise buildings. Some of the measures proposed by this survey included: better CCTV, emergency planning and evacuation, vendor IDs and restricted access, key access system, eliminating loading-dock parking and after hours delivery.

Nadel [9], who has conducted extensive research on building deficiencies and vulnerabilities, identified 10 deficiencies in existing facilities (Table 1) and also suggested enhancement measures for three different types of buildings (Table 2).

Table 1: Top 10 deficiencies found at existing facilities (source: Nadel [9]).

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Overgrowth of vegetation</td>
<td>6. Insufficient operations and implementation for delivery vehicle and material products</td>
</tr>
<tr>
<td>2. Insufficient area for operations and implementation of badge inspection and visitor entry</td>
<td>7. Insufficient security force relative to facility size and operational requirements</td>
</tr>
<tr>
<td>3. Insufficient CCTV</td>
<td>8. Lack of overall parking policies and vehicle ID</td>
</tr>
<tr>
<td>4. Generic exterior glazing</td>
<td>9. Unknown response time to threat</td>
</tr>
<tr>
<td>5. Insufficient ballistic protection for security posts</td>
<td>10. Poor demarcation of property boundary</td>
</tr>
</tbody>
</table>

Both surveys [5] and Nadel [9], however, focused on the actual measures which are or should be in place rather than a strategic approach towards building security in a livable-aesthetic appealing rather than gated environment. The first effort to address security measures within a multidisciplinary context even
beyond the actual structure was in 2000 with the establishment of an Interagency Security Task Force by the National Capital Planning Commission (NCPC), Remo [12] in Washington D.C., in an effort to improve the aesthetics of the security measures. Some of the issues examined included threat profiles, standoff distances, public access and transportation requirements. To ensure a uniform look for security the downtown was divided into “contextual zones” based on location and architectural style and then each contextual zone was further divided into zones of security.

Table 2: Vulnerable building construction features and enhancements (source: Nadel [9]).

<table>
<thead>
<tr>
<th>Material</th>
<th>Area of vulnerability</th>
<th>Enhancements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Steel construction</td>
<td>- column splices&lt;br&gt;- interconnectivity of components of built-up sections&lt;br&gt;- beam-to-column and beam-to-beam connections</td>
<td>- increase weight of column sections at lower levels&lt;br&gt;- full movement connection splices at lower level&lt;br&gt;- full moment capacity beam to column connections</td>
</tr>
<tr>
<td>Glass construction</td>
<td>- brittleness of glass&lt;br&gt;- frame-building connection&lt;br&gt;- limited ductility of frame</td>
<td>- laminated and tempered glass&lt;br&gt;- higher glazing strength&lt;br&gt;- enhanced glass frame design</td>
</tr>
<tr>
<td>Concrete construction</td>
<td>- lack of sufficient ties and stirrups&lt;br&gt;- limited ductility&lt;br&gt;- brisance</td>
<td>- spiral reinforcement or closely spaced ties in columns&lt;br&gt;- continuity of steel reinforcement&lt;br&gt;-higher concrete strength&lt;br&gt;- wraps or jackets around columns</td>
</tr>
</tbody>
</table>

The next effort of a holistic approach towards security came seven weeks after 9/11/01 by the City of Chicago where, as Archibald et al [3] state, the Chicago City Council passed an ordinance that requires and regulates the involvement of high-rise building owners and managers in evacuation planning and training. Chicago buildings are classified as low, medium, or high risk and high-risk buildings are then assessed by a Joint Emergency Responder Team (JERT), which includes members of the Chicago Police Department, Chicago Fire Department, and the FBI. The assessment serves two purposes. First, it identifies the vulnerabilities to building and security managers and secondly it provides the Chicago's Office of Emergency Management and Communications (COEM) with a detailed set of data in the event of a terrorist attack or other disaster. Lower-risk buildings conduct similar self-assessments and submit their results to COEM.
3 A new layered approach towards office building security

3.1 Theoretical framework

A Senior Vice Present of Colliers encapsulated perfectly the way property managers and owners should view office building security in the future; as a balance among: safety – security – convenience and asset preservation (Bergsman [4]). The most significant element, but not mentioned however for creating the equilibrium between the four aforementioned elements, is the effective strategic design of the actual goals to be accomplished. Considering at the same time that private office building owners and managers are faced with the reality of their property in need to be appealing rather than a gated fortress with substantial costs, the task to balance all four elements is even harder. A recent survey conducted by BOMA highlights the cost differences between government and private sector buildings. Security spending by the government increased from $0.87 per sf in 2001 to $1.26 per sf in 2003. In contrast the spending for private sector office building increased from $0.49 per sf to $0.55 for the same period (Chapman [6]). Considering the property aesthetics and cost of security, office owners and managers can be successful in combating terrorism by adopting a preventative layered approach similar to the government buildings. The difference between government and private buildings, however, is the need of office buildings to be both safe and financially survivable within a city’s office market. Archibald et al [3] suggest two primary rationales behind the need of multiple layers: a) Reducing the likelihood of a catastrophic consequence due to an individual point failure, and b) Increasing a building’s robustness to various threats. Adding these two rationales an even more significant point is the deterrence this layering protection approach has on a terrorist event. Terrorists always seek the points of less resistance and the implementation of a layered prevention strategy will probably decrease the possibility of attack in a secured location.

3.2 Formation of a Building Security Task Force and its goals

This paper proposes, as a first step in combating terrorism at the property level, the formation of a Building Security Task Force (BSTF). This Task Force will be multidisciplinary, flexible, but with fewer members than Nadel’s [9] and Owen’s [11] risk assessment group. BSTF will include the heads of: property management, security, human resources and Information Technology (IT) (IT should be included especially in case of “Smart buildings”) as well as the owner, architect and a tenant representative. In cases where an owner or property management company have more than one office properties in their portfolio, the BSTF should be established to oversee all properties within the portfolio, but a separate assessment per building and location need to be performed. The main role of the BSTF is to establish and succeed in three anti-terrorism goals (Detect -Defend - Defeat) (3-D) (Figure 3), which in certain aspects is similar to the 4-D strategy (Defeat, Deny, Diminish and Defend) followed by the U.S in its war on terrorism (White House [17]).
The three – D goals of the Building Security Task Force can be analyzed as follows:

- **Detect**: The security measures in place should be able to detect security breaches. Existing detection measures should be in layered format from the exterior perimeter (e.g. CCTVs, etc) of the building through the interior (e.g. HVAC sensors, metal detectors etc.)

- **Defend**: The questions – issues Owen [11] raises can be also used with some adjustments as a cornerstone for the implementation of the most effective bricks and mortar measures for each property. The two elements he highlights are location and property image; this paper adds also the tenant component.
  
  a. **Location - identity**: physical location (CBD or suburbs), easy to defend or not, neighbors’ identity and risks associated with their proximity
  
  b. **Image**: property owner, mission and religious conviction
  
  c. **Tenants**: types of tenants (financial institution etc.) and their image

Considering AIA [2], Chapman [6], NIBS [10], and Owen [11], the most fundamental protection measures are:

1. **Obstruction**: Can be accomplished by identifying the type of threat (prevention measure) from the following list: (a) unauthorized entry (biometrics, ID access, elevator access cards and limited floor access), (b) insider threats (personnel background checks), (c) explosive threats (standoff distance, setbacks, bollards, concrete barriers, fountain, ponds, reinforced concrete benches, planters and mailroom inspection devices), (d) ballistic threats (critical assets away from roads, redundancy in design), (e) weapons of mass destruction [emergency planning, high elevation intakes, safe rooms and for HVAC there are four types of filter systems: straining (fairly inefficient), impingement (most common, still low efficiency), interception (medium efficiency), diffusion (good efficiency)], and (f) cyber and information security threats (software and hardware devices which can detect perpetrators).

2. **Absorption**: Can be accomplished by protecting a building’s structural and vital vertical systems from fatal damage by appropriate design, which will harden the building skin or by introducing laminated safety glass, window coverings, surface coatings and blast curtains.

Figure 3: Three-D goals for Building Security Task Force (BSTF).
3. **Diversion/Deflection**: another design technique is to impede or deflect an explosion or impacting force to a new or different direction. A roadway is often sufficient to slow a hostile vehicle

- **Defeat**: Has two components, deterrence and diminishing the effects of an attack. A terrorist attack can be deterred if the BSTF utilizes the following three elements:
  
  a. **Intelligence gathering**: The layering of the various security systems from the exterior to the interior of a building should be capable of identifying evolving behavior patterns, especially through the adoption of smart surveillance systems, which can be significantly beneficial in identifying potential threats to a building and area.
  
  b. **Apprehend a suspect**: The combination of smart surveillance systems and well-trained security guards may lead to a suspect apprehension. Depending on the type of potential threat (e.g. industrial espionage or terrorist attack) consultation with the local Joint Emergency Responder Team (JERT) (Emergency responders and Intelligence Agencies at the city level – similar to Chicago) or a Local Joint Terrorism Task Force should be required to implement apprehension or deterrence strategies.
  
  c. **Foiling an attack**: Assuming that a property has various lines of defense from the exterior through the interior, a measure such as a frequent change of security routines does not allow a terrorist perpetrator to identify patterns of security and ways to overcome them; therefore, increasing the probability of foiling a potential attack.

The second component leading to the defeat of terrorist plans is the introduction of measures diminishing the effects of an attack. As Apgar [1] states, corporate real estate safety, security and survival will depend on contingency planning. Companies such as Morgan Stanley had prepared evacuation and “back-up” plans during the Gulf War and reinforced them after 1993 WTC bombing through disciplined organization, systematic training and detailed manuals. In addition, however, to company emergency strategies, BSTF should also develop the following elements:

a. **Emergency and contingency planning**: Since emergency responders are the first personnel called in case of an emergency, there is need to develop emergency plans with these agencies (Fire, Police etc), similar to the Chicago model. The most significant need however is the frequent evaluation of the existing plans in collaboration with emergency personnel in an effort to be prepared and use the most recent security practices. Some of the elements included could be: establishing evacuation routes, shelter areas, appointing evacuation coordinators and prepare for a decentralized command post. Mark stairways.

b. **Training exercise**: Tenant and staff training along with fire drills are very effective in Owen [11] educating individuals not to panic in an actual event. Characteristic are the reports of lack of panic in the World Trade Center building evacuation, due to the significant training, which took place in advance. Archibald et al [3] also highlighted the need for increase in the frequency and realism of evacuation drills even including
emergency responders, such as firefighters, police officers, and utility company emergency workers. As in the case of Chicago, emergency evacuation training takes place often for certain buildings, along with emergency personnel and the evacuation times are often reviewed and measures are taken to improve them.

3.3 Means for BSTF goal accomplishment

Although the security personnel of the BSTF is usually knowledgeable on prevention measures, there is a continuous need of training and adjusting to new evolving threats. This need can be met by the introduction of safety courses and training offered by the local Life and Safety Task Forces (LSTF) (mainly formed by local owners and managers associations) and security companies. LSTF will be also in close collaboration with the Local Joint Terrorism Task Force and/or Joint Emergency Responder Team (JERT) in an effort to be updated on new security needs (Figure 4).

![Diagram of Building Security Task Force (BSTF) training]

The formation of the Building Security Task Force (BSTF) and its 3-D goals are two significant components in the effort to combat terrorism, but there is a clear need for the formulation of a strategy to accomplish the 3-Ds (Figure 3). The strategy proposed is partially drawn from the Five Step Risk Management Process by the US GAO [16]. (Identify assets, identify threats, identify vulnerabilities, assess risks and determine priorities and identify countermeasures). The backbone of the proposed strategy in accomplishing the 3-Ds are the three phases outlined in Figure 5:

-Phase 1. Threat determination and assessment of property condition: This phase encapsulates both the identification of a threat and the assessment of the property weaknesses and strengths. The analysis should be conducted not only for the property, but also for a radius around the property.
Figure 5: Building Security Task Force (BSTF) strategy for accomplishing the 3-Ds. (Risk level table source: UTD and VFA [14]).

- **Threats:** There are mainly two ways to determine a threat; either form in-house intelligence (based on property surveillance) or by external notification by the Local Joint Terrorism Task Force (LJTTF) and/or Joint Emergency Responder Team (JERT). Based on the identified threat the building’s weaknesses and strengths are determined in terms of its security protection. Depending on the source of the threat, a close collaboration might be required with the LJTTF and JERT in identifying potential means of attack and means to mitigate them. In order to maintain the appropriate awareness level the threat assessments need to be updated regularly.

- **Weaknesses – Vulnerabilities:** Can be determined based on the specific type of threat, the measures in place and the experience and education the BSTF has received on the measures needed to address it. In addition to Archibald’s et al [3] structural, operational (tenancy of an icon, emergency training) and contextual vulnerabilities (proximity to other targets), a building might not be prepared for example to deter a car bomb, but after identifying the threat, measures such as elimination of parking spots adjacent to the building and barriers installation may deter such an attack.

- **Strengths:** Can be identified both in terms of the security measures taken to deal with a potential threat, but also in terms of the location, building design etc.

- **Phase 2. Risk Assessment:** The risk assessment of all three elements of phase 1 will be conducted through the risk reduction matrix (Figure 3) and by identifying a property’s priorities.
- Phase 3. Countermeasures: Depending both on the type of threat and the severity of its results two different paths can be followed. In the case of a moderate or severe risk of attack the LJTTF and JERT need to be notified if the threat tip does not initiate from them and protection measures will be decided with their involvement. However, in a low risk situation measures can be determined by the BSTF.

4 Conclusions

This paper proposes the establishment of a Building Security Task Force (BSTF) with vital to the building representatives. The goals of this Task Force are to Detect, Defend and Defeat (3-Ds) a potential terrorist attack targeting a building. In order to accomplish the 3-D goals, the Task Force will be continuously educated by a Life and Safety Task Force (established by city wide building owners and managers) and security companies. The 3-Ds will then be accomplished through the implementation of a 3-phased strategy of Threat Determination, Risk Assessment and Countermeasures.

References