



***IFMA and IFMA Foundation would like to acknowledge and thank those who reviewed, edited and added their expertise to this document.***

Charles N. Claar, PE, CFM, CFMJ, International Facility Management Association

Paul Doherty, AIA, the digit group

L. Carter Farish, CFM, Grubb & Ellis Management Services Inc.

John Glenn, CRP, Independent Consultant

Richard D. Goulet, Hayes Mechanical Inc.

Richard N. King, Grubb & Ellis Management Services Inc.

Kathryn F. Klass, VeriSign Inc.

James E. Loesch, PE, CFM, Johns Hopkins University Applied Physics Laboratory

Peter B. Olinger, Lockheed Martin Missiles & Space Company

Timothy J. O'Malley, CFM, The O'Malley Group

Michael Stephens, VeriSign Inc.

John Sweat, Lockheed Martin Missiles & Space Company

This document was authored by:

Shari F. Epstein, Associate Director of Research,

International Facility Management Association



This paper was made possible by the support of the IFMA Foundation. Established in 1990 as a 501(c)(3) corporation, the Foundation funds research, education and scholarships. By increasing the body of knowledge available to facility professionals, the Foundation advances your profession and career potential.

© Copyright 2002 by:  
IFMA Foundation  
1 E. Greenway Plaza, Suite 1100  
Houston, TX, USA 77046-0194

ISBN 1883176-43-3

# Table of Contents

Overview .....	1
What is terrorism? .....	2
Who and what is at risk .....	2
Vulnerability Assessment .....	4
Physical Security Assessment .....	5
Bombs .....	6
Blast-Hardening	
Mail bombs .....	8
Biological agents .....	8
Biological agents introduced into air handling equipment from outside	
Biological agents introduced into facility by mail	
Chemical/hazardous materials .....	11
Civil Disturbances .....	12
Kidnapping/hostage situations .....	12
Fire .....	13
Power outage/blackouts .....	14
The human element .....	15
The importance of training .....	16
Final words .....	16
Appendix .....	17

# Overview

In an IFMA Web-based poll conducted shortly after the September 11 attacks, seven out of 10 respondents indicated they had disaster recovery and business continuity plans. However, only 26 percent claimed to have a terrorist response plan.

There are many sources available to assist facility managers in being prepared for an emergency, disaster recovery and business continuity plans. The appendix lists several for review. The purpose of this document is to encourage and assist facility managers to create or revise an anti-terrorist plan and terrorist response plan. This document is written for a broad audience, recognizing that it cannot provide a blueprint for every facility. Rather, it addresses measures an organization can do now that could potentially minimize vulnerability or damage should a terrorist choose to strike.

Many of the issues addressed by a terrorist response plan are the same as for an emergency response plan. Fire, explosions, power outages and even chemical and other threats can be the result of a terrorist attack, or they can be the result of an accident. The potential impact on a facility is the same regardless of the source of the threat. Until recently, you may not have included threats related to weapons of mass destruction (WMD) in your emergency response plans unless your facility conducted biological or nuclear research or used HazMat chemicals or explosives. What is presented here is a list of potential threats and how facility managers should prepare for them. This really is no different than preparing for a natural disaster such as an earthquake, flood, hurricane or an accident such as a train hauling hazardous chemicals that derails and burns near your facility. Only the source and intent are different. History has shown us that you never can be completely prepared for every emergency. However, history has also demonstrated that those with a well thought-out and rehearsed plan fare much better and recoup much faster than those who are not ready. As a facility manager, your job is to be ready.

It will take the commitment and support of upper management to create such a plan, but with the events of September 11 still reverberating, most senior managers have moved safety and business continuity to a higher priority. According to a recent PR Week/Burson-Marsteller CEO survey, 81 percent of U.S. chief executive officers acknowledge that their existing crisis management plans were inadequate to handle the myriad of issues arising from the September 11th tragedy. In the past, companies were reluctant to spend money on non-revenue efforts such as business recovery planning in a slow economy, but many are rethinking their approach.<sup>1</sup> The plan must be part of the strategic business plan and must be budgeted appropriately. Those with a solid understanding of the facility, its operations, resources, equipment and personnel are the ideal candidates to create a terrorist plan. Engaging a consultant knowledgeable in anti-terrorism is recommended, for the consultant can help in identifying gaps in the plan.

---

<sup>1</sup> Bob Tedeschi, "Picking up the Pieces," Ziff Davis Smart Business, December 2001/January 2002, 78

## What is terrorism?

The U.S. government defines terrorism as “premeditated, politically motivated violence perpetrated against noncombatant targets by sub national groups or clandestine agents, usually intended to influence an audience.”<sup>2</sup>

“Terrorism is perpetuated by individuals with a strong commitment to the causes in which they believe. An action in one location often brings reaction in another, although not necessarily a coordinated one. The web-like nature of terrorism underscores the need for vigilance in counteracting terrorist groups.

The (1993) bombing of the World Trade Center was a watershed event. It taught us in a painful but unmistakable way that international terrorism can and does occur in the United States.”

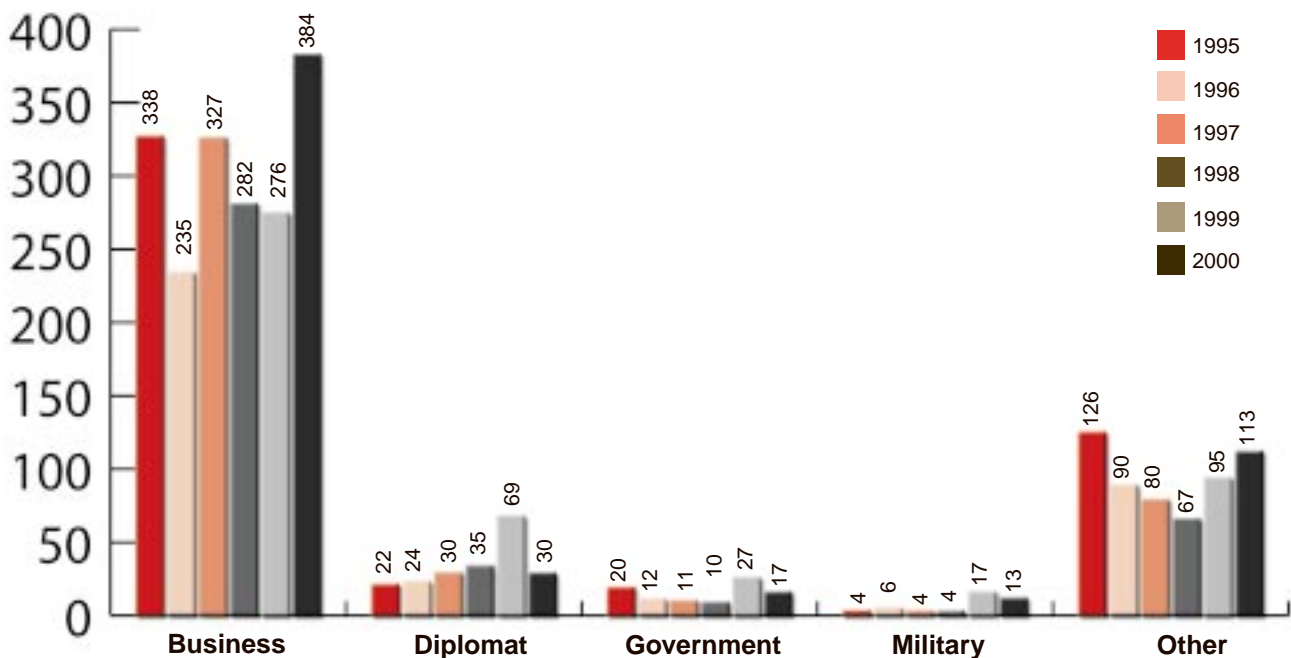
*Dale Watson, Chief International Terrorism Section, National Security Division, FBI Statement given to Senate Judiciary Committee, February 24, 1998*

These statements were made three years before the events of September 11, 2001 unfolded. In recent years, terrorist attacks have become more lethal, with the intent to kill as many people as possible. Until recently, guns and conventional explosives were the predominant weapons. But it can't be ignored that terrorist groups may have acquired access to chemical, biological, radiological or nuclear materials (weapons of mass destruction). However these weapons would be difficult to obtain and use by a non-state sponsored terrorist group.

## Who and what is at risk

The charts, furnished by the U.S Department of State, track international terrorism attacks for the past six years.<sup>3</sup> One of the most striking facts derived from these charts is that business facilities are targeted for attack significantly more often than military, government or diplomatic facilities. Latin America and Western Europe were the regions subject to the most attacks. Bombing is the crime most often perpetrated.

### Total Facilities Struck by International Attacks, 1995-2000

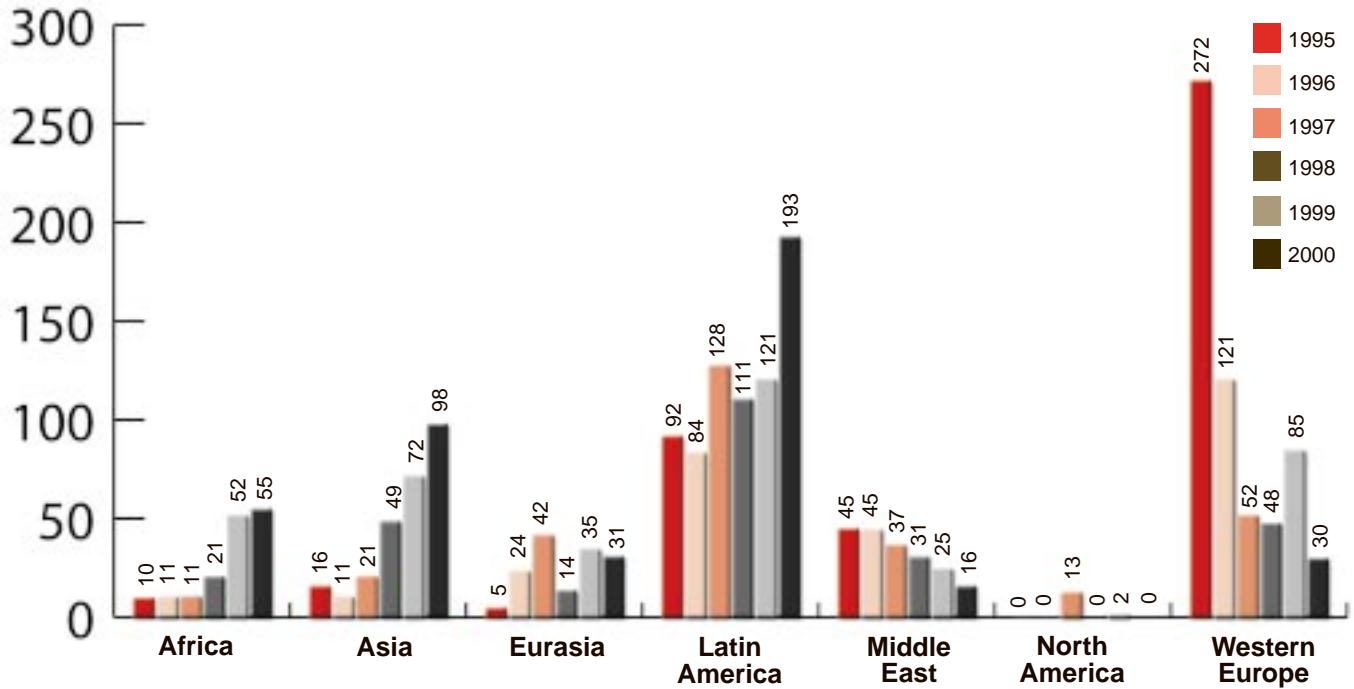


*Patterns of Global Terrorism – 2000, Released by the Office of the Coordinator for Counterterrorism, U.S. Department of State, April 2001*

<sup>2</sup>Title 22 of the United States Code, Section 2656f(d)

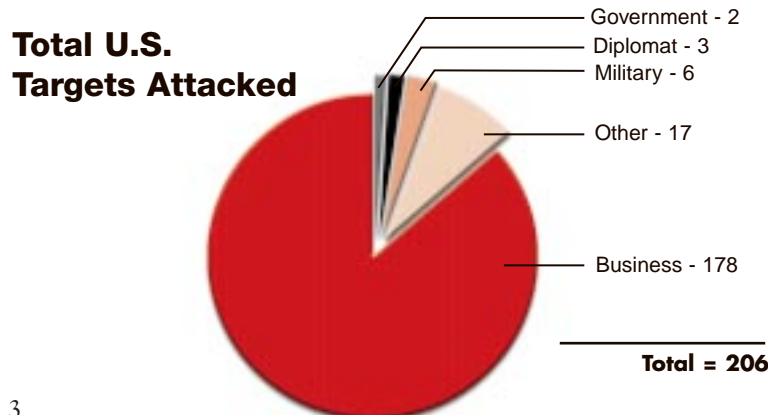
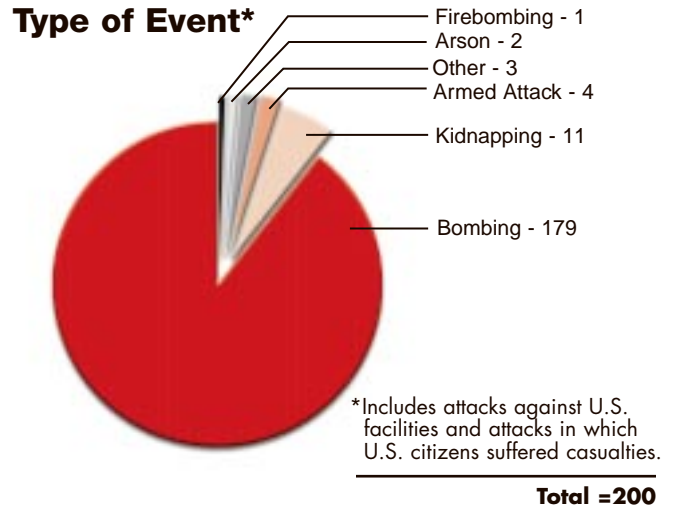
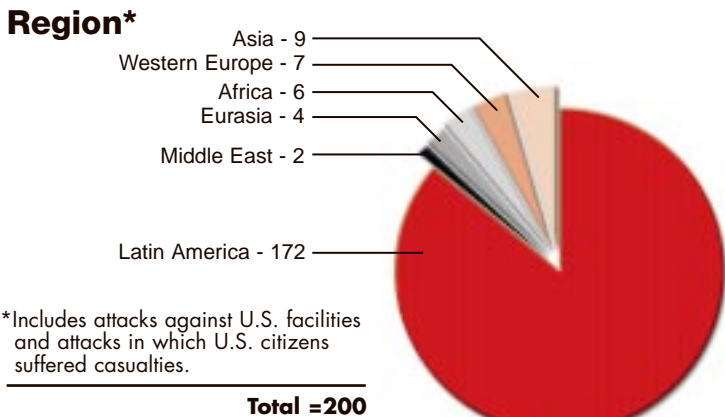
<sup>3</sup>U.S. Department of State, Office of the Coordinator for Counterterrorism, Patterns of Global Terrorism – 2000, (Washington D.C. , April 2001)

## Total International Attacks by Region, 1995-2000



*Patterns of Global Terrorism – 2000, Released by the Office of the Coordinator for Counterterrorism, U.S. Department of State, April 2001*

## Total Anti-US Attacks, 2000



*Patterns of Global Terrorism – 2000, Released by the Office of the Coordinator for Counterterrorism, U.S. Department of State, April 2001*

After the September attacks, we became more cognizant of international terrorism, but what about domestic terrorists? Domestic terrorists represent a variety of causes including social, political and economic concerns. There are right-wing extremists who support anti-government and racial supremacy and left-wing extremists who embrace revolution, anarchy and socialism. There are also special interest extremists who conduct violent acts to change attitudes about their causes such as animal rights, anti-globalization, pro-life, environmental and anti-nuclear. In a May 2001 report to U.S. Senate committee, Dale Watson reported there were 12 known or suspected acts of terrorism in 1999. These included two separate acts committed by lone domestic extremists, eight acts attributed to animal rights and environmental extremists, one bombing incident carried out by separatists in Puerto Rico and one arson committed by possible anarchist or animal rights activist in Washington state.<sup>4</sup> In October 2001, the Animal Liberation Fund (ALF) broke more than 30 windows at a Bank of America facility in Long Island, N.Y. because the bank is a major investor in Huntingdon Life Sciences, a British firm. Earlier in the year, five Bank of New York offices and branches were damaged by a sister organization, Earth Liberation Front.

Some terrorists have targeted commercial buildings for economic gain as opposed to political gain. Terrorists have extorted protection money from building contractors, owners and tenants in Latin America and Ireland. In Nevada, a casino incurred more than \$12 million in damages from a homemade bomb when it chose not to comply with extortion demands.<sup>5</sup>

The implications for business and facilities are far reaching. While government must concentrate on critical infrastructures such as power and energy systems, telecommunications, transportation, banking, water supply, government and emergency services, corporations must take on the added responsibility to become vigilant and less vulnerable to attack.<sup>6</sup> Now is the time to make one's organization a less attractive target and revisit or create business continuity plans.

This document includes a vulnerability assessment, physical security assessment and a list of potential terrorist threats. For each threat, we have provided a checklist of preventive measures and steps that should be taken in the aftermath. Although there is a lot of discussion of the new terrorism (chemical, biological, nuclear and cyber attacks), most terrorist acts are committed using conventional weapons such as bombs and bullets. This document focuses more on the conventional threats.

## Vulnerability Assessment

The questions listed below are intended to help you determine your vulnerability to a terrorist act or other threats.

- Do you have a business continuity plan?
- Have you conducted a counter-terrorism exercise, bringing in the expertise of police, fire and EMT?
- Do you monitor the activities of political extremists in your area or industry?<sup>7</sup>
- Do you have a policy for negotiating with someone who makes a terrorist threat?
- Do you have an economic recovery plan should your organization be subject to a terrorist attack?
- Are you able to document a chronology of actions taken on behalf of those who respond to a terrorist threat or attack?
- If your site is unusable, do you have a contingency plan to relocate to another site?
- Are you a high-risk target such as a telecommunications, government, financial institution or international business?
- Are you near a high-risk target such as a financial center, power plant, government or international site, or a high visibility public target like a stadium or arena?
- Have you appointed a chain of command and developed individual incident response plans should your facility be threatened or attacked?

<sup>4</sup>The Threat of Terrorism to the United States, Louis J. Freeh, Director FBI, testimony before the United States Senate, May 10, 2001

<sup>5</sup>The National Academy of Sciences, "Protecting Buildings from Bomb Damage: Transfer of Blast-Effects Mitigation Technologies from Military to Civilian Applications, 1995

<sup>6</sup>Geary Sikich, "September 11, 2001 Aftermath: Seven Things Your Organization Can Do Now," available from <http://www.Disaster-Resource.com>

<sup>7</sup>Mark I. McNutt, "Vulnerability to Terrorism Evaluation," available from <http://www.Disaster-Resource.com>

## Physical Security Assessment

A good way to prevent terrorist threats to your facility is making it unattractive to perpetrators. Recognizing that not all facilities are the same, here are some basic suggestions to make your facility less vulnerable to attack.<sup>8</sup>

- Keep the facility well-lit, inside and outside.
- Install fencing or controlled access. Consider vehicle gates with retractable barriers and trenches that prevent vehicles from driving into the site.
- Restrict parking to at least 300 feet from building. If this is not possible, limit nearby parking to properly identified employee vehicles and keep visitor vehicles to a distance. If neither of these approaches is possible, consider installing special reinforcing film on windows facing parking areas. (See section on Bombs.)
- Install constructed and strategically placed light bollards to double as vehicle barriers at building entrances.
- Keep heavy shrubs and vines close to the ground, as they can conceal criminals.
- Eliminate window boxes or planters, for they can conceal bombs. If planters must remain, security personnel should check contents regularly.
- Fit ground windows, interior and exterior doors with good quality locks.
- Use security patrol outside and use closed-circuit television and or infrared cameras to monitor outside activity. Use motion sensors that mark the video recording and alert security when someone has entered a restricted area.
- Install a security alarm system and post signs regarding its existence.
- Monitor access control at loading and unloading areas.
- Install entrance/exit doors with hinges and hinge pins on the inside to prevent tampering. Make sure steel door frames fit properly.
- Keep doors to unoccupied offices, boiler rooms, conference rooms, supports spaces, computer rooms, electric switchgear rooms, elevator control rooms locked.
- Maintain a system for key accountability. Test keys regularly to verify they are keyed for correct door(s). Do not give out keys to visitors or outside service personnel.
- Require visitor sign-in, badges and escorts.
- Keep trash areas and dumpsters free of debris, for bombs can be easily concealed in trash receptacles.
- Monitor and clean common areas such as restrooms and stairwells. Cubicles, flower arrangements and artwork can also be used to hide bombs.
- Keep furniture in public areas to a minimum<sup>9</sup>
- Establish controls to either authorize or deny personnel, parcels and materials access to certain areas.
- Train occupants, security and maintenance personnel to look for people acting in a suspicious manner or objects out of place and establish a means to report such activity.
- Consider hiring a security consultant to assess security measures.

The following are more stringent security measures used by the U.S. Department of Defense and its contractors:

- Employee, visitor and contractor badges must be clearly displayed and worn at all times. Employee and other badges are clearly and readily identifiable by color, logo and shape. Train employees to challenge those without badges.
- Random inspection of briefcases, purses, packages and gym bags.
- Use of magnetometers, X-ray screening and explosive detectors.
- Foreign nationals, once cleared, are escorted throughout the property.
- Illegally parked vehicles are subject to immediate towing.
- Limited and documented access through controlled entrances using card-key/sign-in system.
- No personal packages are shipped through the mailroom.

---

<sup>8</sup>U.S. Department of Treasury, Bureau of Alcohol, Tobacco and Firearms, "Bomb Threats and Physical Security Planning," (ATF P 7550.2) (Washington D.C. 1987)

<sup>9</sup>Home Office, United Kingdom, "Bombs – Protecting People and Property, A Handbook for Managers," Fourth Edition, 1994

## Bombs

Even before the bombing of the World Trade Center in 1993, businesses have been subject to bombs and bomb threats. In addition to terrorists, perpetrators could be disgruntled or former employees or corporate spies. Terrorists rely on bombs, for they draw attention, are cheap and easy to assemble and are relatively risk-free to those who plant bombs. When targeting a facility, bombers assess the building's layout including vehicular and foot traffic in and out of the building. They seek facilities with minimal security and multiple entries and exits. Sometimes, if they can't penetrate the targeted facility, bombers have been known to detonate a bomb in an adjacent facility.<sup>10</sup> The pointers below are designed to help reduce the vulnerability to explosive devices of all types.<sup>11</sup>

- Develop a bomb incident plan. Contact local authorities to learn their procedures in handling a bomb threat. Find out if the public safety forces will assist in searching for a bomb. They may not be able respond due to sheer number of crank calls received and staffing limitations. Ask if they offer the services of dogs that are trained in bomb detection. Since you know your facility better than police, you may be asked to search first to see if anything appears suspicious.
- Designate a command center area, preferably in a communications center. Only those assigned should be allowed in the center, but designate alternates just in case. All personnel should be aware of their particular assignments. This is the center where decisions are to be made regarding which actions to take. The command center should have an updated floor plan and a checklist of possible places where bombs could be hidden, as this will assist the search unit. It may be helpful to keep floor plans that show work areas with occupants' names and telephone numbers.
- Train those who answer the phone to listen carefully and ask the right questions by using a form similar to the one included in the appendix. If possible, have another person listen in on the call by sending a secret signal.
- Establish a chain of command, as this will instill confidence and minimize panic. For those in multi-tenant buildings, each tenant should have a representative as part of the plan.
- Have an evacuation plan in place. All evacuation plans must include:
  - Designated routes and exits (primary and alternates)
  - A means of communicating with staff to steer them away from dangerous routes
  - A meeting point at least 1600 ft. (500 m) away from the building
  - A system of hall monitors, assembly monitors and buddies. Hall monitors are trained to know where exits are located and have access to two-way radios. Assembly monitors lead evacuees to the assembly point and maintain contact with hall monitors. The buddy system places employees into groups of four to ten people. Once evacuated, buddies account for each other at the assembly area. If a buddy is missing from a group, one should let the assembly monitor know, so he can contact others assembly monitors areas to see if the missing buddy has been evacuated. If the buddy is not found, assembly monitor should contact hall monitors to look inside for the missing person.<sup>12</sup>
- Train evacuation and search units for their specific roles and make sure they are in constant communication with the command center. Consider periodic use of training films and on-site presentations by local law enforcement specialists. If a danger area is identified, evacuate that floor and the floors above and below. The evacuation unit may also be used as the search unit. Search personnel must be trained and be familiar with any area where a bomb could be hidden. Once an area is searched, it should be marked as such. If a device is located, the evacuation team or search team should leave it alone and notify the bomb squad. If using hand-held radios to communicate, move out of the immediate vicinity to avoid operation of the device.
- Allow the professionals to remove or disarm a bomb. After identifying and reporting the danger area, block off the area. Make sure doors and windows are open to minimize damage and leave the building.

<sup>10</sup> The National Academy of Sciences, "Protecting Buildings from Bomb Damage: Transfer of Blast-Effects Mitigation Technologies from Military to Civilian Applications," 1995

<sup>11</sup> U.S. Department of Treasury, Bureau of Alcohol, Tobacco and Firearms, "Bomb Threats and Physical Security Planning," (ATF P 7550.2) (Washington D.C. 1987)

<sup>12</sup> John Glenn, "Crisis Management – The missing ingredient in many plans," available from <http://geocities.com/CapeCanaveral/8836/crisis.html>; Internet.

In the event of an explosion, the following will occur:

- The police and bomb disposal team will search the area for a secondary device.
- Police, fire and other EMT personnel will be brought in.
- Once the area is cleared and rescue operations are complete, the area of detonation becomes crime scene. It will need to be roped off in order to gather evidence.
- The area will be need to remain restricted for there could be falling glass, broken gas mains or exposed electrical wires.

## **Blast-Hardening**

To mitigate damage from bombs, blast-hardening is recommended. Blast-hardening refers to all measures used to reduce or eliminate the effects of an explosion. Hardening undoubtedly will cost more, whether the facility already exists or is in the design stage. Some of the costs include consulting, nonstandard design, nonstandard construction practices and purchase and use of unusual materials. When retrofitting a facility, one would also incur the cost of retrofit, relocation of subsystems, loss of space or the creation of buffer spaces.<sup>13</sup>

When designing a new facility, here are some considerations that will allow you to harden the facility against explosions:

- Locate vulnerable functions away from public traffic areas to minimize danger. Street frontages should be used for circulation as opposed to offices.
- Provide redundancy of vital systems such as switchgear, primary feeders, power generators, sprinkler mains and fire pumps.
- Create areas of refuge. Using horizontal exits, occupants can flee fire and smoke and move horizontally to a safe area that is protected by a fire barrier.
- Control or eliminate the storage of hazardous materials that could contribute to a fire caused by a bomb.
- Design elevator and stair shafts to resist smoke penetration by pressurization or compartmentation.
- Relocate potentially hazardous functions such as mail and freight handling to a remote location.
- Protect the facility from flying glass, often associated with bomb blasts. Glass shards resulting from flying and falling glass is the primary source of injury in bomb attacks.<sup>14</sup>
  - Consider applying a protective glazing with a high-performance rating (GSA/ISC Condition 2 or higher.) Thermally tempered glazing (TTG), which is designed for loads up to 30 and 40 psi, breaks glass into rock salt-size pieces causing less injury. Polycarbonate glazing, similar to what is applied to a car windshield, prevents the glass from breaking into small pieces, but it may turn the glass into large flying projectiles that could cause injury. Another option is applying Mylar film to glass; however, it may discolor the glass. It, too, could create large pieces of flying glass.
  - Apply transparent polyester anti-shatter film of at least 175 microns thick. Use 300 micron film for glass panes over 100 sq.ft. (10 sm) and ground floor window greater than 32 sq.ft. (3 sm). Film can not be applied to the patterned side of frosted glass.
  - Provide bomb blast net curtains to go with anti-shatter film.
  - Install blast resistant, laminated glass which can withstand high blast pressure without damage provided it is placed in a strong and rigid frame. It should be at least 7.5mm including a minimum of pvb interlayer thickness of 1.5mm.
  - Install blast resistant secondary glazing inside exterior glazing.

---

<sup>13</sup> The National Academy of Sciences, "Protecting Buildings from Bomb Damage: Transfer of Blast-Effects Mitigation Technologies from Military to Civilian Applications," 1995

<sup>14</sup>Home Office, United Kingdom, "Business As Usual, Maximising Business Resilience to Terrorist Bombings, A Handbook for Managers," 1999

Other precautionary measures:

- Implement a clear desk policy that requires papers to be stored in locked cabinets at the end of the day. This will reduce the loss of documents and confidential papers.
- Place covers over PCs, keyboards and other equipment when not in use.
- Back up data regularly and store away from facility. Also store vital documents, insurance policies, contracts with disaster recovery firms and listing of inventory or assets away from the facility.
- Review insurance policies to make sure they are current and cover all potential losses. Consider separate insurance policy for terrorism if not already included in current policy. Business interruption insurance could be beneficial as well.
- Keep vital information such as contact information for key staff members away from the facility.

The U.S. government offers a bomb threat standoff laminated card that describes terrorist bomb threats by threat description (pipe bomb to semi-trailer), explosives capacity (TNT equivalent), building evacuation distance, and outdoor evacuation distance. This card is available through the U.S. Government Bookstore at: <http://bookstore.gpo.gov>.

## **Mail bombs**

Mail bombs can arrive as parcels, padded envelopes or any other type of envelope. They are designed to kill or maim the person opening it, but they can also cause structural damage. Mail bombs rarely occur; however, if a suspected package should arrive, don't touch it. Instead, call the authorities. Here are some signs of suspicious packages.

- Excessive postage (suggesting that the object was not weighed by the Post Office or mailroom);
- Handwritten or poorly typed addresses;
- Incorrect titles;
- Title, but no name;
- Misspellings of common words;
- Oily stains, discolorations or odor;
- No return address;
- Excessive weight;
- Lopsided or uneven envelope;
- Rigid or bulky envelope;
- Protruding wires or aluminum foil;
- Excessive security material such as masking tape, string, etc.;
- Appearance of foreign style handwriting;
- Springiness in the top, bottom or sides;
- Visual distractions;
- Ticking sound;
- Marked with "Personal", "Confidential", "To be opened only by" or "Prize enclosed"; and/or
- Shows a city or state in the postmark that does not match the return address.

## **Biological agents**

Biological agents are organisms or toxins that can produce illness in people, livestock and crops. Because they are difficult to detect, it can take a while for evidence of a biological attack to appear. Signs of exposure to biological agents include individuals or groups feeling poorly, collapsing or experiencing sudden skin blisters, yet there is no obvious explanation or event such as a nearby chemical spill that would cause such a reaction.

Some potential biological agents include anthrax, cholera, ebola fever and small pox. For some agents, vaccines are available; others respond to antibiotics. Although it is difficult to culture, store and transport biological agents, facility managers should be prepared should they find their way into one's facility.

## Biological agents introduced into air handling equipment from outside<sup>15</sup>

### Preventive steps

- Secure equipment room. Access should be limited to known maintenance personnel. Maintenance logs should be kept. Use of electronic keys and other locks that are not easy to duplicate or break are recommended.
- Monitor the air to classify and quantify hazardous substances.<sup>16</sup> This can often be tied into some higher end energy management systems.
- Use surveillance to monitor outside air intakes if they are close to the ground. If biological agents were released into an air intake from outside, a properly designed system with efficient filters may provide some protection when the filters are maintained. The use of filters with filtration small enough to catch most air borne pathogens may require modifications and changes to the system.
- These filters may remove most of the viruses and bacteria, but a rapid detection system is recommended. For some agents, only HEPA filters would be effective, which are expensive and may not fit due to space constraints or fan motor horsepower requirements. Hire specialists to inspect ventilation systems.
- Keep the HVAC system clean to prevent the build-up of organic materials on the cooling coils and other moist areas within the system. Bacteria can feed on the organic material and multiply.
- Provide protective equipment including rubber gloves and shower stations. Test the stations on a regular basis. Make sure the users are trained properly and receive ongoing training for using protective equipment as necessary.
- Train employees how to deal with biological agents and apply first aid. Make sure follow up training is part of the plan.
- Establish contacts with the local police and fire departments and nearby hospitals. Obtain basic medical training (CPR, use of respirators, level one red cross safety training) for all building personnel.

### After the event

- Evacuate the building should one suspect there has been an infiltration of a bacteria or virus. Those inside should place a wet towel or cloth over their mouth and nose and leave the building immediately. Have an evacuation plan and various gathering places. When exiting, go 90 degrees perpendicular to the breeze.
- Administer medical assistance to those who may have been infected. Have medical assistance equipment available strategically placed in various spots throughout the building. Co-ordinate with neighboring buildings.
- Shut off fans and blowers and air intake and close outside openings. Have disconnect switches outside the fan room for safety. Only experienced personnel should be allowed to shut off the fans. Develop a plan to isolate areas of the system.
- Keep in mind that elevator shafts are very efficient ventilators. If a ventilation system is attacked, lock off the elevators if possible. Bring them to the first floor and get them ready for emergency personnel.
- Notify the local emergency management team, police, fire, hospital and the Center for Disease Control of the incident. This should be done by one of two people delegated to contact the authorities.
- Hire specialized services for clean up. Pre-screen and interview these contractors before an incident happens.
- Check records to see if perpetrator was internal. Disgruntled employees are responsible for more than 90 percent of efforts to damage a building or company.
- Purchase replacement protective equipment. Ask the local fire or Hazmat teams where they buy their equipment.
- Update evacuation plan. Insurance companies are good sources of information.
- Disinfect all surfaces including the inside of the HVAC system. Have this done by your specialty contractor only.

---

<sup>15</sup> Robert Baker, "BBJ Environmental Solutions, Inc. Offers Guidelines to Bio-Terrorism and Heating, Ventilating and Air Conditioning (HVAC) Systems," available from [http://www.bbjenviro.com/news\\_releases\\_101001.asp](http://www.bbjenviro.com/news_releases_101001.asp); Internet.

<sup>16</sup> Source: Disruption Threat: Biological Hazards. Contingency Planning & Management. Reprinted with permission from Witter Publishing Corp. Content contained on [www.ContingencyPlanning.com](http://www.ContingencyPlanning.com)

## Biological agents introduced into facility by mail

### Protective Equipment for Mailrooms<sup>17</sup>

#### Masks

The use of masks can help reduce the risk of inhaling anthrax spores. There are a variety of disposable and reusable masks fitted with an appropriate filter (P3) from which to choose. Choose a mask based upon suitability to the task, level of protection, face shape and physical condition. To provide protection, masks must be worn consistently.

#### Hand/Skin Protection

Make sure cuts and open wounds are covered with bandages. Anthrax can pass through minor cuts or abrasions. Gloves are helpful, but they must fit properly and be used consistently. Employees should be trained on how to put on and take off gloves. Keep in mind, some people's skin may be sensitive to latex gloves.

If a suspicious unopened letter or package arrives:

- Do not shake or empty the contents.
- Place the envelope or package in a plastic bag or other container.
- If a container is not available, use clothing, paper or your trash can. Do not remove the cover.
- Then leave the room and close the door, or section off the area.
- Wash your hands with soap and water to prevent any powder from spreading to your face.
- Call the police immediately and notify building maintenance.

What to do with an envelope with powder and the contents spills out onto the surface:

- Do not try to clean up the powder. Cover the spilled contents immediately with anything (clothing, paper, trash can).
- Then leave the room and close the door, or section off the area.
- Wash your hands with soap and water to prevent any powder from spreading to your face.
- Call the police immediately and notify building maintenance.
- Remove heavily contaminated clothing and place in a plastic bag or other container that can be sealed.
- Shower with soap and water as soon as possible

What to do if there is a question of room contamination:

- Turn off local fans or ventilation units in the area.
- Evacuate the area immediately. If evacuation is not feasible due to the evacuation route passing through the danger area, move occupants away from the danger area and wait for instructions from the authorities.
- Close the door or section off the area to prevent others from entering.
- Close all fire doors and windows.
- Call the police immediately and notify building maintenance
- Shut down air conditioning system, if possible.

For persons exposed to biological agents:

- Be calm and don't overreact. Among other things, a calm attitude slows down the body's ability to absorb chemicals. The first thing a responder will do is to tell someone to calm down.
- Do not touch eyes, nose or any other part of the body.
- Wash hands in soapy water.
- Isolate those exposed to the agent by evacuating them to an adjacent unoccupied room away from the hazard.
- Record who and how many may have been exposed.

---

<sup>17</sup> Home Office, United Kingdom, "Chemical Threats by Post," an amendment to "Bombs – Protecting People and Property, A Handbook for Managers," November 2001

## Chemical/hazardous materials

Chemical agents are poisonous gases, liquids or solids that have toxic effects on people, plants and animals. Hazardous chemicals are everywhere; some may even be located on premises already. Some chemicals, while harmless alone, when combined with another can be lethal, such as two cleaning agents, ammonia and chlorine. Separately, they are great cleaning chemicals, but combined, they are a lethal gas.

Chemicals can be scattered easily. Some attack humans; others can affect the food chain. Chemical weapons include mustard gas which burns the lungs, nerve agents such as Tabun and Sarin and VX, a powerful nerve dioxin. Terrorists could also use more commonly available chemicals such as chlorine or ammonia to attack a facility or an entire community. Unlike biological hazards, with which you may not notice the effects for a few hours to days, chemical contamination is usually instantaneous. If you walk into an area and suddenly you have a burning sensation on your skin or eyes, or your nose starts to run, or your eyes start watering, these could be signs of the presence of a chemical agent. Also look for discolored droplets or powder on the ground, plants or cars (check to see when the last rainfall occurred), an unusual smell, a fog, low cloud or smoke. Other signs include suddenly feeling faint or the appearance of skin blisters.<sup>18</sup>

If you suspect there has been a release of chemicals, immediately leave the area and seek help. Ensure that unnecessary people are moved away in a crosswind direction and denied entry. Avoid contact with others until seen by hazmat or fire fighter personnel. Be calm. Among other things it slows down the bodies ability to absorb chemicals. This is why the first thing a responder does is tell someone to calm down. You may need to establish a protective action zone, an area in which people can be assumed to be at risk of harmful exposure and may be in need of either in-place protective shelter or evacuation.

If you are responding to an emergency, walk up to the site. If you run you could be the next victim before you know it. If you have not received training in how to respond to these emergencies, then work on evacuation. If you have ever been to a hazmat site one of the first things that responders determine is how they are going to get out. Then they determine how they will decontaminate themselves upon exiting. Once they decide the plan, then they enter the building.

If possible, have the following information available for hazmat personnel:

- Time of the release;
- Quantity released;
- Color and odor of vapors and any health effects noted;
- Direction and height of any vapor cloud or plume;
- Weather and terrain conditions;
- Entry of material into the environment;
- Any actions initiated by on-site personnel.

Principles of decontamination<sup>19</sup>

- Expect a ratio of 5:1 of unaffected to affected casualties.
- Decontaminate as soon as possible.
- Disrobing is decontamination; top to bottom, the more the better.
- Water flushing generally is the best mass decontamination method. Showering is recommended whenever liquid is transferred from clothing to skin.
- After known exposure to liquid agent, first responders must self-decontaminate as soon as possible to avoid serious effects.
- Control access to the area until it is safe. Only those directly involved in emergency response should be allowed to enter.
- Arrange for ongoing site control, monitoring of the environment and compliance with state and federal regulations regarding disposal.
- Establish a time-line for when employees may return.

---

<sup>18</sup> Home Office, United Kingdom, "Chemical Threats by Post," an amendment to "Bombs – Protecting People and Property, A Handbook for Managers," November 2001

<sup>19</sup> U.S. Army Soldier and Biological Chemical Command (SBCCOM), "Guidelines for Mass Casualty Decontamination During a Terrorist Chemical Agent Incident," January, 2000

## Civil disturbances

Protest activities may be legal or illegal, depending on the situation. They are designed to attract attention, but they can also turn violent should rioting or destruction of property occur. A primary focus of security is to prevent intruders from entering the facility.<sup>20</sup>

### Preventive steps

- Establish alternate entrances and exits for occupants.
- Review current security measures and safeguards.
- Double check security around doors and windows.
- Protect critical areas (control rooms, docks, electrical equipment, boiler rooms, air intake, unit tanks, environmental treatment areas) and install panic alarms linked to security control.
- Meet in advance with law enforcement to learn what specific actions can be taken to remove demonstrators.
- Conduct drills.
- Review penal code to determine which actions are considered non-peaceful behavior.<sup>21</sup>
- Create a response plan that addresses crowd control in a non-confrontational manner.

### During the event

- Contact law enforcement.
- Seal off and protect critical areas.
- Work with police to remove non-peaceful demonstrators and move peaceful demonstrators to other areas such as parking lots and interior roads.
- Increase protective force.

## Kidnapping/hostage situations

If kidnapped or held hostage<sup>22</sup>:

- Remain calm, be polite to captors and cooperate.
- Keep in mind that there may be multiple captors. One captor may be used as a decoy to draw out security personnel to be neutralized by other captors.
- Don't draw attention to yourself with sudden body movements, verbal remarks or hostile looks.
- Discreetly observe the captors, making note of physical characteristics, voice, language and dress.
- Prepare yourself for possible verbal or physical abuse, lack of food, water and sanitary conditions.
- If allowed, read, sleep or write to occupy your time.
- Make mental notes of directions, time of transit, noises and other factors that may help to identify your location.
- Anticipate isolation and efforts to disorient and confuse you.
- Do not aggravate your captors.
- Do not get into political or ideological discussions.
- Attempt to develop a positive relationship with your captors.
- Eat what is offered to maintain your strength.
- If interrogated, keep in mind that terrorists will play "good guy/bad guy."
- If forced to present terrorist demands to authorities, state clearly that the demands are from your captors.
- During rescue, drop to the floor and be still. Don't make any sudden moves, and wait for instructions.
- Don't make derogatory comments regarding your captors should others still be held captive.

<sup>20</sup> Source: Disruption Threat: Civil Disturbances. Contingency Planning & Management. Reprinted with permission from Witter Publishing Corp. Content contained on [www.ContingencyPlanning.com](http://www.ContingencyPlanning.com)

<sup>21</sup> Synthetic Organic Chemical Manufacturers Association, "Site Security Guidelines for U.S. Chemical Industry," A Product of Partnership among American Chemistry Council, Chlorine Institute Inc., Synthetic Organic Chemical Manufacturers Association, October 2001

<sup>22</sup> The Joint Chiefs of Staff, "Service Member's Personal Protection Guide: A Self-help Handbook to Combating Terrorism," JS Guide 5260, July 1996.

## Fire

Many times fires will occur as the result of a terrorist attack such as a bomb. To minimize the effect of a fire, here are some preventive measures:<sup>23</sup>

- Install smoke detectors and test and change batteries.
- Install fire alarm that will notify the fire department and suppression systems.
- Make sure facility meets fire codes. Ask fire department to inspect.
- Conduct fire drills on a regular basis.
- Develop an evacuation plan and designate staff members to serve as fire marshalls.
- Review insurance for fire coverage.
- Create and enforce a no smoking policy.
- Install and regularly maintain sprinklers, fire hoses, fire extinguishers fire doors, smoke and fire dampers and fire resistant walls.
- Replace damaged electrical cords. Minimize use of cords into one electrical outlet.
- Allow sufficient space around heaters and copy machines for air to circulate.
- Store flammable liquids and materials in a secure, safe place.
- Keep vital information such as contact information for key staff members away from the facility.
- Maintain a listing of inventory or assets away from the facility.
- Establish a preferred status relationship with a qualified disaster recovery/restoration specialist.

After the event:

- Close off the affected area.
- Secure the area to provide protection of assets and set up a process to allow entrance only to those with proper authorization.
- Inventory all damaged areas and equipment. Estimate the cost.
- Document damage on video or other media.
- Determine structural damage; roof and floors may be damaged and subject to collapse. Have a registered structural engineer perform a structural damage assessment to determine if there have been distortions in structural columns, beams and slabs, fracturing of connections or spalling or cracking of concrete members. If such conditions exist, surveys should be done to determine extent on structural integrity.<sup>24</sup>
- Perform an assessment of both affected and unaffected areas to determine if contamination by fire by-products has occurred. Polyurethane foam when burned produces hydrogen cyanide. Poly vinyl chloride (PVC) when burned can create hydrogen chloride gas that can combine with water to produce hydrochloric acid. Other by-products include nitrates, sulfates, hydrofluoric acid and hydrogen bromide.
- Check for mold and mildew should there be standing water or humid condition for more than a day. Mold and mildew can affect the HVAC system, paper, magnetic media and building structure.
- Do not turn on the HVAC system, for it could spread asbestos and other dangerous particles. The HVAC system should be examined and decontaminated by a Certified Industrial Hygienist. This can be accomplished using a biocide.
- Check for contaminants in water. Inorganic salts and atmospheric particulate can be introduced into the water through a fire. Water will need to be analyzed for ionic content, acidity, suspended solids and organic content.
- Electronics should be examined and tested by experienced technicians who can determine if they still meet manufacturer's performance specifications. If there is thermal damage, it is highly unlikely the equipment will work. If there is just a little smoke damage, it may be okay to restore and use. If the equipment has been subject to a moist environment for longer than a day, corrosion will have occurred rendering the equipment obsolete.<sup>25</sup>
- Create a single point of contact who will allow occupants to be kept informed as to the status of the building. If possible, make arrangements for occupants to retrieve their personal belongings.

---

<sup>23</sup> Source: Disruption Threat: Fires. Contingency Planning & Management. Reprinted with permission from Witter Publishing Corp. Content contained on [www.ContingencyPlanning.com](http://www.ContingencyPlanning.com).

<sup>24</sup> Pat Moore, "Important Damage / Site Assessment", available from [http://www.strohlsystems.com/BCP/EssaysArticles/damage\\_assessment.asp](http://www.strohlsystems.com/BCP/EssaysArticles/damage_assessment.asp); Internet

<sup>25</sup> Pat Moore, "Important Damage / Site Assessment," available from [http://www.strohlsystems.com/BCP/EssaysArticles/damage\\_assessment.asp](http://www.strohlsystems.com/BCP/EssaysArticles/damage_assessment.asp); Internet

## Power outage/blackouts

This is the most common business interruption. Possible causes include severe weather, electrical equipment failure, human error and sabotage.

Preventive steps:

- Determine the length of the usual outage.
- Determine outage history for your facility. Keep in mind that some utilities do not count an outage of less than one minute as an outage.
- Determine legal requirements for emergency power.
- Determine your facility needs for standby power in addition to legal requirements. Consider priorities/load requirements with respect to length of time required. For instance, some computers can be shut down while others must remain operational.
- Determine how long you think you may require or want emergency or standby power.
- Determine prime mover fuel — natural gas or diesel.
- Construct adequate fuel storage facilities.
- Protect critical applications with UPS systems backed-up with generators.
- Size on-site generation equipment to handle existing load requirements and add capacity for growth.
- Determine load transfer sequence, the most critical loads should be transferred to standby power first.
- Test operation at least monthly.
- Train key electricians on all operational phases of load transfer and emergency generation equipment operation.
- Have backup generators available — either purchased or leased through a generator supplier open 24 hours a day — as a last resort.
- Construct access for easy connection of back-up generators to existing electrical system. A pre-wired transfer switch and external receptacle can save time in an emergency. Coordinate plug details with the generator supplier.
- Be sure electrical staff is trained to connect back-up generation to existing electrical system.
- Arrange for back-up fuel for generators should the outage last longer than expected.<sup>26</sup>
- Keep a stockpile of batteries and flashlights throughout the facility.
- Monitor and maintain all key electrical equipment for the facility. Since transformers 500 kVA and larger are not usually manufacturer stock items, consider purchasing spare transformation for critical loads or arranging with local utility for emergency lend/lease.
- Use battery-operated radios, cell phones and beepers.
- Maintain a current list of telephone numbers including local utility provider.

After the power outage:

- Determine if problem is confined to your facility or is local or regional in nature.
- Turn off all non-essential loads.
- Establish a load start-up procedure when returning to normal power.
- Decide if occupants should be sent home or relocated.

<sup>26</sup> Source: Disruption Threat: Power Outages. Contingency Planning & Management. Reprinted with permission from Witter Publishing Corp. Content contained on [www.ContingencyPlanning.com](http://www.ContingencyPlanning.com).

## The human element

A business can have a disaster recovery and business continuity plan and still not be able to survive. Why? Because management did not consider how an event or disaster can affect its employees, a company's most valuable and volatile asset. An incident like a bomb, fire, explosion or criminal act invades a worker's comfort zone. Often the result is stress and trauma. Even those who witness the event remotely or see other people suffering may experience stress or trauma. A good response plan incorporates human needs in its disaster planning. Here are some signs of a stress<sup>27</sup>:

Does the employee:

- Overreact to real or imagined criticism?
- Miss deadlines or arrive late?
- Have mood swings?
- Miss work?
- Have difficulty with assignments?
- Startle easily?
- Show signs of guilt?
- Seem irritable or are they unusually argumentative?
- Use poor judgement?
- Isolate himself/herself?
- Show fear or seem anxious?
- Seem unable to remember details or appear confused?
- Show a disinterest or disregard in work?

Keep in mind that stress is inevitable and it will not last. However, a good plan recognizes that everyone is affected and will need access to professional help such as a clinical psychologist. Some workers are more affected than others and may suffer from symptoms of post-traumatic stress disorder (PTSD). The symptoms may persist for months after the event. These are some common symptoms of PTSD<sup>28</sup>.

### Re-experiencing

One may feel they are experiencing the event again through flashbacks or nightmares. The event dominates their thoughts, causing symptoms such as panic attacks, excessive sweating, racing heart or rapid breathing.

### Avoidance

The survivor may choose to avoid situations that remind them of the trauma, sometimes forcing the person to remain house-bound. If one does encounter a reminder, it causes anxiety. Another form of avoidance is where the individual chooses to zone out; the person is physically there, but the mind is elsewhere.

### Hyperarousal

Trauma causes the body to go into overdrive. The respiratory, circulatory and digestive systems become hyper sensitive. People who suffer from hyperarousal are easily startled. Sufferers may become irritable and take out their anger on others. Hyperarousal also can lead to self-destructive behaviors such as alcohol and drug abuse.

---

<sup>27</sup> Dan Paulk, "A Post-Crisis Message to Managers - Do You Have a Troubled Employee?", available from [http://www.disaster-resource.com/articles/98px\\_9.htm](http://www.disaster-resource.com/articles/98px_9.htm); Internet.

<sup>28</sup> The Association for Advancement of Behavior Therapy, "Survivors of September 11, 2001 – Facts About Trauma: What to Expect and How to Get Help," <http://www.aabt.org/091101/public/trauma.html>; Internet.

## The importance of training

Many of the preventive measures discussed refer to proper training. All the best developed plans and procedures can fall apart without proper training and frequent drills and exercises. Onetime safety training is worse than useless. Keep in mind that staff turnover happens frequently, and not everyone is knowledgeable of the plan. Training must include everyone in the company, from administrative staff to executives. Although training and drills take workers away from their regular work, it can minimize damage later on.<sup>29</sup> Training helps everyone be aware of responding to an unfamiliar event and give some feeling of empowerment in an environment that may seem overwhelming.<sup>30</sup> Consider training all employees on basic life safety procedures including first aid, CPR, evacuation, assembly and accountability.<sup>31</sup>

Here is an example. What if a bomb threat is called in? The receptionist has a list of questions to pose to the caller and specific directions at her desk (see Appendix.) You have a bomb incident plan. But what if the receptionist is away from her desk and the call is redirected to someone who is filling in and has no training? This is not an uncommon situation. Furthermore, several other staff members who were trained as marshalls are out to lunch. And finally, several new hires have been added, but the transition has not been updated in the plan. This is a recipe for disaster. Good planners know to cross-train, plan for contingencies and conduct frequent exercises to detect any gaps in the plan.<sup>32</sup>

## Final words

The likelihood of your facility experiencing a terrorist attack is small, but considering the full array of natural and man-made disasters, something could happen. Think about this statistic attributable to the U.S. Department of Labor — 43 percent of businesses that experience a disaster never reopen.<sup>33</sup> Why put you and your facility at additional risk? Now is the time to create or revise your disaster and recovery plans. Once you have the plan in place, don't put it on the shelf. Make sure it remains updated and practice, practice, practice.

---

<sup>29</sup> John Glenn, "Crisis Management in Three Words," <http://www.global.continuity.com>; Internet.

<sup>30</sup> Douglas M. Henderson, "How American Business Can Respond," <http://www.Disaster-Resource.com>; Internet.

<sup>31</sup> Geary Sikich, "September 11, 2001 Aftermath: Seven Things Your Organization Can Do Now," available from <http://www.Disaster-Resource.com>; Internet.

<sup>32</sup> John Glenn, "Crisis Management in Three Words," <http://www.global.continuity.com>; Internet.

<sup>33</sup> Steve Davis, "Business Continuity Considerations for Research and Development Organisations," <http://www.global.continuity.com>; Internet.

## Appendix

### ACTIONS TO BE TAKEN IN THE EVENT OF A BOMB THREAT IS CALLED IN

Record the exact wording of the threat:

Record time of call: \_\_\_\_\_

#### ASK THESE QUESTIONS:

1. Where is the bomb right now?
2. When is it going to explode?
3. What does it look like?
4. What kind of bomb is it?
5. What will it cause to explode?
6. Did you place the bomb?
7. Why?
8. What is your name?
9. What is your address?
10. What is your telephone number?

RECORD TIME CALL COMPLETED: \_\_\_\_\_

IF CALLER ID IS AVAILABLE, RECORD NUMBER LISTED: \_\_\_\_\_

INFORM MANAGER

CONTACT THE POLICE

ABOUT THE CALLER:

Male  Female

THREAT LANGUAGE:

Well-spoken  Irrational  Taped  Abusive  Incoherent  Message read from script

CALLER'S VOICE:

Angry  Stutter  Slow  Squeaky  
 Calm  Rapid  Giggling  Slurred  
 Crying  Deep  Nasal  Accent\*\*  
 Clearing throat  Disguised  Lisp  Normal  
 Excited  Familiar\*  Hoarse  Muffled

\* If voice is familiar, whom did it sound like?

\*\* What type of accent?

BACKGROUND SOUNDS:

Street noise  Voice  Household noises  Phone booth  
 Clear  Factory machinery  Animal noises  PA system  
 Music  Office machinery  Static  Other\_\_\_\_\_

Was the caller familiar with the area?  Yes  No

Signature:\_\_\_\_\_

Print Name:\_\_\_\_\_

Date:\_\_\_\_\_

(Source: Adopted from *Bombs - Protecting People and Property*, Fourth Edition, Home Office and *Bomb Threats and Physical Security Planning*, Bureau of Alcohol, Tobacco and Firearms)

## Reference sources

### Books

Emergency Management Planning Handbook, Geary W. Sikich (1996) McGraw-Hill

Protecting Buildings from Bomb Damage: Transfer of Blast-Effects Mitigation Technologies from Military to Civilian Applications (1995) Committee on Feasibility of Applying Blast-Mitigating Technologies and Design Methodologies from Military Facilities to Civilian Buildings, National Research Council

### Web Sites

Contingency Planning & Management Magazine  
<http://www.contingencyplanning.com>

US Environmental Protection Agency  
<http://www.epa.gov>

FEMA - Emergency Training  
<http://www.fema.gov/em/training.htm>

The Emergency Management Institute provides independent study courses on disaster preparedness, disaster assistance, and hazardous materials are available for the general public from the Emergency Management Institute at no cost. Special seminars, workshops, and broadcasts are offered at no cost via satellite as part of FEMA's Emergency Education Network, called EENET.

Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP)  
<http://www.epc-pcc.gc.ca>  
Formerly Emergency Preparedness Canada (EPC)

Community Preparedness Web Site Project  
<http://www.prepnow.org/>  
Prepare Now was developed to provide free preparedness resources to nonprofits serving special-needs and high-risk clients. The majority of the information included here was developed by community-based organizations in areas affected by the 1989 Loma Prieta earthquake in Northern California. There is exceptionally useful information in 9 languages. For agencies, there is a short plan on how to Write An Agency Disaster Plan in Six Weeks.

EDEN  
<http://www.agctr.lsu.edu/eden/>  
Extension Disaster Education Network, is a collaborative multi-state effort by Extension Services across the country to reduce the impact of disasters.

Extension Disaster handbook  
<http://disaster.ifas.ufl.edu/>  
The Disaster Handbook Web is a Cooperative Extension effort. It covers disasters of all types and is an excellent resource. There is also a plain text version.

The Business Continuity Institute  
<http://www.thebci.org/>

American Red Cross  
<http://www.crossnet.org/>

Canadian Red Cross  
<http://www.redcross.ca/>

American Society for Industrial Security (ASIS)  
<http://www.asisonline.org/>

Association of Contingency Planners (ACP)  
<http://www.acp-international.com/>

Business Recovery Managers Association  
<http://www.brma.com/>

Center for Education and Research in Information Assurance and Security (CERIAS)  
<http://www.cerias.purdue.edu/>

Chemical Emergency Preparedness and Prevention Office  
<http://www.epa.gov/swercepp/>

Disaster Mental Health  
<http://ourworld.compuserve.com/homepages/johndweaver/>

Disaster Recovery Information Exchange (DRIE)  
<http://www.drie.org/>

Disaster Report Archive  
<http://www.eqe.com/publications/>

Disaster Resource Guide  
<http://www.disaster-resource.com/>

Disaster Resources  
<http://www.ag.uiuc.edu/~disaster/disaster.html>

DisasterPlan.com  
<http://www.disasterplan.com/>

Emergency Information Infrastructure Partnership (EIIP)  
<http://www.emforum.org/index.html>

Firewise  
<http://www.firewise.org/>

Global Continuity  
<http://www.GlobalContinuity.com/>

Information Security News  
<http://www.infosecnews.com/>

Insurance Information Institute  
<http://www.iii.org/>

International Association of Emergency Managers (IAEM)  
<http://www.iaem.com/>

International Center for Disaster Mitigation Engineering  
<http://incede.iis.u-tokyo.ac.jp/>

International Disaster Recovery Association  
<http://www.idra.com/>

International Facility Management Association (IFMA)  
<http://www.ifma.org/>

National Fire Protection Association (NFPA)  
<http://www.nfpa.org/Home/index.asp>

National Institute for Urban Search and Rescue  
<http://niusr.org/>

National Interagency Fire Center  
<http://www.nifc.gov/>

NGA Emergency Management Best Practices  
<http://www.nga.org/>

RiskINFO: Resources for Risk Management, Safety, and Insurance Professionals  
<http://www.riskinfo.com/>

Small Business Administration Disaster Assistance  
<http://www.sba.gov/DISASTER/>

The Natural Hazards Research and Applications Center  
<http://www.colorado.edu/hazards/>

The Safety Connection  
<http://www.safetydeck.com/>

U.S. Department of the Interior: Natural Hazards  
<http://www.doi.gov/nathaz/index.html>

U.S. Office of Homeland Security (OHS)  
<http://www.whitehouse.gov/homeland/>  
The new Executive office created 10/8/01 coordinates more than 40 federal agencies, has a \$25M budget, and administers \$40B emergency appropriations, with the support of the Homeland Security Council.

BIOTERRORISM- Federal Research and Preparedness Activities  
<http://www.gao.gov/new.items/d01915.pdf>  
Publication Date: Sep-01GAO-01-915  
Appendixes include: Biological Agents and Pathogens, Summaries of Selected Federal Policy and Planning Documents, Federal Response Plan With Terrorism Incident Annex, Presidential Decision Directives, U.S. Policy on Counterterrorism, U.S. Government Interagency Domestic Terrorism Concept of (3) the federal government's capabilities to respond to a domestic terrorist incident, (4) progress the federal government has made in helping state and local emergency responders prepare for a terrorist incident, and (5) progress made in developing and implementing a federal strategy for combating cyber-based attacks. This capping report updates and summarizes our extensive evaluations conducted in recent years of federal programs to combat domestic terrorism and protect critical infrastructure.

Centers for Disease Control, Bioterrorism Preparedness and Response - Home Page  
<http://www.bt.cdc.gov/>  
CDC Health Alerts, Advisories, and Updates. MMWR (Morbidity and Mortality Weekly Report)

US EPA Counter Terrorism Efforts  
<http://www.epa.gov/swercepp/cntr-ter.html>  
This Web site outlines the counter-terrorism efforts of the U.S. Environmental Protection Agency. It includes links to EPA offices involved in these efforts: the Chemical Emergency Preparedness and Prevention Office (CEPPO), the Office of Emergency and Remedial Response (OERR), the Office of Radiation and Indoor Air (ORIA), and the National Enforcement Investigations Center (NEIC).

Counterterrorism and Incident Response  
<http://www.llnl.gov/nai/rdiv/rdiv.html>  
This program focuses on the response phase. It develops technologies and capabilities to deal with WMD (Weapons of Mass Destruction) emergencies or terrorist incidents. We also serve as the Lawrence Livermore National Laboratory focus for local, national, and international emergency response to WMD incidents.



IFMA FOUNDATION  
Research • Scholarships • Education

1 E. Greenway Plaza, Suite 1100  
Houston, TX, USA 77046-0194