

ACTS OF VIOLENCE

Preparedness for terrorism, active shooter, workplace violence, bomb threats, suspicious packages, and civil disorder

ISSUE: JULY 2017

[SUBSCRIBE TO PREPAREDNESS BULLETINS](#)

© 2017 PREPAREDNESS, LLC

Active shooter, homegrown violent extremist, lone wolf, and “run, hide, fight” are relatively new to our vocabulary as the concern over acts of violence has grown. Acts of violence can occur without warning, and most active shooter incidents are over before law enforcement arrives on scene. Sole reliance on police is not sufficient. Employees must be able to recognize an act of violence in progress and take the best available protective action.

Impacts of acts of violence include more than casualties and property damage. Businesses must plan for business interruption and the emotional recovery of workers following an incident. A preparedness program that is based on an assessment of risk; maintains strategies for prevention and deterrence; and includes emergency planning that has been implemented by training and exercises is essential.

Active shooter incidents in the United States from 2000-2013 took the lives of 486 people with 557 wounded¹. The majority of these incidents occurred in commerce/business and educational occupancies. The specter of terrorism has intensified in recent years as ISIS inspired individuals perpetrate acts of violence in the United States, Europe, and around the world. Since the terrorist attacks of 9/11 there have been 276 terrorist incidents in the United States resulting in 124 fatalities and 580 injuries.² As significant as these casualty statistics are, 417 work-related

homicides occurred in the United States in just one year—2015.³

Protests following police-involved shootings and surrounding the 2016 Presidential election have occurred across the United States. Some have escalated into civil disorder and rioting. Bomb threats—many communicated by electronic mail—have plagued schools and universities. Concern about suspicious packages following the October 2001 anthrax incidents continues today.

Defining the Problem: Threats & Acts of Violence

TERRORISM. Acts of terrorism in the United States have been perpetrated by those inspired by extremist Islamic ideology, white supremacists, abortion activists, Earth Liberation Front, Animal Liberation Front, and “unaffiliated individuals.” Leading targets have included private citizens and property, businesses, religious

³ *Fatal Occupational Injuries, 2015*, U.S. Department of Labor Statistics, December 16, 2016

¹ Blair, J. Pete, and Schweit, Katherine W. *A Study of Active Shooter Incidents, 2000 - 2013*. Texas State University and Federal Bureau of Investigation, U.S. Department of Justice, Washington D.C., 2014

² Global Terrorism Database, National Consortium for the Study of Terrorism and Responses to Terrorism, University of Maryland, College Park, MD 20740

In This Bulletin

Defining the Problem: Threats & Acts of Violence	1
Conducting a Risk Assessment to Identify Vulnerabilities & Planning Scenarios	4
Actions to Prevent or Deter Acts of Violence	4
Emergency Planning to Protect Life & Property	7
Suspicious Package	9
Business Continuity & Recovery	10
Program Implementation: Establishing a Capability to Protect Life & Property	10
Resources for Risk Assessment, Prevention, Deterrence & Plan Development	11

figures/institutions, government-non-diplomatic, abortion-related facilities, and educational institutions. While the concern over terrorist use of weapons of mass destruction (chemical, biological, radiological, and nuclear) is real, incidents over the past several years have seen the use of “low-tech” weapons including motor vehicles, knives, and even pressure cookers.

Federal Definition of “Terrorism”

United States Federal laws and regulations include multiple definitions of terrorism. “Terrorism includes the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.” (28 C.F.R. 0.85 (n)). Domestic terrorism is defined as “activities that—(A) involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State; (B) appear to be intended— (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and (C) occur primarily within the territorial jurisdiction of the United States.” (18 USC § 2331)

Recent incidents of terrorism include shootings at a Charleston, SC church, Colorado Springs Planned Parenthood, Pulse nightclub in Orlando, and the San Bernardino Regional Center. Recent attacks using motor vehicles as weapons have been perpetrated in the UK, at the Bastille Celebration in Nice, France, at a Christmas market in Germany, and on the campus of Ohio State University. Stabbings have been perpetrated at the University of California Merced campus, a shopping mall in Minnesota, and at a Columbus, OH restaurant.

IMPROVISED EXPLOSIVE DEVICES (IEDS). The term IED has been associated with war, but easy access to instructions and ingredients has resulted in numerous incidents involving the use of IEDs in the United States. IED attacks remain the primary tactic for terrorists seeking a relatively uncomplicated, inexpensive means for inflicting mass casualties and maximum damage. A series of bombings in Seaside Park, NJ and New York City in September, 2016 targeted a charity race and a Manhattan neighborhood. Unexploded

devices including a pressure cooker were found at both the New Jersey and New York City bombing sites.

BOMB THREATS. Once communicated by telephone, today bomb threats are often communicated by electronic mail and may surface on social media. More than 100 evacuations resulted from emailed bomb threats to the University of Pittsburgh in 2012. Numerous schools in New England were targeted in 2014 and 2016. Although the vast majority of threats are false, all must be taken seriously and a threat assessment conducted to determine the best course of action.

SUSPICIOUS PACKAGES. Letter bombs and the 2001 mailing of anthrax demonstrated the potential dangers of threats perpetrated by mail. Terrorist use of vehicle borne explosives has expanded the types of suspicious items to be alert for.

A suspicious *item* is defined as a bag, package, vehicle, or other item that is reasonably believed to contain explosives, an improvised explosive device (IED), or other hazardous material that requires a bomb technician and/or specialized equipment to further evaluate it.

WORKPLACE VIOLENCE. Workplace violence is any act or threat of physical violence, harassment, intimidation, or other threatening disruptive behavior that occurs at the work site.⁴ It ranges from threats and verbal abuse to physical

⁴ *Domestic Violence Assaults in the Workplace Study*, J. Lee, D. Trauth, Peace at Work, 2009

Terrorism Statistics

- 276 terrorist **incidents** in the USA from 9/12/2001 – 12/31/2015
- **Targets:** Private Citizens and Property (62), Businesses (56), Religious Figures/Institutions (40), Government-Non-diplomatic (31), Abortion-related (23), Educational Institution (18)
- **Perpetrators:** “Unaffiliated Individual(s)” 118, “unknown” 65, Earth Liberation Front (40), Animal Liberation Front (25), anti-abortion activists (9)
- 124 fatalities, 580 injuries
- **Primary Weapon used:** Incendiary (129), Explosives/bombs/dynamite (62), Firearms (45), Biological (19), Melee (6), Vehicle not including explosives (5)

Source: Global Terrorism Database, National Consortium for the Study of Terrorism and Responses to Terrorism, University of Maryland, College Park, MD 20740

assaults and even homicide. It can affect and involve employees, clients, customers, and visitors.

Homicide is currently the fourth-leading cause of fatal occupational injuries in the United States. According to the Bureau of Labor Statistics, 417 of 4,836 fatal workplace injuries in 2015 were workplace homicides. Workplace homicides rose by 2 percent in 2015, with shootings increasing by 15 percent. Assailants in workplace homicides differed greatly depending on the gender of the decedent. Approximately 43 percent of female decedents were fatally assaulted by a relative or domestic partner; the corresponding figure for male decedents was 2 percent. Acts by a relative or domestic partner are domestic violence perpetrated in the workplace.

OSHA reports that nearly 2 million American workers report having been victims of workplace violence each year. Many more cases go unreported. Research has identified factors that may increase the risk of violence for some workers. These factors include exchanging money with the public and working with volatile, unstable people. Working alone, in small groups, or in isolated areas may also contribute to the potential to become a victim of violence. Providing services and care, and working where alcohol is served may also impact the likelihood of violence. Additionally, time of day and location of work, such as working late at night or in areas with high crime rates, are also risk factors that should be considered when addressing issues of workplace violence. Among those at higher-risk are delivery drivers, healthcare professionals, public service workers, customer service agents, and law enforcement personnel.

ACTIVE SHOOTER. U.S. government agencies (DOJ/FBI, Education, and DHS/FEMA) define active shooter as “an individual actively engaged in killing or attempting to kill people in a confined and populated area.” The term is now commonly used to describe all acts of violence involving firearms, but most active shooter incidents are not acts of terrorism, which requires a motive of political or social change.

Active Shooter Incidents in the United States 2000-2013

- Deaths: 486, wounded: 557 (not including the shooters)
- Average number of incidents annually: 16.4 per year last seven years of the study period
- 70% occurred in either a commerce/business or educational environment
- 60% of the incidents ended before police arrived
- All but 2 incidents involved a single shooter
- In at least 9 incidents, the shooter first shot and killed a family member(s) in a residence before moving to a more public location to continue shooting
- In at least 6 incidents, the shooters were female
- In 64 incidents (40%), the shooters committed suicide; 54 shooters did so at the scene of the crime

Blair, J. Pete, and Schweit, Katherine W. A Study of Active Shooter Incidents, 2000 - 2013. Texas State University and Federal Bureau of Investigation, U.S. Department of Justice, Washington D.C., 2014

The frequency of active shooter incidents is increasing, and the majority of incidents occur in places of business, commerce, and education. Most incidents involved a single shooter; more often male than female. The majority of incidents were over before law enforcement arrived, and in 40% of incidents the shooter committed suicide.

CIVIL DISORDER & RIOTING. Protests and demonstrations surrounding the 2016 Presidential election occurred in more than two dozen cities from Nov. 9-27, 2016. Protests in Oakland, CA involved dozens of incendiary fires, and protests in Washington, D.C. on Inauguration Day resulted in objects being thrown at police, a motor vehicle set on fire, and damage to businesses.

The term civil disorder is defined in the United States Code of Regulations (18 USC § 232) as “any public disturbance involving acts of violence by assemblages of three or more persons, which causes an immediate danger of or results in damage or injury to the property or person of any other individual.”

Following police-involved shootings, protests erupted in Charlotte, Milwaukee, New York, Chicago, St. Paul, and Baton Rouge. Following the death of Freddie Gray in the custody of Baltimore Police in April 2015, peaceful protests escalated into rioting that resulted in injuries to at least

twenty police officers, at least 250 arrests, 285-350 businesses damaged, 150 vehicle fires, 60 structure fires, and 27 drugstores looted. A state of emergency was declared in Baltimore requiring activation of the National Guard and hundreds of State Police.

In Ferguson, MO protests and rioting followed the police-involved shooting of Michael Brown on August 9, 2014 and the announcement that police would not face indictment. At least a dozen buildings were set on fire and looted, many of them local businesses. Dozens of cars, including two police cruisers and a row of cars at a dealership were vandalized and left charred.

These incidents highlight the potential impacts of civil disorder on business operations, which can be significant and lasting for days until curfews are lifted and damage repaired.

ABDUCTION & KIDNAPPING. Abduction and kidnapping are other acts that require planning. Child abductions by non-custodial parents or sexual predators are a concern in schools but can be perpetrated at any day care or child care center or playground. Kidnap and ransom of employees traveling in riskier countries around the world has been a longstanding corporate concern.

Conducting a Risk Assessment to Identify Vulnerabilities & Planning Scenarios

A risk assessment that identifies potential acts of violence, develops planning scenarios, and identifies vulnerabilities of people, property, and operations should be conducted. Scenarios should take into consideration the potential locations and timing when an act of violence could occur. Vulnerable times are when large numbers of persons arrive and at the end of the day when most leave. Scheduled special events when large numbers of persons congregate should be carefully planned, and awareness of spontaneous demonstrations is imperative.

The risk assessment should evaluate the ability to detect threats and acts of violence, alert first responders, and warn people to take protective action. The adequacy of, and vulnerabilities or weaknesses in, prevention, deterrence and protection should be evaluated and mitigated to

the extent feasible. The risk assessment should evaluate the following:

- Site location, layout, and building exterior
- Building design and layout including egress routes and areas of refuge
- Surveillance, alerting, warning, communications, and protection systems
- Physical and operational security
- Employee risk factors including travel to, and work at, off-site locations
- Human resources policies and procedures
- Workplace violence prevention program
- Emergency planning for acts of violence including coordination with law enforcement
- Employee and responder training and drills and responder exercises

Actions to Prevent or Deter Acts of Violence

Physical & Operational Security

Knowledge of the concepts of crime prevention through environmental design (CPTED) and an understanding of the tactics of perpetrators of acts of violence is helpful when evaluating a site and access to buildings. Use of published assessment guides and checklists can aid in the identification of vulnerabilities and to evaluate preparedness.

Clear lines of sight and adequate illumination are essential for surveillance and to deter criminal acts. Potential spots where perpetrators can conceal their presence should be identified and eliminated. Fencing and locked or supervised gates can restrict access to areas of the property, and locked doors with access control systems can prevent unauthorized access to buildings.

Operational security is the human element of security. It includes processes to gather information and intelligence; evaluate evolving threats including local and regional events; and implement security commensurate with the threat level. Operational security is dependent on having access to threat intelligence and trained staff capable of implementing security measures. Everyone has some responsibility for security—to follow established security rules and be aware of persons or behavior that may constitute a threat. Operational security should include the following commensurate with the facility's threat level.

- Conduct pre-employment background checks
- Establish credentialing procedures that restrict access for employees and approved contractors to authorized areas
- Screen visitors, require an escort, and provide a visitor's badge
- Maintain control of building and utility diagrams; share with public safety
- Install video surveillance in accordance with national standards to cover the exterior and interior of all access points and select interior spaces; provide the ability to capture and export images and remote access to video surveillance during an emergency
- Establish interoperable communications and procedures for unification of command with public safety
- Implement the DHS “If You See Something, Say Something™” campaign. Develop criteria and reporting procedures for suspicious and irrational behaviors; unknown persons photographing, video recording, sketching, or pace counting on or in proximity to the premises; repeat visitors or outsiders who have no apparent business in non-public area; unattended vehicles; abandoned parcels, suitcases, backpacks, and packages.
- Develop a site security plan that includes visitor and package screening, threat detection, alerting of first responders, warning of persons to take protective actions, and communications protocols and procedures
- Document the locations of exits; post easily understood diagrams with primary and alternate paths to exits within each room; identify and include the locations of safe rooms on diagrams
- Develop and implement emergency procedures for threats and acts of violence identified during the risk assessment and protective actions for life safety (evacuation/run, lock-down/hide/shelter-in-place, and fight/counter)
- Provide training to enhance awareness of security measures; identify persons loitering, surveilling, or attempting to enter unauthorized areas; protocols and procedures for

reporting incidents; and emergency procedures including protective actions for life safety

- Conduct drills for protective actions including evacuation, shelter-in-place, and “run, hide, and fight”
- Host pre-incident planning visits to familiarize public safety with the site, buildings, and emergency protocols
- Conduct periodic exercises to familiarize personnel with emergency plans and to evaluate plans, procedures, capabilities, and resources

Workplace Violence Prevention

There are many policies and procedures that if implemented can reduce the risk of violence in the workplace. Anti-harassment and discrimination, substance abuse, business conduct, and electronic communications/computer use policies can help to eliminate behaviors and acts that cause workers to violently react to coworkers who they believe are bullying, abusing, or threatening. Any work environment that tolerates threatening or abusive behavior is at risk.

Related policies that establish an employer's right to access an employee's workplace computer, desk, locker, and other items may be necessary to investigate a credible complaint.

Risk factors that may expose employees to higher incidence of violence include working at night, working alone (on or off-premises), handling cash; and interacting with persons under the influence of drugs or alcohol. Workers in night retail establishments, healthcare institutions (especially emergency departments), and social services agencies are particularly at risk.

Circumstances or stressors such as an impending layoffs or organizational change that elevate tension, stress, or conflict in the workplace should be recognized and appropriate measures taken to mitigate risk.

Termination of employment can be the cause for workplace violence, so planning in advance may be warranted. Planning should begin with a threat assessment; provision of assistance for terminated employees to transition to the next phase of their life; and security measures during and following the termination meeting.

Establishing a threat assessment team to evaluate threatening behaviors and incidents

is a good practice and common in public schools and higher education. Suggested team members include human resources, security, legal, safety, union representative, employee assistance program (EAP) provider, outside mental health professionals, and law enforcement.

SIGNS OF POTENTIAL WORKPLACE VIOLENCE. Perpetrators of workplace violence may be current or former employees. Domestic disputes are also the source of workplace violence when the perpetrator goes to the workplace knowing that is where the victim can be found.

It's important to educate employees about the potential warning signs that may be exhibited by someone who could become violent. Employees should be instructed to contact their supervisor or human resources if they observe an employee exhibiting potentially violent behavior. The following behaviors may indicate a propensity for violence:⁵

- A history of threats or violent acts, including threats or violence occurring during employment and a criminal history suggestive of a propensity to use violence to project power and to control others, or as a response to stress or conflict.
- Threats, bullying, or other threatening behavior, aggressive outbursts or comments, or excessive displays of anger.
- Verbal abuse or harassment by any means or medium.
- Harboring grudges, an inability to handle criticism, habitually making excuses, and blaming others.
- Chronic, unsubstantiated complaints about persecution or injustice; a victim mindset.
- Obsessive intrusion upon others or persistent unwanted romantic pursuit.
- Erratic, impulsive, or bizarre behavior that has generated fear among co-workers.
- Homicidal or suicidal thoughts or ideas.
- A high degree of emotional distress.
- Apparent impulsivity and/or low tolerance of frustration.
- A fascination with weapons, a preoccupation with violent themes of revenge, and an unusual interest in recently-publicized violent

⁵ ASIS SHRM WVPI.1-2011, *Workplace Violence Prevention and Intervention*, ASIS International and the Society for Human Resource Management

events, if communicated in a manner that creates discomfort for co-workers.

- Any behavior or collection of behaviors that instill fear or generate a concern that a person might act out violently.

Life or work changes may also contribute to the state of mind of a person who commits a violent act. The following life or work changes were identified by the U.S. Department of Homeland Security⁶:

- Marginalization or distancing from friends and colleagues.
- Changes in performance at work.
- Sudden and dramatic changes in home life or in personality.
- Financial difficulties.
- Pending civil or criminal litigation.
- Observable grievances with threats and plans of retribution.

PRECAUTIONS FOR PERSONS WHO HAVE BEEN THREATENED. A workplace violence prevention program should establish procedures to protect employees who have taken out a technical restraining order (TRO) or who have been threatened. If the perpetrator subject to the TRO has a history of violence, the threat level is increased. At the security or reception desk, post photos of persons restricted from entering and a description of motor vehicles they are known to drive. Schools, day care centers, and operators of outdoor recreation area frequented by children may consider posting photos of registered sex offenders.

If the threat level is high because of a known threat, consider providing enhanced security at the beginning and end of business hours, which are the times when domestic assaults perpetrated in the workplace are statistically more likely to occur. Other strategies include relocating a threatened employee's parking spot to a more secure location, assigning the employee to another work location, or allowing telecommuting. Regulatory compliant and constant supervision of all child and day care facilities and control of all visitors should be provided.

⁶ *Pathway to Violence Warning Signs and What You Can Do*, <https://www.dhs.gov/sites/default/files/publications/dhs-pathway-to-violence-09-15-16-508.pdf>

Bombing Prevention

Suicide bombings are a frequent occurrence in war zones. A suicide bombing is a terrorist tactic where the perpetrator is actively engaged in killing or attempting to kill people in a confined and populated area, through the use of a concealed body-borne improvised explosive device (IED) or a vehicle-borne IED.

Physical and operational security to prevent an attack is the first line of defense. For properties that are open to the public, an awareness of the potential indicators of a suicide bomber may enable warning and intervention. Potential indicators of a suicide bomber include the following.⁷

- People wearing baggy or heavy clothing to conceal a device.
- Individuals sweating, acting irritable, or displaying other signs of nervousness or anxiety.
- Backpacks or packages held in an unusual or delicate manner.
- Wires hanging from or connected to clothing.
- Avoidance of security personnel or cameras.
- Hands kept in pockets or firmly gripping a switch-like object.

Emergency Planning to Protect Life & Property

Emergency plans should be established following national standards such as NFPA 1600 and applicable regulations. Plans should include protective actions for life safety, threat and hazard specific procedures, defined roles and responsibilities, lines of authorities, an incident management system, and the identification and assessment of required resources. Implementation of plans should be accomplished through training, drills, and exercises discussed at the end of this bulletin.

Protective Actions for Life Safety

The emergency operations plan should define actions to protect life safety from foreseeable hazards. Terminology for protective actions has changed over time complicating common usage and understanding essential to prompt action. Review and agree upon common terminology within your organization, with building man-

⁷ *Suicide Bomber Awareness*, Private Sector Advisory, Federal Bureau of Investigation, Department of Homeland Security

agement and tenants, and with public safety responders.

The three basic protective actions for acts of violence are:

- **EVACUATION** when there is a hazard such as a fire, bomb threat, or suspicious package inside the building and you must move to a safe location usually outside the building. “**RUN**” is the protective action to escape an armed perpetrator or active shooter inside a building.
- **LOCKDOWN** (“**HIDE**”) when there is an armed perpetrator in the building or believed to be inside, but a safe path to escape is not available. This option may also be referred to as “**SHELTER-IN-PLACE**.” The term shelter-in-place was originally used to describe protection from a hazardous materials release outside a building. The term may also be used to describe sheltering from any hazard outside.
- **COUNTER** (“*fight*”) when confronted with an armed perpetrator and you must take physical action to take down or distract a perpetrator to protect your safety or the safety of others.

A public-address system that can broadcast a warning throughout all buildings is essential. The system should be audible and intelligible throughout the building. Multiple persons should be able to broadcast a warning from multiple locations in the building as soon as a threat is detected. Keep in mind that the security desk at the front door may be the first target of the perpetrator.

If an armed perpetrator is inside a building threatening or actively using a weapon to harm people, occupants must be aware of their options:

“RUN” OR EVACUATE. If there is a safe path to exit away from an armed perpetrator, running is the best option. Individuals will have to assess whether the path between the location of the perpetrator(s) and the exit is clear. If there is no place to hide or lockdown protected from the perpetrator, then running may be the only good option.

When escaping a perpetrator, choose the best escape path using secondary exits, passageways through adjacent rooms, and windows. When running away from the building, seek a solid barrier and run in an evasive zig-zag path if under fire.

As you approach police, keep hands up and relay any information about the perpetrator.

Evacuees should assemble at a safe location away from the building—not at their assigned evacuation assembly point, which is in close proximity to the building. Accountability of evacuees will be difficult, but must be accomplished.

“HIDE” OR LOCKDOWN. Hiding from a perpetrator is a protective action often referred to as “lockdown.” Unlike evacuation, it is not safe for a team to direct the movement of building occupants to safety when an armed perpetrator is roaming the building. Rather, every person must be able to hear a lockdown warning and evacuate (“run”) or take cover immediately.

While in lockdown, occupants should hide within a room behind a locked or barricaded door. Turn off the lights, get down on the floor away from the entrance door and any windows, and remain silent to prevent the perpetrator from finding you. Remain “silent and invisible.” Use any phone silently and without allowing a lighted screen to disclose your location. Communicate the location of any injured and the description, location, direction of travel, and weapons carried by the perpetrator(s).

Everyone should be prepared to remain in lockdown for an extended period until police enter or a recognized voice sounds the “all clear.” Procedures should also address what to do when the fire alarm sounds, which can be activated by the perpetrator or when smoke detectors sense the discharge of a firearm.

“FIGHT” OR COUNTER. If unable to run and confronted by an armed perpetrator intent on harm, the remaining option is to fight back. Hit the attacker with whatever is available—throw books, scissors, backpacks, laptops, chairs, and other things. If in numbers, rush the attacker. Attack the perpetrator’s eyes and push the barrel of the firearm away. Charge the perpetrator from behind if possible, but low to knock him/her to the floor. When the attacker is disabled, run.

Civil Disorder & Rioting

Advance notice of scheduled events and awareness of spontaneous gatherings, demonstrations, and protests that could lead to civil disorder is essential to allow time to implement reasonable preparedness measures. Monitor the media,

social media, and advisories from public officials and law enforcement. The information gathered and intelligence developed will enable decisions regarding facility operations, preparedness activities, and response actions should the situation escalate to threaten employees or facilities.

Preparedness actions should include verification that all security measures are in place commensurate with the threat level and instructions from public authorities. Move anything outside that could be vandalized or used as a projectile inside. Motor vehicles should be relocated to a safe location. Fences, gates, and exterior doors should be locked and secure. Exterior lighting should be fully functional to illuminate all sides of the buildings. Where installed, window shutters should be closed and secured. Anything subject to vandalism should be moved, if possible, to a location that affords greater protection. Establish plans to close air intakes to prevent entry of smoke or riot control agents. Enable all security systems to detect and prevent unauthorized entry.

Enhance security staffing levels commensurate with the risk assessment. All two-radio and mobile telephone communications equipment sufficient spare batteries should be fully charged and available. Verify all fire protection, emergency power supplies and their fuel supply, communications, and warning systems are in reliable condition.

Plan for the arrival and departure of employees and visitors based on the risk assessment and instructions from authorities. Plan an alternate evacuation route or defend in place strategy should the disturbance disrupt or block an orderly evacuation. Inform employees about the current situation and how to receive official information regarding evacuation, alternate travel paths to approach or exit the building, and building closure.

Bomb Threats

Threat assessment is an important first-step when responding to a bomb threat. It will determine actions to take including the level of public safety response, the scope of the search, and whether or not to evacuate building(s). Each incident is unique and all circumstances must be

evaluated by the assessment team consisting of building management, security, and police.

Information gathered from whoever receives the threat is crucial. Bomb threat forms should be immediately available and information received by phone, email, verbal report, social media, writing on the wall, or rumor should be documented. Any evidence should be preserved for police.

Bomb Threat Risk Ratings

Low Risk Threats

- Lack realism and pose a minimum risk to the victim and/or public safety. The probable motive is to cause disruption.
- Threat is vague and indirect.
- Information in the threat is inconsistent, implausible, or lacks detail.
- Caller is definitely known and has called numerous times.
- Threat was discovered instead of delivered (e.g., a threat written on a wall).

Medium Risk Threats

- Threat has an increased level of realism and could be carried out, although it may not appear entirely realistic.
- Threat is direct and feasible.
- Wording in the threat suggests that the perpetrator has given some thought to how the act will be carried out.
- Threat may include indications of a possible place and time.
- No strong indication that the perpetrator has taken preparatory steps, although there may be some indirect reference pointing to that possibility.
- Indication that the perpetrator has details regarding the availability of components needed to construct a bomb.
- Increased specificity to the threat (e.g. "I'm serious!" or "I really mean this!").

High Risk Threats

- Threat is specific and realistic and appears to pose an immediate and serious danger.
- Threat is direct, specific, and realistic and may include names of possible victims, specific time, or location of the device.
- Perpetrator provides his/her identity.
- Threat suggests concrete steps have been taken toward carrying out the threat.
- Perpetrator makes statements indicating they have practiced with a weapon or have had the intended victim(s) under surveillance.

Massachusetts Bomb Threat Guidance for local police, fire, and school officials, 2014

In some jurisdictions, police and fire will not respond to bomb threats in private buildings unless a suspected explosive device has been found. Determine in advance the criteria for police and fire response to your facility.

RESPONSE ACTIONS. Dial 911 and request police and fire to initiate a threat assessment team response. Police will determine what resources including the Bomb Squad will respond. Explosive detection canines may be used for low, medium and high-risk threats at the discretion of the police threat assessment team and the K-9 handler.

Decide, with threat assessment team, on the action or combination of actions to take including whether to evacuate the entire building, part of the building, or shelter-in-place and whether a search will be conducted. The scope of the search is dependent on the threat assessment. Communicate the bomb threat to building occupants with instructions to evacuate or remain in place.

Suspicious Package

A suspicious item is any item (e.g., bag, package, vehicle, etc.) that is reasonably believed to contain explosives, an improvised explosive device (IED), or other hazardous material that requires a bomb technician and/or specialized equipment to further evaluate it. Examples that could indicate a bomb include unexplainable wires or electronics, other visible bomb-like components, and unusual sounds, vapors, mists, or odors. Generally speaking, anything that is **HIDDEN, OBVIOUSLY** suspicious, and not **TYPICAL (HOT)** should be deemed suspicious. In addition, potential indicators for a bomb are threats, placement, and proximity of the item to people and valuable assets.

Not all items are suspicious. An unattended item is an item of unknown origin and content where there are no obvious signs of being suspicious. Facility search or evacuation is not necessary. If a package is deemed "suspicious," the following action should be taken.

- Notify security that a suspicious package has been detected. Alert everyone in adjacent areas that a suspicious letter or package has been found and direct them to clear the area.

If the suspicious item is believed to be a bomb, evacuate the building.

- Anyone in contact with any powder or substance believed to have been released from the package should seek decontamination immediately and should segregate from others not exposed. Shut down the building's ventilation system if shutdown can be done safely.
- If possible, document the reasons for identifying the package as suspicious. Without making direct contact with the suspicious item, record all available information from all sides including name and address of addressee and sender, post office codes, stamps, and cancellation date, any other markings or labels found on the item, any other peculiarities (stains, tears, tape, flaps not glued). If possible, photograph from all sides without moving. Contact the addressee to determine if package was expected.
- If the package cannot be verified as legitimate within a reasonable period, notify police.

Business Continuity & Recovery

Acts of terrorism can have a significant impact on business operations locally and regionally with cascading impacts that can extend beyond international borders. Business impacts following the terrorist attacks of September 11, 2001 were felt around the world. Stock markets, businesses, and schools were closed; air travel was shut down; travel was restricted; and grief and fear affected many. Following the Boston Marathon bombings in 2013, access to buildings on the blocks surrounding the bombings were restricted. Businesses couldn't open. For many hours following the 2016 ambush shootings of police in Dallas, access to the streets and buildings around El Centro College were cordoned off.

A security perimeter is established by police where a crime is committed and maintained until the collection of forensic evidence and on-scene investigation is complete. Depending on the nature of the incident, the security perimeter could extend many blocks beyond the area where damage occurred and may remain in place for days following the incident.

BUSINESS CONTINUITY PLANNING: An act of violence is not a common scenario for business continuity planning, but it should be considered. Restoration of a building and planning for occupancy by skittish workers concerned about their safety should be addressed. Plans should address employees working from an alternate location and the provision of information, technology, and other resources required for essential business functions to continue at a minimally acceptable level.

EMPLOYEE ASSISTANCE & SUPPORT. Emotional trauma is widespread following an act of violence. Concerns about security will be common. The outpouring of support for friends and colleagues who are casualties needs to be supported. Grieving and healing must be addressed through counseling, memorials, and ongoing support. Resources available from employee assistance programs should be made available promptly and supported as long as needed.

Program Implementation: Establishing a Capability to Protect Life & Property

Most acts of violence occur without warning, so the amount of time to react is minimal. Further challenging response, a perpetrator on the move prevents trained staff from directing movement to areas of refuge. Everyone needs to understand their options and quickly decide whether to run, hide, or fight. Drills should practice evacuation (running), lockdown, and sheltering-in-place.

TRAINING. Everyone should be familiar with the sound of the fire alarm system, emergency voice communication system, or mass notification system used for warning purposes. Everyone should know the primary and secondary paths to an exit and their primary and secondary assembly areas.

Employees should assess their areas so they will know where and how to take cover if a "lockdown" warning is broadcast and where to go if there is an order to "shelter in place."

All persons should be informed to leave belongings behind when "running" and to raise hands and follow instructions of arriving law enforcement officers who at that time wouldn't know who is the perpetrator. The locations of shelters safely away from the building and the need to check in with a supervisor for accountability should be stressed.

Training should address discrete communications to relay information about the location, description, and weapons carried by perpetrators. The availability of wired telephones and any limitations on wireless communications should be addressed. Sharing of mobile telephone numbers to enable communicating information via text messages should be explored.

DRILLS. Adults learn by doing, so drills are an important learning tool. Evacuation drills are also required by many regulations. Design evacuation drills to challenge people to find a secondary exit, to test warning and notification systems, and to practice accounting for the safety of all evacuees. Use drills to practice broadcasting warning instructions and to evaluate the audibility and intelligibility of the warning signal and announcements.

Lockdown drills require only a limited amount of time and can be done in any weather. Prior to all drills, options should be reviewed, and the locations of exits and areas of refuge should be identified. Drills should reinforce the concept of seeking refuge, barricading, and hiding with lights out and devices silenced.

Engage public emergency services as much as possible. Drills are an excellent opportunity to work together. The presence of fire and law enforcement personnel adds realism to drills and helps impress the importance of drills.

EXERCISES. Exercises to familiarize personnel with plans for acts of violence are essential. The goals of these exercises should include defining roles and responsibilities; communicating lines of authority within the organization and with public emergency services; reviewing detection, alerting, warning, and communications capabilities, limitations, and interoperability; establishing incident command; familiarization with building layout and ingress and egress routes; access to video surveillance systems; and procedures for different types of incidents.

Tabletop exercises can review many of plans and procedures, but full-scale exercises are the best means of training personnel, evaluating capabilities, and practicing incident command.

Resources for Risk Assessment, Prevention, Deterrence & Plan Development

Links to many resources to help you develop, implement and evaluate your organization's preparedness program can be found on "[Links to Program Resources](#)" page ("Resources" menu) of Preparedness, LLC's website. Be sure to check out the Preparedness Bulletin titled "[Protective Actions for Life Safety](#)" and the program self-assessment checklist based on [NFPA 1600](#).

About Preparedness, LLC

Preparedness, LLC is a client-focused risk consulting company. Our mission is to safeguard people, protect property, minimize business interruption, and protect an entity's image and reputation. Our vision is to thoroughly understand each client's business and become a long-term, trusted advisor.

If you have questions, or need assistance with the development, implementation, or evaluation of your preparedness program, please contact us.

Subscribe to Preparedness Bulletins

[Click here](#) and sign up for our Preparedness Bulletins. You can unsubscribe at any time.

PREPAREDNESS, LLC

(781) 784-0672

INFO@PREPAREDNESSLLC.COM

[HTTPS://PREPAREDNESSLLC.COM](https://PREPAREDNESSLLC.COM)

© 2017 Preparedness, LLC

PREPAREDNESS