RiskTopics

Guidelines For Reducing Exposure To Terrorism Risk In Public Spaces

October 2015

In recent years, private and public access organizations such as hotels, retail, shopping malls, sports complexes and other businesses, commonly referred to as “soft targets”, have increasingly become targets for acts of terrorism or extreme violence. Preparation, training and awareness along with completing a comprehensive risk assessment are necessary steps to help prevent or mitigate such events and enhance your overall risk management program.

Introduction

According to the U.S. Federal Bureau of Investigation, domestic and global acts of terrorism, along with acts of extreme violence have two common characteristics: First, they involve acts dangerous to human life. Second, they appear to be intended to intimidate or coerce a civilian population to influence governmental conduct via mass destruction, assassination, or kidnapping. Incidents of these nature are increasingly being perpetrated on private business and other public access operations. Under the standard of reasonable care, as the owner and/or operator of a business that is open to public access, you have a responsibility to provide a reasonable level of safety and security.

This Risk Topic will provide useful information for businesses and venues open to the public to help them protect their visitors, guests, and patrons from acts of terrorism and acts of violence as well as to help mitigate potentially severe business interruption losses. Malicious damage, shoplifting, and nuisance exposures are limited in scope and magnitude. Terrorist acts are often violent and intended to cause mass hysteria, personal injuries, and/or major property damage.
Discussion

Examples of terrorist attacks and threats on public venues have included:

- **February 2015** – United States, Secretary of Homeland Security warns shopping malls across United States, Canada, and United Kingdom to be vigilant after a terror group called for attacks. Several malls throughout the U.S. and Canada were specifically named in the threat.

- **July 2012** – Gunman opens fire in a movie theater in Aurora, CO, killing 12 and injuring over 70 patrons. Since this attack other movie theaters have been the sites of attacks resulting in loss of life and injuries.

- **June 2014** – A shooting attack at a Las Vegas, NV, restaurant – five killed.

- **April 2013** – Explosive device detonated in phone booth outside a hotel – one person injured.

- **November 2013** – Gunman opened fire on TSA Agents at Los Angeles International Airport. One TSA Agent was killed, two others were wounded and five civilians suffered injuries.

- **June 2011** – Attack on Super Market Area in Pakistan. Eighteen killed and 80 injured, with 20 retail shops destroyed.

- **September 2001** – United States, Terrorists flew airliner into World Trade Center in New York City resulting in the deaths of 2,606 people and over $2 billion in physical damage.

- **July 2009** – Two suicide bombers detonated inside hotel restaurants with 9 patrons killed.

- **November 2008** – Four armed assailants carried out an extended attack on large hotel in India. Over three days there were eight coordinated attacks resulting in 171 deaths and 250 injuries. The hotel sustained very severe damage.

- **2006 United States** – National Football League received dirty bomb threat targeting 7 NFL stadiums.

- **2005 United States** – Oklahoma University student prematurely detonated himself outside an 84,000 patron packed stadium.

- **2003 United States** – Continental Airlines Arena bomb threat.

- **April 1995, United States** – Bombing of a federal building in Oklahoma City, OK. Among the 168 killed were 19 children in a daycare center within the structure. The blast destroyed or damaged 324 buildings causing over $650 million in physical damage.

The New York World Trade Center contained dozens of retail stores and restaurants all of which were destroyed in the attack. Running beneath the towers was a commuter rail line which was severely damaged too. Beyond the horrific loss of human life, the infrastructure loss was massive. In addition to the towers numerous adjacent buildings were also destroyed or severely damaged. Countless businesses were destroyed and thousands of employees displaced.

Terrorist threats involving soft targets cannot be overlooked or minimized because of the large concentration of people coupled with the human population being a major target of the terrorist. History has shown that preparation and risk management can help mitigate these kinds of catastrophic losses. Investigations after a
number of incidents revealed that terrorists had targeted facilities and placed them under surveillance prior to their attack. In other examples, security controls were challenged prior to an attack to determine the expected response from the organization or company. In some cases, a business or operation was infiltrated by the attacking group placing an “employee” on the inside to gain valuable operational information prior to an attack.

**Risk Assessment**

All businesses should complete a comprehensive risk assessment to identify and enhance potential weaknesses in the overall risk management/emergency preparedness plan. There are numerous risk assessment protocols that can be utilized to complete a formal risk assessment. ASIS International has published a general security risk assessment guideline that can be used as a resource. A comprehensive risk assessment should include:

* Identify assets of the organization
* Identify potential loss scenarios
* Identify vulnerabilities
* Impact of potential event
* Prevention and mitigation of event
* Develop recommendations to close vulnerability gaps
* Cost/benefit analysis
* Testing and review of program

Each component of the risk assessment should be thoughtfully and honestly addressed as well as communicated to enhance the overall effectiveness of the assessment. Members of the management team involved in the risk assessment should include, but may not be limited to, Security, Legal, Human Resources, Operations, Facilities and Risk Management.

Follow up of the risk assessment and regular review of security and emergency preparedness protocols should be conducted to ensure your plans are up to date, especially when new operations or extensive renovations are introduced.

A list of actionable strategies to supplement and enhance communications, protection, mitigation and emergency response plans should be established. These strategies should focus on “Preparedness-Response-Recovery” approach to help reduce the adverse impact on your business as well as to help insure business continuity and resiliency. Insurance policies and coverages should be reviewed with insurance brokers and agents. In completing the risk assessment it may help to ask the following two questions:

- What areas would be of interest to me?
- What parts of the facility or structure might I be able to breach?

**Emergency Action Plan**

A formal emergency action plan (EAP) should be developed and implemented for your business. The EAP should include actionable items for all foreseeable emergency situations including terrorism, workplace
violence, fire, extreme weather, power outage and medical emergencies. A formal EAP document should include:

- Backing up important records, removing or securing high value assets, checking mail, packages, and incoming shipments for suspicious packages, evaluating vendors and suppliers.
- Assign responsibility for implementing the plan.
- Designate a media spokesperson.
- Implement communication plans for security personnel so they receive developing situational information.
- Hotels instruct reservation department employees to inform guests calling the hotel of a potential disturbance in the area.
- Consider revising no-show billing practices for reservations canceled or not honored during the disturbance.
- Stock adequate supplies of food and beverage to last for an extended duration disturbance.
- Establish policies and procedures to make the safety and security of visitors and guests a top priority.
- Determine law enforcement, mall and hotel security, third party and other internal response, communications, capabilities, etc.
- Determine changes to corporate arrest/apprehension guidelines to protect management and employees from injury.

Security Actions

A formal security plan should be developed and implemented proactively. A strong and comprehensive security program is a valuable tool to aid in the prevention of an extreme act. The security plan cannot be a “one size fits all” approach to security. The security plan should be tailored to each specific location. A formal security plan should consider, but may not be limited to the following:

- Gates and perimeter entrances are secured when not attended
- Verify protective window grills for all accessible windows, including basement windows. Where shutters are provided can they be closed in the event of a threat? Remove high-value goods from display windows. Consider moving guest tables away from high profile windows. Consider the installation of roll down burglar gates for new or remodeled retail locations. Consider the installation of impact resistant film for glass windows and doors at a minimum.
- Maintain exterior doors in a closed and locked position wherever possible, including basement level doors. Verify all locks are secure from tampering. Where hotels do not have a front door is there a plan in place to provide protection to the front entrance, such as a physical barrier which could be quickly relocated?
- Secure elevated doors, windows, and other access points, such as air intakes or determine if they be eliminated? These include rooftop locations.
• Are “No Trespassing” signs installed?

• Is there an electronic illegal entry system? Is there a procedure to insure it remains in operable condition? And are all features activated to the extent possible?

• For manual card access systems, establish policies to avoid entry of unauthorized persons.

• Are any closed circuit video surveillance systems in good working order? Enhance video surveillance to all key areas, such as rear doors, entrances, lobby, and receiving docks.

• Enhance security staff levels based on results of risk assessment findings. Contract with outside vendors if necessary before an act occurs.

• Are pre-employment verification policies in place and enforced, including for vendors where possible?

• Are all suppliers and receivers known? Do they carry identification? Who has access to delivery schedules?

Fire Protection

• Ensure that all fire protection systems are maintained in good working condition.

• Secure all flammable and combustible materials. Are fuel pumps locked? Are chemical storage areas secured? Are gas cylinders chained and locked or removed from site? Are corrugated cartons and other materials removed from the site on a routine basis?

Emergency Power

• Take action to verify emergency system is ready. Is the emergency fuel tank filled? Are emergency lights in working condition?

• Is additional emergency generator fuel available to supply power for an extended period of time?

Evacuation

• Initiate actions based on the risk assessment.

• Plan for the evacuation of all employees and customers. Based on your risk assessment this may involve all persons, or all persons except security staff or other key personnel.

• Plan an alternative evacuation route or defend in place strategy for employees and customers in the event an act blocks or prevents an orderly evacuation.

Awareness of an actual threat or act

Once an act of terrorism or extreme violence has been identified, the safety of life should be the main priority. There are numerous publically available resources that address response to an actual threat. Public resources available include the Department of Homeland Security (DHS) and Federal Bureau of Investigation (FBI). These resources are an excellent source of training materials such as the Run, Hide Fight video series. Additional possible considerations include:
1. Immediately notify the police of the threat or act providing as much information as possible, including a description of individuals if possible. Subsequently, notify internal security, district and corporate management and/or legal counsel.

2. Do NOT confront terrorists. Protect employees and customers.

3. Evacuate the building if safe to do so. Once evacuated report to a designated regrouping location.

4. Verify that all security measures are working and enhance the security threat level to the extent that operations will allow:

   **Passive:**
   - Fences-Close and lock all gates
   - Windows-Close window protective systems such as shutters.
   - Doors-Close and lock all exterior doors.

   **Active**
   - Electronic illegal entry systems-Activate the perimeter monitoring system (activate also if full evacuation is planned).
   - Close all internal fire doors as time permits

5. Evacuation – Initiate evacuations in accordance with the situational risk assessment.

6. Be honest with customers and guests about the situation. Provide updates as possible. If evacuation is not deemed to be a safe alternative, encourage customers and guests to remain on the property. Relocate customers and guests away from entrances and windows. Relocate employees away from exteriors and parking garage.

7. Relocate all ground floor hotel guests or workers to upper floors out of harm’s way.

8. Reporting – Maintain an incident log and complete reports as soon as it is safe to do so for appropriate reporting to the corporate, legal and insurance company claims notification.

**Following the act when authorities advise it is safe:**

1. Account for employees, customers, and guests.

2. Cooperate with police and other authorities.

3. Secure all surveillance records.

4. Provide copies of videos and witness statements as directed by corporate office and legal department.

5. Critique event response. Obtain local management and employee feedback

6. Update policies and procedures.

7. Enhance security systems, building physical security and staffing as necessary.
For employees remaining on the property during an act of terrorism:

1. Plan and provide housing if necessary. Ensure that employees at work have a means to stay if necessary.

2. Ensure employees have a means to contact their families which may help alleviate the problem of employees wanting to leave and go home.

3. Be aware of any curfews in effect which will limit the availability of employees, especially during nights and weekend shifts. Employees may not have the opportunity to get to/from work so plan accordingly.

4. During and immediately following an act use one entrance which is strictly controlled by security. Only employees scheduled to work should be allowed access into the building.

Conclusion

The risk of terrorism or extreme violence is unfortunately real and has occurred with very costly consequences in terms of human life, human suffering, physical damage, and business interruption. Consequences may continue long after an act of terrorism. How well a firm or organization can protect its visitors, customers, and/or guests may determine how quickly the firm recovers, if at all. In addition to the catastrophic exposure to personal injuries, property damage, and business interruption a firm or organization’s brand and corporate name damage is lasting. A comprehensive risk assessment with strategies to mitigate the identified risks and vulnerabilities can mitigate losses and preserve your good name.
References


Department of Homeland Security, [www.dhs.gov]

The information in this publication was compiled from sources believed to be reliable for informational purposes only. All sample policies and procedures herein should serve as a guideline, which you can use to create your own policies and procedures. We trust that you will customize these samples to reflect your own operations and believe that these samples may serve as a helpful platform for this endeavor. Any and all information contained herein is not intended to constitute advice (particularly not legal advice). Accordingly, persons requiring advice should consult independent advisors when developing programs and policies. We do not guarantee the accuracy of this information or any results and further assume no liability in connection with this publication and sample policies and procedures, including any information, methods or safety suggestions contained herein. We undertake no obligation to publicly update or revise any of this information, whether to reflect new information, future developments, events or circumstances or otherwise. Moreover, The Zurich Service Corporation reminds you that this cannot be assumed to contain every acceptable safety and compliance procedure or that additional procedures might not be appropriate under the circumstances. The subject matter of this publication is not tied to any specific insurance product nor will adopting these policies and procedures ensure coverage under any insurance policy.

©2015 The Zurich Services Corporation