



Loss Control Department
Technical Information Paper Series

After the Flood:
*Safety Tips for
Business Owners*

Copyright © 1999 The Hartford Loss Control Department
TIPS Series S 970.026 Printed in U.S.A.

This document is provided for information purposes only. It is not intended to be a substitute for individual legal counsel or advice on issues discussed within. Readers seeking resolution of specific legal issues or business concerns related to the captioned topic should consult their attorney and/or insurance representative.

After the Flood: Safety Tips for Business Owners

TAKE IMMEDIATE STEPS TO ENSURE PERSONAL SAFETY. DO NOT ENTER A FLOOD-DAMAGED BUILDING WITHOUT ENSURING PROTECTION FROM COLLAPSE, ELECTROCUTION, HAZARDOUS MATERIALS, AND CONTAMINATION.

Cleaning up a flood-ravaged business—one of the first steps toward recovery—can be a difficult and disheartening task. It can also be dangerous. Here is information to help you get started—safely. The information presented here is mostly in checklist format, and follows this general outline:

- 1. Take Immediate Steps to Ensure Personal Safety**
- 2. Secure the Buildings and Utilities**
- 3. Identify Damage and Begin Clean-Up of Building Contents**
- 4. Decontaminate Buildings and Contents**
- 5. Ensure Worker Safety During Clean-Up**

Take Immediate Steps to Ensure Personal Safety

Before you can even enter your property to assess the damage and begin clean-up and repair, you must take steps to protect the health—indeed, the lives—of workers and volunteers who have come to help.

Before Entering A Flood-Damaged Building

- Remember that buildings that have been submerged or have withstood rushing flood waters may have suffered structural damage and could be dangerous.
- Before entering a building, check for structural damage. Don't go in if there is any chance that the building, or parts of it, may collapse. If you see damage, have a qualified person check the building before you enter.
- Never assume that water-damaged structures or ground are stable.
- Assume that all stairs, floors, and roofs, and overhangs are unsafe until they are inspected.

When You Enter A Flood-Damaged Building

- Once you are certain that the building is safe to enter, make sure the electricity is turned off at the meter or at the street before you enter. Determine that all electrical hazards are controlled.
- Enter the building carefully. Leave immediately if shifting or unusual noises signal a possible collapse.
- If the door sticks at the top, it could mean your ceiling is ready to fall. If you force the door open, wait outside the doorway in case debris falls.
- Check the ceiling for signs of sagging. Wind, rain, or deep flooding may wet plaster or wallboard. It is very heavy, and will be dangerous if it falls.
- Upon entering the building, do not use matches, cigarette lighters, or any other open flames, since gas may be trapped inside. Use an explosion-proof flashlight or chemical light stick to light your way.
- If you suspect a gas leak or smell gas, or if you hear blowing or hissing, open a window and leave the building and premises *immediately*. Call the gas company from a different location. Do not re-enter the building.
- Be aware of the possibility of electrical shock and the possibility of injuries caused by hidden sharp objects.
- Look out for animals, especially snakes. Displaced animals may seek shelter in your building. Seek the assistance of an animal control officer to remove unwanted animals.

Ensure Electrical Safety to Prevent Electrocution

- Turn off the power at the main breaker or fuse on the service panel (if you can reach these without stepping in water; otherwise, have your utility company disconnect the power at the meter. Take this important step even if the power is off in your community.
- Do not turn the power back on until electrical equipment has been inspected by a qualified electrician.
- Shut off the water.
- Never touch electrical equipment if the ground is wet, unless you are absolutely certain that the power is off.
- Stay well away from downed power lines and electrical wires, and report these to the proper authorities. Electrocution is a major source of deaths in flooded areas. Electric current passes easily through water and soil. You can be electrocuted even if you only *approach* a downed power line.
- Look for electrical system damage: sparks, broken or frayed wires, smell of burning insulation.
- Do not energize equipment that is, or has been, wet, until it has been properly dried, cleaned, repaired or restored, and inspected.

Take Steps to Prevent Fires

- Shut off gas at the main valve, if you are trained to do so; otherwise, have your gas company do this.
- Inspect storage and piping systems containing flammable liquids; repair leaks or damage as soon as possible. Provide supports and anchors for damaged or floating tanks and piping.
- Prohibit smoking. Post a fire watch until all fire protection systems are functional and normal operations are resumed.

Be Cautious About Hazardous Materials

Flood waters can dislodge tanks, drums, pipes, and equipment, which may contain hazardous materials such as pesticides, chemicals, or fuels.

- Do not attempt to move unidentified dislodged containers without first contacting the local fire department or hazardous materials team.
- If you are working in potentially contaminated areas, wear appropriate protective clothing and respirators.
- Thoroughly wash all clothing and parts of your body that may have come in contact with sewage or other contaminants or with hazardous substances or chemicals. Use soap and clean water. Use waterless sanitizers if uncontaminated water is not available.

Be Cautious About Contaminated Floodwaters

Floodwaters are often contaminated with biohazards (sewage, medical waste, animal waste and carcasses) or other hazardous materials (fuels, asbestos, farm chemicals, etc.). Flood-damaged buildings may also have damp areas where molds, mildews, and other organisms thrive.

- Assume that anything touched by floodwater is contaminated.
- Use appropriate personal protective equipment, including goggles, respirators, gloves, etc., if you must come in contact with flood waters.
- Make sure that all workers have current tetanus shots.

Getting Around Safely

- Emergency workers will be assisting people in flooded areas. You can help them by staying off the roads and out of the way. Keep listening to the radio for news about what to do, where to go, or places to avoid.
- Roads may still be closed because they have been damaged or are covered by water. Floodwaters often erode roads and walkways. Barricades have been placed for your protection. If you come upon a barricade or a flooded road, turn around and go

another way. Don't try to assess the depth of the water on a road. If the road is covered, *don't cross it*. Don't drive over low-water bridges.

- If your vehicle stalls, get away from it and get to higher ground. A car will float in as little as two feet of water. More people drown in their cars than anywhere else.
- Remember that standing water may be electrically charged from underground or downed power lines.
- Be careful walking around. Flooding may have caused familiar places to change, and steps and floors are often slippery with mud.
- Do not walk through flooded areas. As little as six inches of moving water can knock you off your feet.
- Stay away from areas subject to additional flooding, such as low areas, stream beds, and ditches.
- Stay on firm ground.
- Be especially careful at night or in dark conditions when it is harder to see flood dangers.
- Flooded areas can be covered with debris, including nails and broken glass. Flood waters and debris may hide live animals or animal carcasses, and flood waters are often contaminated with biohazards (sewage, medical waste, animal waste and carcasses) or other hazardous materials (fuels, asbestos, farm chemicals, etc.). Wear appropriate personal protective equipment if you must come in contact with flood waters.
- To reduce the risk of drowning; avoid working alone, and wear a Coast Guard-approved life jacket when you are working in or near flood waters.

Secure the Buildings and Utilities

Secure the Facility

- Post security guards to monitor your property and facilities, since alarm systems may not be functioning, and since buildings may have to be left open during salvage and restoration.
- Provide guards with names of staff or contractors who have permission to be at the site.

Inspect, Repair, and Restore Fire Protection Systems

Fire can pose a major threat to an already badly damaged flood area for several reasons: inoperative fire protection systems, hampered fire department response, inoperable firefighting water supplies, and flood-damaged fire protection systems. In addition, the presence of live electrical circuits and equipment, accumulated debris, and floating flammable liquids can increase the risk of fire. Workers and employers must therefore take extra precautions.

- Restore fire protection systems as quickly as possible. Flood waters can rupture flammable liquid tanks and piping and clean-up activities will generate large piles of debris, and the risk of fire is high.
 - Examine fire protection systems for physical damage.
 - Test sprinkler control valves to make sure they are in the “open” position. If valves are closed, check for broken or disconnected piping before you reopen them. Remove water and mud from valve pits.
 - Inspect for obstructions in yard mains and sprinkler systems, if open bodies of water have been used for suction.
 - Inspect supports and foundations around tanks and yard main systems; flood waters may have caused washouts.
 - Inspect and repair pumps, drivers, and controllers.
 - Replace fire extinguishers.

Inspect, Repair, and Restore Other Essential Safety Devices

- Replace all gas control valves, electric circuit breakers, ground fault circuit interrupters (GFCIs), and fuses that have been under water to avoid electrocutions, explosions and fires. Even if these safety devices appear to function after being submerged in a flood, they are unfit for continued use and cannot be repaired. They may eventually fail, causing electrocutions, explosions or fires.
- Have a qualified technician inspect other parts of gas and electric appliances that have been submerged (such as fans, motors, electric circuits, and venting systems) to ensure continued safe operation. Replace appliances if needed.
- Replace smoke detectors and carbon monoxide (CO) alarms that have been submerged.

Ensure Fire Safety During Clean Clean-Up and Restoration

- Be sure that the sprinkler system is inspected and fully functional before beginning any welding or hot work.
- Be sure to follow proper controls for welding and hot work repairs.
- Provide at least two fire extinguishers, each with a UL rating of at least 10A, at every cleanup job.
- Remove combustible debris as soon as possible.

Clean and Restore Electrical Equipment Properly

- Dry electrical equipment: Open equipment doors, pull out drawers, etc., to allow water to run out. Remove standing water with wet vacs. Use low pressure air to blow out trapped water. Use absorbent pads to take up water if needed.
- Remove water from under raised floors, such as in computer rooms.
- Unplug appliances and lamps, remove light bulbs, and remove cover plates of wall switches and outlets that got wet.

- If local building inspection code allows you to disconnect wiring from switches and outlets, do so and throw away the switches and outlets. If your building inspector says that you cannot disconnect the wiring, pull them forward, away from the wall, and leave them connected.

Identify Damage and Begin Clean-Up of Building Contents

Document the Damage

- Once it is safe to enter the building, make a preliminary tour of all affected areas. Wear protective clothing.
- Do not move equipment or other objects without documenting their location and condition.
- Use a Polaroid-type camera or video camera to record conditions of structure, equipment, and furnishings. Make sure images clearly record the damage. Supplement these with better quality photos when necessary.
- Make notes and voice recordings to accompany the photographs.
- Assign staff to keep written records of contacts with insurance agents and other investigators, staff decisions on retrieval and salvage, and costs associated with clean-up and salvage.
- Make visual, written, and voice records for each step of salvage procedures.

Begin Clean-Up

After the flood waters have subsided, start to clean and disinfect the building. However, don't work in or around any flood-damaged building until it has been examined and certified as safe for work by a qualified person.

- Remove standing water from the facility. Use a mop, squeegee, absorbent materials, or a wet/dry vacuum cleaner.
- Begin draining the basement in stages, about a third of the water volume each day. Pumping out water too quickly may cause structural damage.
- Provide air movement and control humidity. Keep the building cool.
- Remove as much mud as possible. Once you've checked the water system for leaks, hose down the inside of the building and its contents. It's best to use an attachment that sprays soap to wash and rinse the walls, floors, furniture, sockets, electrical boxes and other major items that got muddy.
- Clean and dry damaged equipment and property (take care of the most important pieces first). Take special steps with documents and computer files.
- Dispose of all debris properly. Follow all applicable regulations regarding hazardous wastes, disposal, and recycling. If necessary, contract with a hazardous waste firm for proper handling of hazardous materials.
- If necessary, contract with a disaster recovery consultant to complete the necessary cleanup and restoration.

Decontaminate Buildings and Contents

- Remove loose dirt and debris from affected surfaces, using a power hose.
- Use a combination of household bleach (1/2 cup bleach per gallon of water) and soap or detergent to wash down walls, floors, and other contaminated areas, including exterior surfaces.
- Keep the surface wet for 5-15 minutes.
- Rinse thoroughly with a power hose to remove any residue. This will eliminate fungal problems and their dangers.
- Follow directions on containers and take particular note of warnings. Do *not* mix cleaning compounds containing ammonia with bleach.
- Remove heating and cooling registers and ducts, then hose the ducts to prevent contamination from blowing through the ducts at a later date. After hosing duct work, wash with a disinfectant or sanitizer that is phenolic or pine-oil based. If ducts are in concrete or otherwise inaccessible, have them cleaned professionally.
- Discard clothing, carpets, upholstered furniture, and similar items if they cannot be cleaned and disinfected.
- Take immediate action to minimize the growth of molds and fungi.
 - Inventory all flooded areas so that every water-damaged area is identified, treated, and cleaned.
 - Remove and dispose of all wet ceiling tiles and drywall within 24 hours of water contact.
 - Remove and replace all drywall and insulation up to 12 inches above the water line.
 - Dry all wet light fixtures.
 - Replace water-damaged furniture, including wood, or clean it with a 10% bleach solution. (Note: be sure to verify that bleach will not discolor or damage surfaces before application. When in doubt, test in a small hidden area before general application.) Discard furniture made of or with particle board or pressed board. Treat fabrics as you would carpeting (see below).
 - Leave all cabinets and drawers open to facilitate air flow for drying. Treat surfaces of cabinets and drawers with the dilute bleach solution.
 - Remove and discard all non-essential wet files and paper. Remove essential paper to a location where it can be dried, photocopied, and discarded.
 - If a large amount of paper cannot be dried within 24 hours, rinse essential files with clean water and freeze them temporarily until proper drying can take place. (Freezing will prevent mold growth.)
 - Immediately remove as much water as possible from wet carpeting, using a water vacuum.
 - After wet vacuuming, shampoo the carpet with a 10% bleach solution twice within a thirty minute period. Begin shampooing immediately after wet vacuuming. Spot test an inconspicuous area before proceeding.
 - Rinse the carpet with clear water to remove the bleach, and ensure that the carpet is totally dry within 12-24 hours of treatment.

- If the carpet fades with the bleach solution, then dry the carpet immediately and treat it with an alternate biocide. Consult a public health official, microbiologist, or industrial hygienist to determine the right biocide.
- When any form of biocide (including bleach) is used, increase air circulation and ventilation.
- Use dehumidifiers and air conditioning to speed the drying process.
- If odors or complaints of health effects exist after the clean up, consult an industrial hygienist or environmental microbiologist to determine the need for bioaerosol testing.

Ensure Worker Safety During Clean-Up

Stress, Long Hours, and Fatigue Increase the Risks for Injuries and Illness

Continued long hours of work, combined with emotional and physical exhaustion and losses from damaged homes and temporary job layoffs, can create a highly stressful situation for flood cleanup workers. Workers exposed to these stressful conditions have an increased risk of injury and emotional crisis, and are more vulnerable to stress-induced illnesses and disease. Emotional support from family members, neighbors, and local mental health professionals can help to prevent more serious stress-related problems in the difficult months ahead. People working in all phases of flood cleanup can reduce their risks of injury and illness in several ways:

- Set priorities for cleanup tasks and pace the work over several days (or weeks).
Avoid exhaustion.
- Resume a normal sleep schedule as quickly as possible. Get plenty of rest and take frequent rest breaks *before* exhaustion builds up.
- Take advantage of disaster relief programs and services in your community.
- Be alert to emotional exhaustion or strain. When family members and neighbors are unavailable for emotional support, consult professionals at community health and mental health centers.

Be Ready to Provide First Aid

First aid, even for minor cuts and burns, is extremely important when exposure to waters potentially contaminated with human, animal, or toxic wastes exists. Immediately clean out all open wounds and cuts with soap and clean water. Most cuts, except minor scratches, sustained during flood cleanup activities will warrant treatment to prevent tetanus. If you are injured, contact a physician to determine the necessary type of treatment.

Provide Assistance to Employees and Their Families

- Employees may be stranded at your facility. Be prepared with food, water, blankets, transportation, radios, etc.
- Good communication is essential. Help your employees stay in touch with their families. Provide frequent updates about the status of the flood, community recovery, and your plans for recovery.
- If necessary, help your employees secure shelter, medical care, food, water, clothing, cash, transportation, disaster aid, etc., for themselves and their families. The recovery of your business depends on the availability of your workers.
- Provide information and assistance to help employees and their families deal with injuries or deaths, or with damage to their homes and property (see attached).

Provide Appropriate Personal Protective Equipment

For most work in flooded areas, you will need the following personal protective equipment: hard hats, goggles, heavy work gloves, respirators, and watertight boots with steel toe and insole (not just steel shank). Excessive noise from equipment such as chain saws, backhoes, tractors, pavement breakers, blowers, and dryers may cause ringing in the ears and subsequent hearing damage. If you are working with any noise over which you must shout to be heard, wear earplugs or other hearing protection devices.

Ensure Electrical Safety

Use extreme caution while working with electrical equipment, attempting to restore power, or clearing areas near downed power lines. These steps may save your life:

- Treat all power lines as energized until you have followed the required procedures for de-energizing and testing them with an appropriate testing device. Do not rely on "fuzzing" to determine if a power line has been de-energized.
- Verifying that a line is not energized may not ensure your safety. You must also ground lines on both the load and supply sides of the work area. Grounding is necessary to protect you from the hazards of feedback electrical energy from a secondary power source, such as a portable generator.
- When restoring power in underground vaults, added precautions are necessary to prevent explosions. As vaults containing electrical connections are drained or pumped out, and as connections are energized, potentially explosive gases may form. Follow appropriate regulations for working safely in confined spaces.
- When using gasoline and diesel generators to supply power, switch the main breaker or fuse on the service panel to the "off" position *prior to starting the generator*. This will prevent inadvertent energization of power lines from "backfeed" electrical energy from the generators, and will help to protect utility line workers from possible electrocution. If clearing or other work must be performed near a downed power line, contact the utility company to discuss de-energizing and grounding or shielding of

power lines. Extreme caution is necessary when moving ladders and other equipment near overhead power lines to avoid contact.

Be Cautious About Carbon Monoxide

Flood cleanup activities may involve the use of gasoline- or diesel-powered pumps, generators, and pressure washers. Because these devices release carbon monoxide, a deadly, colorless, odorless gas, operate all gasoline-powered devices outdoors and *never* bring them indoors. It is virtually impossible to assess adequate ventilation.

Prevent Musculoskeletal Injuries

Cleanup workers are at risk for developing serious musculoskeletal injuries to the hands, back, knees, and shoulders. Special attention is needed to avoid back injuries associated with manual lifting and handling of equipment or debris and building materials. To help prevent injury, use teams of two or more people to move bulky objects, avoid lifting any material that weighs more than 50 pounds (per person), and use proper automated-assist lifting devices.

Prevent Thermal Stress

- ❑ ***Heat.*** When clean-up takes place during warm weather, workers are at serious risk for developing heat stress. Excessive exposure to hot environments can cause a variety of heat-related problems, including heat stroke, heat exhaustion, heat cramps, and fainting. To reduce the potential for heat stress, drink a glass of fluid every 15 to 20 minutes and wear light-colored, loose-fitting clothing. Additionally, incorporate work-rest cycles into work routines, work during the cooler hours of the day, when possible, or distribute the workload evenly throughout the day. When air conditioning is unavailable, open windows and use fans.
- ❑ ***Cold.*** Standing or working in water which is cooler than 75°F (24°C) will remove body heat more rapidly than it can be replaced, resulting in hypothermia. To reduce the risk of hypothermia, wear high rubber boots, ensure that clothing and boots have adequate insulation, avoid working alone, take frequent breaks out of the water, and change into dry clothing when possible.

Ensure Safe Work in Confined Spaces

If you are required to work in a boiler, furnace, pipeline, pit, pumping station, septic tank, sewage digester, storage tank, utility vault, well, or similar enclosure, you should be aware of the hazards of working in confined spaces. Toxic gases, a lack of oxygen, or explosive conditions may exist in the confined area, resulting in a potentially deadly atmosphere. Because many toxic gases and vapors cannot be seen or smelled, never trust your senses to determine if safe entry is possible. *Never* enter a confined space, even to rescue a fellow worker, unless you have been properly trained! If you do not have the proper training and equipment, contact your local fire department for assistance.

Ensure That Only Trained Workers Operate Heavy Equipment

Only people who are properly trained should operate heavy equipment (such as bulldozers, backhoes, and tractors).

Be Aware of Agricultural Hazards

If you are involved in cleanup efforts on or near farms, you may face these additional hazards:

- ❑ *Confined Spaces on Farms.* Molding or fermenting agricultural materials in confined spaces may generate large amounts of toxic gases which could cause lung damage or death if inhaled. Turn on fans or blowers in silos and other storage areas at least 30 minutes before entering and leave them on while working. Never open an oxygen-limiting silo if heating is suspected. Also, never enter these areas alone, and always use a full body safety harness.
- ❑ *Respiratory Hazards.* Wet hay, grain, silage, compost, and other organic/agricultural materials often grow large amounts of bacteria and mold during warm weather. Breathing these organisms and the organic dust produced may cause lung disease. Use proper engineering controls, including adequate fresh air ventilation. When exposure to organic dust cannot be avoided, use NIOSH-certified air-purifying respirators with high efficiency particulate air (HEPA) filters to reduce the risk.
- ❑ *Fire Hazard of Stored Hay.* Wet hay will mold very quickly. The biological processes involved in the formation of bacteria and mold can cause the hay to undergo spontaneous combustion. Monitor wet hay for odors, hot and damp areas, and rising vapors. If you detect these hazards, remove the wet hay from the building.

Sources of Information and Assistance

American Red Cross (www.redcross.org)
Environmental Protection Agency (www.epa.gov)
Federal Emergency Management Agency (www.fema.gov)
National Electrical Manufacturers Association (www.nema.org)
National Institutes for Occupational Safety and Health
(www.cdc.gov/niosh/flood.html)
Occupational Safety and Health Administration (www.osha.gov)
Public Risk Management Association (www.primacentral.org)

This document is provided for information purposes only. It is not intended to be a substitute for individual legal counsel or advice on issues discussed within. Readers seeking resolution of specific legal issues or business concerns related to the captioned topic should consult their attorney and/or insurance representative.



Loss Control Department
Technical Information Paper Series

Preparing for and Responding to Bomb Threats and Letter Bombs

Copyright © 1999 The Hartford Loss Control Department
TIPS Series S 570.050 Printed in U.S.A.

This document is provided for information purposes only. It is not intended to be a substitute for individual legal counsel or advice on issues discussed within. Readers seeking resolution of specific legal issues or business concerns related to the captioned topic should consult their attorney and/or insurance representative.

Preparing for and Responding to Bomb Threats and Letter Bombs

Introduction

While bombings instigated by terrorists, vandals, or disgruntled employees are not a new phenomenon, an increased number of bombing incidents in recent years has heightened awareness of this threat to individuals, businesses, and the public well-being. Since it is impossible to predict if, when, where, or how a bomb or bomb threat might affect your facility, you must be prepared at all times to respond to a real bomb or a bomb threat.

About 5-10 percent of bomb threats involve real bombs. Targets include individuals, businesses, schools, and public or government facilities. Perpetrators may be motivated by revenge, vandalism, political or religious convictions, or mental illness.

The information presented here is intended to be used as a guide. For maximum protection, develop detailed emergency preparedness policies and procedures tailored to your facility. Work with police and other local officials to make best use of the resources in your community.

About Different Kinds of Bombs

A bomb is an explosive device capable of injuring and killing people and of damaging or destroying property and buildings when it is detonated or ignited. Most bombs are homemade and will likely be one of three types: explosive, letter, or incendiary.

Explosive bombs cause damage through fragmentation (like shrapnel), heat, and blast waves. Shrapnel may cause injuries or death to people nearby. Heat may also cause secondary fires. Blast waves can damage or destroy buildings or vehicles and kill or injure people. Explosive bombs may be planted in buildings or in vehicles.

Letter bombs (also called mail bombs or package bombs) are explosive devices in containers designed to look like letters or packages. The U.S. Postal Inspection Service reports that of 170 billion pieces of mail processed in a typical year, only a very few letter bombs—an average of 16—are reported or investigated. However, this number is on the increase. Because it is impossible for the Postal Inspection Service to inspect each piece of mail, mail recipients must assume a large share of the responsibility for protecting themselves against letter bombs. Letter bombs can often be identified by their odd shape or packaging, by the way in which the package is addressed, or by odd characteristics such as protruding wires or a strange smell (see letter bomb checklist in the appendix).

Incendiary bombs (also called fire bombs or “molotov cocktails”) cause fire without substantial explosion or blast. They generally consist of a fragile container (such as a glass bottle) filled with a flammable liquid (such as gasoline) with a source of ignition (such as a rag stuffed in the bottle to serve as a wick). They are easily and cheaply made, difficult to trace, and a favorite weapon of rioters and vandals.

A bomb may be a *straight bomb*, in which no attempt has been made to make the bomb look anything different than what it is; or it may be a *concealed bomb*, one that has been disguised to resemble some other object (such as a briefcase or package).

Bombs may be triggered by *time delay mechanisms* (can delay detonation from a few seconds to several months), *remote controls* (radio transmitter and receiving device), or *target (victim)-activated devices*, which rely on some action by the intended victim (e.g., opening a letter bomb).

Be Prepared for Bomb Threats at Your Facility

Take a proactive approach: be prepared. Do all you can to protect your employees, facilities, and other assets from damage caused by a bomb and from the loss of productivity caused by panic, evacuations, and media attention.

Develop an Emergency Preparedness Plan (EPP), which includes policies, procedures, and resources for preparation, response, and recovery from real and threatened emergencies. Include provisions for bombs and bomb threats. Appoint an Emergency Coordinator and an Emergency Response Team. Train security personnel to respond to bomb threats and situations. Keep employees, emergency responders, and community officials informed of your emergency preparedness plans so that affected individuals and organizations can act effectively should the need arise.

Develop a flow chart or procedure for how to deal with a bomb threat (see sample flow chart). For example, suppose that a bomb threat call is made to your facility’s switchboard operator. Following the predetermined plan, the operator gathers appropriate information (e.g., time of call, exact words of caller) and asks appropriate questions (e.g., “Where is the bomb? What does it look like?”). (See sample checklist.) The switchboard operator immediately notifies the Emergency Coordinator and the police department; the Emergency Coordinator activates the Emergency Preparedness Plan.

Establish procedures to authorize, initiate, and accomplish evacuation, sheltering, and personnel accountability. Hold evacuation drills regularly so that all occupants will be familiar with evacuation routes and routines.

Review security policies and procedures to ensure that bomb situations are taken into consideration. Establish effective security against bombs and bomb situations.

Review security against building and car bombs. Follow standard recommendations for physical and access security. Do not allow parking within 300 feet of the building. If this is not possible, allow only properly identified company or employee vehicles to park closest to your facility. Control traffic access to loading docks, etc. Screen all individuals entering the facility. Keep doors, windows, and other entrances shut and locked when not in use. Screen all packages and bags brought in by visitors and employees. Instruct all employees to report any suspicious individuals, behavior, vehicles, or packages.

Review security against letter bombs. Centralize mail facilities, and locate them away from other work areas. Train mailroom personnel to recognize and respond to suspicious packages. Provide training to non-mailroom staff in other departments who screen, sort, or distribute mail. Get a portable x-ray machine to screen suspicious packages. Instruct all employees to report any suspicious mail or packages, including special deliveries.

Ensure that your facility has an effective fire prevention and protection program. Practice good housekeeping to reduce fire risk; keep the facility clean and free from flammable and combustible materials.

What to Do When A Bomb Threat is Received

Assume that every threat is a real one, but don't overreact. Terrorists *want* to disrupt operations and cause panic.

Telephoned Threats. The person who takes the call and speaks to the caller should record as much information as possible. Use a bomb threat call checklist (see sample). Make every effort to keep the caller talking and on the line (so that the call might be traced). Notify a supervisor or co-worker that a bomb threat is in progress. Keep calm, listen to the caller, do not interrupt, and remain courteous. Ask the caller to repeat information, as a means of prolonging the conversation. Record all information gathered during the call, as well as any impressions of a qualitative nature.

Written Threats. Notify appropriate officials immediately. Save all materials from written bomb threats (envelopes, containers, phone notes, etc.). Do not handle these materials more than necessary, to preserve fingerprints or other evidence.

If a Threat Appears to Be Genuine. Engage the Emergency Preparedness Plan. Deploy the facility's Emergency Coordinator and the Response Team to their appropriate roles and responsibilities. Notify security, supervisors, and building management personnel, but no one else. Let the appropriate people contact the police, bomb squad, media, etc. The Emergency Coordinator will make decisions about what actions to take immediately (ignore the threat, evacuate immediately, search the facility, delay evacuation, etc.).

What to Do When a Suspicious Package is Received

- Notify supervisor and internal security.
- Call the Postal Inspection Service, who will send technicians to examine and possibly dispose of the item.
- Call the police.
- Photograph or videotape the item, or make a written description.
- Handle it as little as possible, both to prevent detonation and to preserve evidence.
- Store it in a remote but open place until officials arrive. Do not put it into an enclosed space (such as a drawer or cabinet) or under water.

Bomb Searches

Let the local bomb squad supervise and conduct any bomb search, accompanied by someone who is familiar with the building. Do not use radio communications during the search, as the radio signal might set off a bomb.

If a Bomb is Found

- Do not touch, move, tamper with, or attempt to detonate any bomb or suspicious object or package.
- Identify its exact location, and report this information to the appropriate personnel.
- Run a string or piece of tape from the bomb to the nearest building entrance so that bomb technicians can get to the bomb quickly and unaided.
- If necessary, place sandbags or mattresses *around*, never on, the suspicious object. Do not cover the object.
- Block off the danger zone, with a clearance of at least 300 feet around the suspicious object (this includes floors above and below).
- Open all doors and windows to minimize blast damage.
- Evacuate the building.
- Do not permit re-entry until the object has been disarmed or removed and until the building has been declared safe.

If a Bomb Explodes

- Activate the Emergency Response Plan.
- Evacuate survivors and injured people. Search for injured and dead. Account for everyone.
- Get medical attention for injured people.
- Initiate other emergency services (fire suppression, security cordon, etc.).
- Be alert for gas and water leaks, electrical hazards, falling materials, etc.
- Be extremely cautious entering a damaged building; collapse could occur.
- Notify proper authorities.

- Remember that there could be a second bomb in the area, set to go off where evacuees or emergency personnel may be congregating. Conduct a careful and thorough search for more bombs. Be alert for additional threats or other communication from the perpetrator(s).
- Preserve evidence. Take pictures, use a video camera, and make notes.
- Make sure that evacuees and survivors are kept available for interviews by appropriate authorities.
- Maintain security at the site to prevent looting and vandalism.

Evacuation Planning

Evacuation of employees and visitors from the facility is the first priority during an emergency. A bomb or bomb threat situation may require the evacuation of all or part of the facility.

Decisions about evacuation must be made only by a person who is authorized to do so, according to the facility's Emergency Preparedness Plan. This will probably be the Emergency Coordinator or his or her designate. To control panic, an evacuation must be carried out in a controlled manner under the direction of authorized personnel.

Evacuation and sheltering procedures should include information about conditions under which an evacuation is ordered, individuals responsible for ordering the evacuation, evacuation routes and maps, etc. Be sure to consider needs for transportation, shelter, water, and food.

Personnel accountability procedures should designate an assembly area (and alternate area) where personnel should gather after an emergency; include a head-count system; and establish procedures for accounting for visitors, customers and vendors.

Do not use elevators during a bomb threat evacuation, as elevators are likely places for bombs.

What NOT to Do in a Bomb Situation

Do not panic. Do not touch, move, tamper with, or attempt to open or detonate any suspicious package. Do not discuss what is going on; leave this to the person designated to communicate with the public and the media. Do not contact the media.

Communicating with Employees, the Public, and the Media

Your facility's Emergency Preparedness Plan should include procedures to alert and warn employees of emergencies. Employees should understand the types of communication methods that are in place within their organization (e.g., public address system). Each employee should know how to operate the equipment (e.g., how to activate alarms and fire extinguishers).

Your EPP should also include a notification flow chart for the Emergency Response Team and other EPP members. The notification chart can include:

1. Emergency Coordinator
2. Response Team
3. Senior management
4. Outside response organizations
5. Neighboring businesses
6. Employees' families
7. Customers
8. Media

Appoint a single person (with backup) to serve as your organization's spokesperson for dealing with the media and the public. No one else should discuss the situation with outsiders or the media. This policy ensures that only accurate, consistent information will be issued to the media and to the public.

Conclusion

Every individual, business, school, and public or government facility is vulnerable to bombs and bomb threats. Because bomb incidents are rare and unpredictable, it's tempting to regard the threat as one unlikely to affect your facility. However, effective planning and preparation could make all the difference in preventing or mitigating a disaster for your employees, your business, your property, and your community.

This document is provided for information purposes only. It is not intended to be a substitute for individual legal counsel or advice on issues discussed within. Readers seeking resolution of specific legal issues or business concerns related to the captioned topic should consult their attorney and/or insurance representative.

References

Bintliff, Russell L. *The Complete Manual of Corporate and Industrial Security*. Englewood Cliffs, NJ: Prentice-Hall, c1992.

Handbook of Loss Prevention and Crime Prevention, 3rd ed., ed. by Lawrence J. Fenelly. Boston: Butterworth-Heinemann, c1996.

Hofmann, Mark A. "Expert Tips to Defuse Mail Bomb Risks." *Business Insurance*, January 13, 1997, pp. 1, 44

Office and Office Building Security, 2nd ed., by Ed San Luis et al. Boston: Butterworth-Heinemann, c1994.

Pouzar, Ed. "Defusing Threats." *Public Risk*, October 1996, pp. 16-17.

Preparing for Emergencies: A Program for Business Survival. New York: American Insurance Services Group, Engineering and Safety Service, c1991.

Ryan, James H. "Before the Bomb Drops." *Management Review*, August 1995, pp. 39-42.

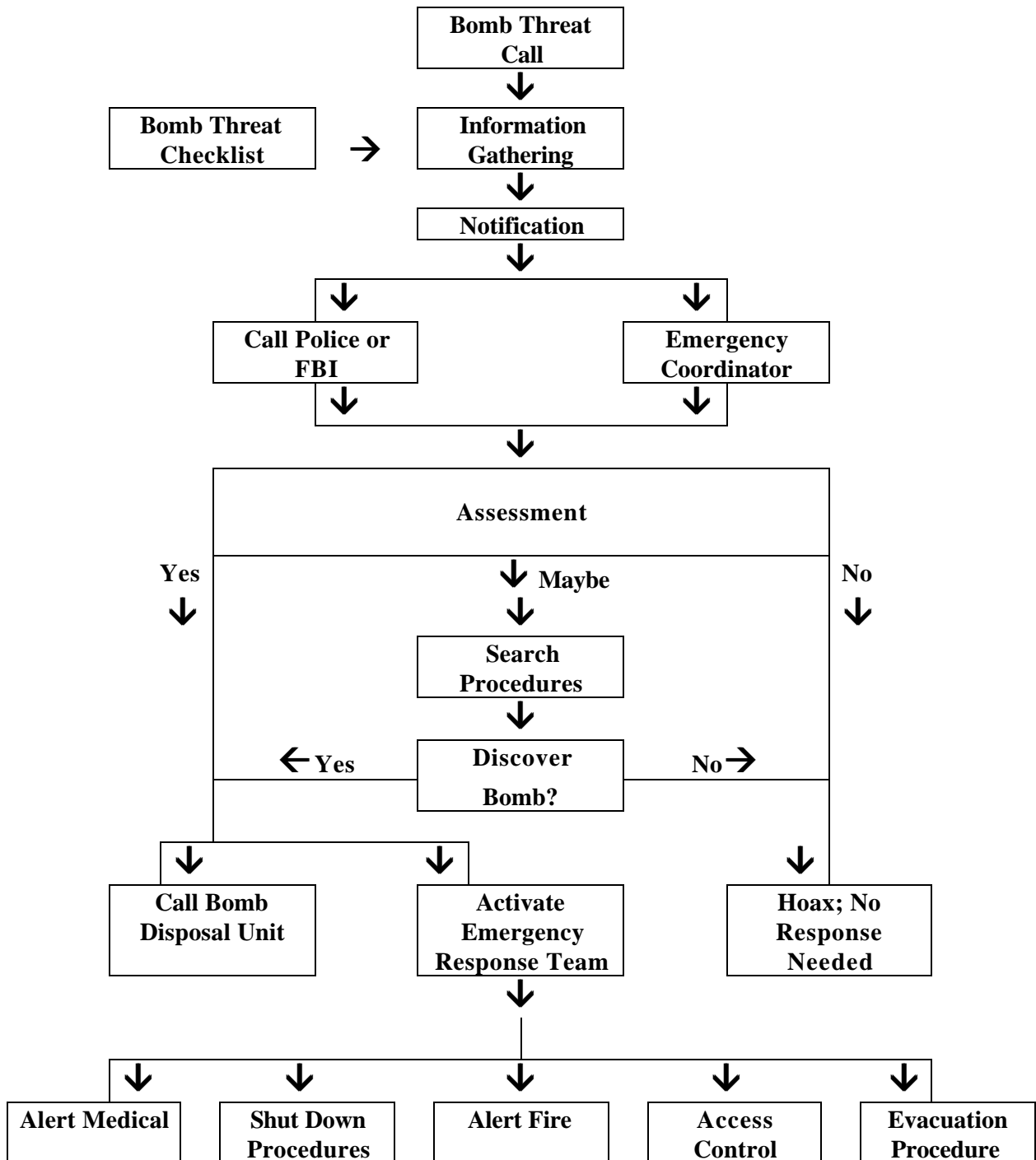
Security Manager's Handbook, 2nd ed. Waterford, CT: Bureau of Business Practice, c1989; revised c1992.

Siljander, Raymond P. *Introduction to Business and Industrial Security and Loss Control: A Primer for Public Law Enforcement and Private Security Personnel*. Springfield, IL: Charles C. Thomas, c1991.

Stringfield, William H. *Emergency Planning and Management: Ensuring Your Company's Survival in the Event of a Disaster*. Rockville, MD: Government Institutes, c1996.

Other information, especially about letter and mail bombs, was provided by the United States Postal Service and the Department of the Treasury (Bureau of Alcohol, Tobacco, and Firearms). Detailed information is available at the ATF's home page on the World Wide Web (<http://www.atf.treas.gov>)

Flow Chart for Response to a Bomb Threat



Source: Planning for Emergencies, American Insurance Services Group

Bomb Threat Checklist

Keep calm. Listen. Do not interrupt. Be courteous. Keep the caller talking. Ask the caller to repeat information. Record information. Notify a supervisor or co-worker that a bomb threat is in progress.

Exact time of call: _____ am _____ pm Date: _____ Day: M T W Th Fr Sa Su

Exact words of caller: _____

QUESTIONS TO ASK:

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

CALLER'S VOICE SOUNDED LIKE: (check all that apply)

Voice Qualities <input type="checkbox"/> Normal <input type="checkbox"/> Soft/Quiet <input type="checkbox"/> Loud <input type="checkbox"/> Slow <input type="checkbox"/> Rapid <input type="checkbox"/> Squeaky/High <input type="checkbox"/> Deep <input type="checkbox"/> Whispering <input type="checkbox"/> Shouting <input type="checkbox"/> Broken <input type="checkbox"/> Calm <input type="checkbox"/> Excited	<input type="checkbox"/> Nasal <input type="checkbox"/> Ragged <input type="checkbox"/> Raspy <input type="checkbox"/> Breathly <input type="checkbox"/> Cracking <input type="checkbox"/> <input type="checkbox"/> Caller is: <input type="checkbox"/> Male <input type="checkbox"/> Female <input type="checkbox"/> Adult <input type="checkbox"/> Child	Demeanor <input type="checkbox"/> Sincere <input type="checkbox"/> Disguised <input type="checkbox"/> Angry <input type="checkbox"/> Stressed <input type="checkbox"/> Sincere <input type="checkbox"/> Crying <input type="checkbox"/> Giggling <input type="checkbox"/> Laughing <input type="checkbox"/> Intoxicated <input type="checkbox"/> Righteous <input type="checkbox"/> Clears throat <input type="checkbox"/> Irrational	Accent <input type="checkbox"/> Accented <input type="checkbox"/> Local Accent <input type="checkbox"/> No Accent <input type="checkbox"/> Foreign: Describe accent? <input type="checkbox"/> Distorted <input type="checkbox"/> Familiar? Sounds like who?	Language <input type="checkbox"/> Uneducated <input type="checkbox"/> Educated <input type="checkbox"/> Distinct <input type="checkbox"/> Slurred <input type="checkbox"/> Stuttering <input type="checkbox"/> Lisp <input type="checkbox"/> Foreign Lang? <input type="checkbox"/> Foul Message <input type="checkbox"/> Spoken <input type="checkbox"/> Taped <input type="checkbox"/> Read
--	--	--	--	---

BACKGROUND NOISE SOUNDED LIKE: (check all that apply)

Surroundings <input type="checkbox"/> Office <input type="checkbox"/> Construction <input type="checkbox"/> Traffic <input type="checkbox"/> Party <input type="checkbox"/> Household <input type="checkbox"/> Kitchen	<input type="checkbox"/> Factory <input type="checkbox"/> Street <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Noises <input type="checkbox"/> PA System <input type="checkbox"/> Music <input type="checkbox"/> Machines <input type="checkbox"/> Bells <input type="checkbox"/> Static <input type="checkbox"/> Siren	<input type="checkbox"/> Quiet <input type="checkbox"/> Voices <input type="checkbox"/> Laughter <input type="checkbox"/> Animals <input type="checkbox"/> TV <input type="checkbox"/>	Telephone Call <input type="checkbox"/> Internal call <input type="checkbox"/> External call <input type="checkbox"/> Phone booth <input type="checkbox"/> Local <input type="checkbox"/> Long distance <input type="checkbox"/>
---	---	---	---	---

Name and position of the person who received and/or handled the call: _____

Call received at (location): _____

Call received at phone number: _____

Caller ID or similar ability? _____

Call reported to: _____

Call reported at (date and time): _____

Additional remarks _____

IMPORTANT PHONE NUMBERS:

POSITION OR AGENCY	PERSON TO CONTACT	PHONE NUMBER
Emergency Coordinator		
Emergency Coordinator Backup		
Security		
Local FBI Office		
Local US Postal Inspection Service		
Local Bureau of Alcohol, Tobacco, and Firearms		
Police		
Local Bomb Squad		
Fire Department		
Ambulance		
Mayor or other local official		
Hospital		

Responding to Letter and Mail Bombs

How to Recognize a Letter or Mail Bomb. *Letter bombs, also called mail bombs or package bombs, might display one or more of these elements, although not all may apply to every suspicious package:*

- mailed from a foreign country
- excessive postage; stamps versus metered mail
- no return address, or false return address
- postmark differs from return address
- restrictive or special handling instructions (“special delivery,” “air mail,” or “foreign mail”)
- misspelled words; poorly written or typed; poor handwriting; labels of cut-and-paste letters
- addressed to a specific individual
- wrong title with name of addressee, or addressed to a title but without a specific name
- restrictive instructions (“to be opened by addressee only,” “personal,” “confidential,” or “private”)
- addressee is not familiar with name and address of sender
- visual distractions (drawings, unusual statements, hand-drawn postage)
- letter-sized or larger package
- rigid, lumpy, or bulky envelope; stiffer or heavier than normal
- irregularly shaped or unevenly weighted package
- lopsided weight; soft spots or bulges
- messily wrapped package; different types of tape; excessive wrapping or taping; string
- marked “fragile,” “rush,” “handle with care,” or “do not delay”
- protruding wires, aluminum foil
- odd smells
- oily stains or discolorations

What to Do When a Suspect Package or Letter is Received

- Do not open any suspect letter or package.* Letter bombs may be triggered by a pressure release activated when the package is opened or when a string is cut.
- Isolate the suspect package, but do not put it into an enclosed space (such as a drawer or cabinet) or under water.
- Open windows in the immediate area.
- Contact police and other security officials immediately (bomb disposal unit, fire department, hospital, municipal officials, etc.).
- Activate the response team of the Emergency Preparedness Plan
- Make decisions about evacuation.

Security Against Letter Bombs

- Centralize mail facilities, and locate them away from other work areas.
- Train mailroom personnel to recognize and respond to suspicious packages
- Provide training to non-mailroom staff in other departments who screen, sort, or distribute mail.
- Get a portable x-ray machine to screen suspicious packages.
- Instruct all employees to report any suspicious mail or packages, including special deliveries.



Loss Control Department
Technical Information Paper Series

Continuity Planning for Computer Operations: *An Overview*

Copyright © 1998 The Hartford Loss Control Department
TIPS Series S 625.301 Printed in U.S.A.

This document is provided for information purposes only. It is not intended to be a substitute for individual legal counsel or advice on issues discussed within. Readers seeking resolution of specific legal issues or business concerns related to the captioned topic should consult their attorney and/or insurance representative.

Continuity Planning for Computer Operations: An Overview

Understanding the Need for Emergency Preparedness Planning

In a recent survey, half the risk managers surveyed reported that their organizations had experienced natural or human disasters. Were their facilities prepared for these events? Perhaps not. Despite the need, many risk managers fail to prepare adequately for emergencies. Consider these statistics:

- Fewer than 25% of American businesses have contingency plans.
- In the United States, 68% of business-affecting disasters are caused by human error; 25% by technology (hardware and software) failures; 5% by natural disasters; and 2% by intentional causes.

In terms of business survival, the results can be devastating...

- Of companies that experience a disaster but have no business recovery plan in place, 43% never reopen.
- Of 350 businesses operating in New York's World Trade Center before the 1993 bombing there, 150—that's 43%—were closed a year later.
- 70% of businesses that closed for a month or more failed to reopen, or failed altogether within three years.
- Most companies that must operate ten or more days without their computers will never fully recover.

...and the costs enormous:

- Within eight days of an extended computer outage, a company loses an estimated 2 to 3 % of its gross sales.
- 55% of organizations have experienced a disruption or inability to access computer systems for more than an hour, and 11% of large computer users report disruptions of a day or more.
- Three-quarters of businesses reach critical or total loss of functionality within two weeks of losing computer support.

Why Plan for Emergencies?

Disaster can strike at any time. Although most people think of disasters as naturally occurring events such as hurricanes or earthquakes, other events or conditions can have disastrous effects. Changes in how business is conducted can exacerbate emergency situations. The growing dependence on technology and the increasingly complex hazards of various manufacturing operations and processes increase the frequency, immediacy, and severity of disasters—both natural and technological—and contribute to the difficulty of recovery. In today's business climate, it is more important than ever to have a well-considered, comprehensive *Emergency Preparedness Plan* in place and ready to be activated.

How Can an Emergency Preparedness Plan Make a Difference?

Having an Emergency Preparedness Plan allows you to make decisions about how to proceed with emergency response and recovery *before* an emergency situation develops, when you are best able to make difficult decisions. Pre-planning allows for better prevention, better response, and better recovery. Should a disaster strike, the actions taken in the first minutes and hours can make all the difference to how soon—or *if*—normal operations can be resumed.

Without a plan, people will spend the initial precious minutes of an emergency situation frantically trying to decide what to do, who should do it, and what to tackle first. With a comprehensive plan in place, an organized, prioritized, *practiced* response can begin immediately, thus mitigating damage and perhaps even preventing loss of life.

In a recent survey, four of five risk managers reported that their plans had been effective during emergency situations. Another study showed that companies with disaster recovery plans experience an average disruption of four to six hours, whereas companies without such plans experience average disruptions of ten hours.

Although developing and implementing an effective Emergency Preparedness Plan can be costly and time-consuming, these costs are insignificant when compared to the potential losses a company must bear in the event of a major catastrophe.

What Is an Emergency Preparedness Plan?

An Emergency Preparedness Plan (or EPP) is the development, documentation, testing, evaluation, and implementation of policies, procedures, organizational structure, information, and resources that an entity can use to assess potential hazards, develop and prepare an appropriate response to each hazard, and develop and prepare strategies for recovery.

While Emergency Preparedness objectives may differ from one organization to another, they are almost always directed toward protection of people, protection of property, and preparation for the organization to resume productive operations as soon as possible.

An Emergency Preparedness Plan generally encompasses three areas:

- Emergency Preparedness** is the process of developing and defining roles and responsibilities, procedures, and resources for the Plan.
- Emergency Response** is the process of implementing the organization's policies, procedures, and actions to stabilize and control an emergency as it occurs and throughout its duration.
- Emergency Recovery** is the process of implementing the organization's policies, procedures, and actions to resume the organization's normal operation.

Why Computer Operations Should Be Covered by Your Organization's Emergency Preparedness Plan

For most companies, the information created, processed, and stored using computer systems is a vital corporate asset that must be safeguarded. This recognition, along with legislation implying executive accountability for business continuity, has led to an increase in the need for disaster recovery planning for automation hardware, software, and data. The increased functionality of automation equipment, increasingly widespread computer literacy, and innovative uses such as electronic commerce on the Internet, have made automation integral to success in delivering products and services.

However, *protection* of this valuable asset is often overlooked or only nominally considered when automation projects are initiated. This lack of foresight can make it difficult to backtrack to justify the costs of developing and maintaining disaster recovery plans at a later date. By developing a business contingency *strategy*, you will provide the framework for disaster recovery plans that integrate your business and continuity planning.

Roles and Responsibilities

Management must be involved at all levels to provide commitment, input, decisions, and approval. Technical support personnel are needed to provide information on hardware, software, and data requirements; to help plan the recovery process; and to assist with testing. Depending on the size of the company, one or more staff members may be dedicated to the development of the business impact analysis, disaster recovery plans, ongoing Plan maintenance, and periodic testing.

Getting Started

Ideally, planning for any automation project will incorporate business contingency planning. Include discussion of criticality, protection, and recovery of automation hardware, software, and data in planning for any project. Include costs for protection, mitigation, and disaster recovery in the project funding.

For many organizations, though, this planning has not been done. Typically, an organization will have a long-established mix of personal computers, distributed systems, and possibly a mid-tier or mainframe computer, that is somehow interrelated and constantly changing. There may be little or no documentation of the systems available. Since the development funds have probably been exhausted, there are no ready resources for emergency planning or recovery.

If your organization is in a similar situation, you can start the emergency planning process first by defining what is critical, and then by establishing what level of risk you are willing to accept. This is accomplished by conducting a risk analysis or business impact analysis.

Business Impact Analysis

An effective business impact analysis (BIA) will establish a clear picture of the critical functions or services that are dependent on computer automation that must be restored following an emergency. Since the BIA also serves to communicate to management the potential effect of emergency situations on automated functions, it can also be used to obtain management's commitment to provide the resources needed to accomplish disaster planning, or to confirm management's acceptance of the risk of *not* planning for disaster recovery.

In a business impact analysis, you will define and prioritize critical functions of the business, establish recovery time-frame requirements, and determine the computer automation necessary to support the critical functions. Thus, you can develop specific mitigation and disaster recovery plans appropriate to support the critical function requirements.

Develop Plans Specific to Your Needs

Depending on the size and complexity of your organization, one plan may cover all of your automation processes, or you may need separate plans for special needs. Individual plans may be required for the hardware (such as a distributed system or network communications environment) and the software (such as the operating platform, application software, and data repositories). You may even need to create separate plans for types of data repositories, such as hierarchical databases or relational databases, if they are handled by specialized units.

Preparedness

Prevention and protection are the best and most economical strategies for emergency preparedness. Effective protection of automation hardware, software, and data repositories prevents disasters *and* significantly reduces the *impact* of potential disasters. For hardware, simple measures such as surge protectors, battery backups, uninterruptable power supplies (UPS), physical security, and environmental control can provide basic prevention. Make backup copies of critical software and data on a regular basis, and store them offsite, along with equipment configuration files, current recovery plans, and documentation.

More complex preparedness strategies for hardware may involve backup generators, equipment redundancy, quick-ship contracts, vendor hot sites or cold sites, mobile recovery units, and/or reciprocal agreements. Data and software protection may include disk mirroring, shadow copies, image copies, incremental backups, access security, virus protection, and/or hierarchical storage techniques. Bear in mind that the increase in the cost of preparedness is generally exponential as you approach zero tolerance for down time.

Recovery

Develop plans for the recovery of automated processes and communication networks connecting all data processing environments. These plans must clearly document the hardware, software, and data requirements. A good plan will identify assumptions, recovery location(s), recovery and management teams, notification and contact lists, response procedures, recovery processes, minimum recovery requirements, and functions or services to be recovered. Develop an ongoing process for testing and maintaining the Plan. The management of the areas or functions supported by the Plan should review and approve the Plan in order to ensure its consistency with their expectations.

References

- DePompa, Barbara. "Disaster strikes! Are you ready?" *Information Week*, 527: 49-64, May 15, 1995.
- Devlin, Edward S., et al. *Business Resumption Planning*. Boston, MA: Auerbach Publications, c1997.
- Dunham, Ralph. "Are you ready for disaster?" *Computing Canada*, 23 (7): 32, March 31, 1997.
- Effgen, K. F. "Presenting the business case for a network-based disaster recovery planning program." *Telecommunications* 26 (11): 28, 30, November 1992.
- Winslow, Ron, and George Anders. "How new technology was Oxford's nemesis." *Wall Street Journal*, Col. 3, Pg. 1, Sec. B, Thursday, December 11, 1997.

This document is provided for information purposes only. It is not intended to be a substitute for individual legal counsel or advice on issues discussed within. Readers seeking resolution of specific legal issues or business concerns related to the captioned topic should consult their attorney and/or insurance representative.

Continuity Planning for Computer Operations: An Overview

Roles and Responsibilities

- Management must be involved at all levels to provide commitment, input, decisions, and approval.
- Technical support personnel will be needed to provide the hardware, software, and data requirements, to help plan the recovery process, and to assist with testing.
- One or more staff members may be dedicated to the development of the business impact analysis, disaster recovery plans, ongoing Plan maintenance, and periodic testing.

Getting Started

- define what is critical
- establish what level of risk you are willing to accept

Business Impact Analysis

An effective business impact analysis (BIA) can

- define and prioritize the critical functions or services that are dependent on computer automation that must be restored following an emergency
- establish recovery time-frame requirements
- determine the computer automation necessary to support the critical functions
- obtain management's commitment to providing the resources needed to accomplish disaster recovery, or confirm management's acceptance of the risk of *not* planning for disaster recovery.

Develop Plans Specific To Your Needs

- Determine the extent of planning needed for your organization. Depending on the size and complexity of your organization, one Plan may cover all of your automation processes. Separate Plans may be required for
 - hardware (such as a distributed system or network communications environment)
 - software (such as the operating platform, application software, and data repositories)
 - types of data repositories, such as hierarchical databases or relational databases, if they are handled by specialized units.

Preparedness

- Hardware protection measures (surge protectors, battery backups, uninterruptable power supplies [UPS], physical security, and environmental control)
- Software protection measures (make backup copies of critical software and data on a regular basis, and store them off-site, along with equipment configuration files, current recovery plans, and documentation)

Recovery

Develop plans for the recovery of automated processes and communication networks connecting all data processing environments.

- A good plan will identify:
 - assumptions
 - recovery location(s)
 - recovery and management teams
 - notification and contact lists
 - response procedures
 - recovery processes
 - minimum recovery requirements
 - functions or services to be recovered
- Develop an ongoing process for testing and maintaining the Plan.
- Request that management of the areas or functions supported by the Plan review and approve the Plan, in order to ensure its consistency with their expectations.

General Emergency Instructions

- Develop policies and procedures for all potential disaster scenarios, especially those that are likely to occur frequently, or those that could have a severe impact, such as:
 - heating, air conditioning, or power outage
 - medical emergency
 - communication line failure
 - hurricane, tornado, flood, earthquake, snow or ice storm
 - civil disorder, computer hacker, or bomb threat
 - fire or smoke emergency
 - water main break, sprinkler leakage, or sewage backup
- Create a contingency plan for “mutual aid” assistance from other companies or vendors.
- Formalize and stage practice exercises.
- Formalize a 24-hour emergency line of credit, for immediate access.

Continuity Planning for Computer Operations: Software and Network Protection

Inventory Controls

- Maintain a current inventory of all hardware and upgrades.
- Create a master log of DIP switch and jumper settings.
- Create a master log of miscellaneous cables, gateways, wire frames, and other equipment.
- Maintain a current inventory of all software and upgrades.
- Create a master log of software service packs, fixes, and order of installation.
- Log the configuration settings used for the installation of hardware and software.
- Store warranties, manuals, installation booklets, and other paperwork away from computer.
- Store original copies of software and upgrades away from computer.

Saving and Restoring Documents

- Make a copy first, then store originals and use the copy.
- Obtain as much RAM as you can afford on clients and servers.
- Enable “full auto saves” versus “fast saves,” for easier restorations.
- Enable “make back-up copy” whenever offered, to protect originals.
- Name and save documents immediately, to place working document into hard disk space.
- Re-save documents often, especially after many revisions.
- Copy documents onto sets of “copied” diskettes. If one fails, there is a second copy.
- Make regular “mini” backups of “my documents” or similar files.
- Use removable diskettes (e.g., ZIP, Jazz, TR tapes) for mini backups.
- Rotate mini backup media, and replace media at 80 percent use level.

Software And Data Duplication

- Use automated software to conduct daily incremental backups.
- Use automated software to conduct weekly full backups to be sure that all resources are covered.
- Rotate backups through a set cycle.
- Maintain at least three copies in rotation, with at least one copy stored off-site.
- Replace backup media at 80 percent recommended use, to avoid bad sectors, etc.

Storage of Software and Data Backup

- Place backups in U.L.-listed records containers.
- Store containers off-site at a location that is accessible 24 hours a day, 7 days a week.
- Ensure that off-site storage is environmentally conditioned and secured, allowing only authorized access.
- Ensure that off-site storage is far enough away so that it will not be affected by an area-wide disaster that may involve the company location.
- Clearly mark containers that have critical backups and documentation (e.g., use red containers).
- Rotate off-site backups.
- Use off-site backups when performing disaster recovery exercises.

Virus Protection

- Install virus protection software for network servers.
- Install virus protection software for client computers.
- Run background checking portion of virus software at all times.
- Automatically scan all disks, removal disks, and tapes at least weekly, (preferably nightly).
- Automatically scan all client computer hard disks at least weekly (preferably daily at logon).
- Automatically update virus protection software at least monthly.
- Scan all diskettes, removable media, CDs, and DVDs before use.
- Before using input from the Internet or electronic mail, load it to diskette and scan.
- Develop procedures for handling viruses, in order to limit their impact should they enter the system.

Software and Hardware Compatibles

- Develop software and hardware certification procedures.
- Always pre-test new software and hardware on non-critical PCs.
- Test, re-test, and test again, until there are no apparent conflicts.
- Develop a contingency fall-back plan *before* installation of changes to critical systems.
- Be ready for client and server “crashes,” and have backup drives ready “online.”

Internets, PPTP and VPNs

- Use encryption on Point to Point Transfer Protocols (PPTP) when using any ISP (Internet Service Provider) to connect to Virtual Private Networks (VPN).
- Use firewall and proxy servers to insulate your network from the Internet.

- Use encryption on E-mail, documents, teleconferencing, and Internet phone, when working with sensitive data.
- Block, or severely restrict access to, files, modems, printers, and faxes from Internet users.
- Use “Caller ID” services to identify hackers and password-cracker programs.
- Lock out hackers and password-cracker programs after three attempts.
- Change passwords at least quarterly, and require new passwords of 8 to 64 alphanumeric characters.
- Use private and public key encryption services whenever possible.

Intranets, LANS, and WANS

- Carefully control access to software, data files, printers, modems, and faxes within an Intranet.
- Change passwords at least quarterly, and require new passwords of 8 to 64 alphanumeric characters.
- Set company-wide system and user policies, and update them daily.
- Disable access by temporary or terminated employees, vendors, and customers.
- Lock down desktop software installation whenever possible.
- Create “read only” folders on Intranets.

Continuity Planning for Computer Operations: Hardware Protection

Hard Drive Maintenance and Upkeep

- Always make a full backup before performing hard drive maintenance.
- Clean out temporary files regularly.
- Clean out the “trash can” or “recycle” bin at least weekly.
- Clean out “trash cans” or “deleted items” folders in electronic mail programs.
- Archive and clean out calendar information at least twice per year.
- Run compression utilities for various programs that use “data bases,” at least weekly.
- Run basic “scan disk” (or similar software) at least weekly on all machines, or at startup.
- Run thorough “scan disk” (or similar software) at least twice a year to mark defective sectors.
- Run a hard disk defragmentation program at least monthly, to increase computer efficiency.

Hardware Duplication

- Contract for hot site, warm site, cold site, or mobile unit vendor services.
- Contract with hardware vendors for quick shipment of critical equipment.
- Check software contracts/licenses for clauses pertaining to use at alternate location during emergencies.
- Create a contingency plan for the purchase, installation, and certification of replacement equipment.
- Determine the excess cost associated with “Rush” manufacturing, installation, and certification.

Duplicate Servers

- Determine the cost of purchasing and installing a true duplicate server.
- Determine the cost of upgrading the “back-up” server to full server.
- Determine the cost of duplicate software, including license fees for multiple users and sites.
- Determine the cost to maintain “exact” duplicate servers, including all overhead expenses.
- Locate servers in separate areas, fire divisions, or buildings.

Continuity Planning for Computer Operations: Facilities, Environmental Controls, and Security

Main and Emergency Power

- Ensure that power panels are fed from separate trunk lines.
- Ensure that power panels are easily accessible.
- Ensure that power to critical equipment is distributed from separate power panels.
- Verify that circuit breakers are clearly marked and up to date for all attached equipment.
- Ensure that panels, circuit breakers, and UPS rating exceed the total wattage of all attached equipment.
- Ensure that panels, circuit breakers, and UPS rating exceed the total volt-ampere rating of all attached equipment.
- Maintain line-to-line steady state voltage at +10% to -8% of the normal rated voltage.
- Verify that all critical communication equipment is protected by noise-shielded and surge-protection devices.
- Verify that all critical equipment is powered by an Uninterruptable Power Supply (UPS).
- Ensure that the UPS is “network aware” and capable of starting the shutdown process.
- Ensure that the UPS is fed from filtered surge-protected power units.
- Use backup emergency generators for “No Down Time” applications.
- Ensure that emergency systems shut-down procedures are documented; include procedures for an ordered systems shut-down.
- Ensure that emergency room power down is available in the room and at a remote location.

Environmental Controls

- Maintain computer room air temperatures at 72° F, with a variance of no more than +/- 2° F.
- Maintain computer room humidity at 50%, with a variance of no more than +/- 10%.
- Ensure that computer fans have unrestricted intake of cool room air.
- Maintain media storage in conditions with similar temperature and humidity as the computer room.
- Allow transported media to adjust to computer room conditions before use.
- Conduct regular housekeeping and dusting.
- Professionally clean inside ductwork and under raised floors periodically.
- Use HEPA filters in vacuums, to limit re-circulation of dust.

- Use dust covers to protect unused and powered down printers, faxes, scanners, and keyboards.

Detection and Suppression Systems

- Ensure that fixed fire detection, alarm, and fire suppression systems are installed and maintained according to local and National Fire Protection Association (NFPA) codes, OSHA requirements, and manufacturers' specifications.
- Install wet or pre-action sprinkler systems in all areas.
- Install fire alarm signals in all areas.
- Verify that fire alarm systems transmit signals to a 24-hour monitoring station.
- Install smoke detectors below the raised floors, on ceilings, and above suspended ceilings.
- Install a water detection system if flooding is a potential hazard under raised floors.
- Test all detection, alarms, and suppression equipment on a regular basis.
- Place CO₂ U.L.-listed fire extinguishers near computers.
- Provide regular training in the use of fire extinguishers to employees.
- Install illuminated exit signs and post evacuation routes in all areas.
- Practice evacuation drills regularly.
- Post the emergency number on all phones (i.e., "9-911" or "911").
- Provide a floor panel lifter for immediate access to the area under raised floors.
- Provide water-tight salvage covers.

Security Controls

- Limit access to computer areas (use ID cards, key pads, door locks, and guard stations).
- Limit access to computer systems (use BIOS passwords, client and network passwords).
- Secure and limit access to location of keys, passwords, combination lock numbers, etc.
- Install burglary/intrusion alarm systems, closed-circuit TV monitoring, guard services, and sign-in and sign-out sheets.
- Use "power on" locks on computers.
- Keep computers, especially laptop equipment, out of sight; lock computers on or in desks, cabinets, or in a storage room.
- Change combinations and passwords quarterly, or when personnel changes occur.



Loss Control Department
Technical Information Paper Series

Preparing for Earthquakes

Copyright © 1999 The Hartford Loss Control Department
TIPS Series S 970.023 Printed in U.S.A.

This document is provided for information purposes only. It is not intended to be a substitute for individual legal counsel or advice on issues discussed within. Readers seeking resolution of specific legal issues or business concerns related to the captioned topic should consult their attorney and/or insurance representative.

Preparing for Earthquakes

What is an Earthquake?

An *earthquake* is a shaking of the earth that is volcanic or tectonic in origin. Though earthquakes do not occur frequently, they can be very disruptive because they affect very large areas and occur with no warning.

Earthquakes vary in duration. The shaking can be a single event of a few seconds, or it may be a series of events of varying duration. The series can occur over several hours, days, weeks, or even months.

Severe tremors that occur after the main seismic event can be particularly damaging, since structures may have already been weakened during the initial shake. These tremors also have a devastating effect on many people who have already gone through previous shaking.

The energy expended during an earthquake will vary depending on the location. It will affect structures differently depending on soil type, geological formation, the distance from the epicenter, the type of structure, and other factors.

Where Do Earthquakes Occur?

Most Americans think that earthquakes are limited to the West Coast. However, they occur in other areas of the country. Some areas are more likely to experience earthquakes than others.

Know the earthquake potential of the area in which the facility is located. Information about active fault zone locations is usually available through local municipal planning departments. Dangerous areas include:

- areas near fault lines
- soft, water-saturated soils, such as mud or artificial fill
- certain sands that liquefy and amplify shaking
- areas prone to settling or landslides.

When Do Earthquakes Occur?

Earthquakes occur without warning. Since it is not possible to predict an earthquake, all preparations must be done with the anticipation that an event may occur at any time.

Emergency Preparedness: Before the Earthquake

- Establish an Emergency Preparedness Plan (EPP) that takes prevention, emergency response, and disaster recovery into consideration. If an EPP is already in place, review and update it as needed for earthquake readiness.
- Designate an Emergency Coordinator and an EPP Team. Assign responsibility to specific employees for advance arrangements to initiate the plan.
- Develop a contingency plan to allow for continued business operations.
- Conduct a hazard assessment and safety appraisal of the facility and its operations. Upgrade deficient areas.
- Upgrade the facility to current earthquake codes.
- Inspect tanks, stacks, signs, and chimneys for deterioration and bracing. Repair and strengthen as necessary.
- Identify and designate safe shelter areas in the structures.
- Identify and designate at least two evacuation routes for all areas.
- Brace all tall shelves and cabinets, tall machinery and equipment, or any top-heavy objects that could topple.
- Brace and support overhead-mounted fixtures, suspended ceilings, piping, heaters, and other overhead-mounted devices.
- Provide flexible fuel supply connectors.
- Bolt down and secure fuel-fired appliances.
- Provide isolation valves for piping systems.
- Provide adequate support for mainframe computers.
- Provide alternate energy sources for vital equipment and services.
- Provide auxiliary equipment and energy supplies for critical services such as communications and lighting.
- Plan for continuous plant security.
- Plan for customer and client awareness and communications.
- Provide an alert and warning system for all personnel on the premises.

Emergency Response: During the Earthquake

Most earthquakes last only a few seconds to a couple of minutes. There's not much time to do anything other than sound an alarm to warn all personnel to seek cover in the designated safe areas.

Emergency Recovery: After the Earthquake

It is important to know that aftershocks can occur after the main event. They can be as strong as the main event, but they usually diminish in strength. However, *extreme caution must be exercised*, since structures may have been weakened during the initial shaking.

- Be prepared for aftershocks.
- Shut down equipment and evacuate the building.
- Stay out of the building until the aftershocks have ceased and the building has been inspected and declared safe.
- Conduct a roll call of all personnel on site (including visitors).
- Inspect the structure.
- Shut off all leaking utilities.
- Inspect all utilities and turn off those that are damaged.
- Do not use open flame in enclosed areas where flammable gases may be present.
- Brace, relocate, or remove any hazards that could fall during aftershocks.
- Document the damage.
- Communicate with employees and customers to keep them apprised of the damage and organizational progress.
- Begin salvage operations.

This document is provided for information purposes only. It is not intended to be a substitute for individual legal counsel or advice on issues discussed within. Readers seeking resolution of specific legal issues or business concerns related to the captioned topic should consult their attorney and/or insurance representative.



Loss Control Department
Technical Information Paper Series

Fire Prevention and Protection

Copyright © 1998 The Hartford Loss Control Department
TIPS Series S 680.003 Printed in U.S.A.

This document is provided for information purposes only. It is not intended to be a substitute for individual legal counsel or advice on issues discussed within. Readers seeking resolution of specific legal issues or business concerns related to the captioned topic should consult their attorney and/or insurance representative.

Fire Prevention and Protection

Overview

Fire represents one of the greatest hazards that an organization can encounter. Each year, several thousand lives are lost to fires, tens of thousands of people are seriously injured, and billions of dollars worth of property is destroyed or damaged by fires.

Smoking materials are the number one cause of civilian fire deaths in residential occupancies, accounting for nearly one-fourth of deaths; most of these are due to the ignition of upholstered furniture, mattresses, or bedding.

Arson and smoking dominate the ignition scenarios of fatal fires in public assembly properties (e.g., educational, health care, or correctional facilities).

Industrial fires often start with defects in the machinery (e.g., processing equipment) or electrical equipment, or from improper handling of flammable liquids and gases.

Most fires can be prevented by the use of proper building materials, identification and protection of special hazards, detection and suppression equipment, education, and the involvement and commitment of the organization's senior management.

Emergency Preparedness: Before a Fire

- Establish an Emergency Preparedness Plan (EPP) that takes prevention, emergency response, and disaster recovery into consideration. If an EPP is already in place, review and update it as needed for fire readiness.
- Designate an Emergency Coordinator and an EPP Team. Assign responsibility to specific employees for advance arrangements to initiate the plan.
- Conduct a hazard assessment and safety appraisal of the facility and its operations.
- Develop smoking regulations that are supported and enforced by management.
- Develop safe procedures for handling and storing flammable gases and liquids.
- Adopt a safe means of performing hot work (e.g., welding).
- Employ good housekeeping methods; do not allow rubbish to accumulate.
- Upgrade the facility to meet current fire codes.
- Use noncombustible and fire-resistant building materials.
- Ensure that a preventive maintenance program for operational equipment (building utilities, processing equipment, and material handling equipment) meets manufacturer's specifications and industry standards.
- Install fire detection systems (e.g., fire alarm systems) and fire suppression systems (e.g., fire extinguishers, sprinkler systems, and carbon dioxide) in the building, particularly in hazardous locations.
- Test all fire and life safety detection and suppression equipment per local and national fire codes.

- Ensure that there is an adequate water supply for the sprinkler system. Evaluate the water supply's volume, pressure, and duration (e.g., pressure, suction, or gravity/elevated tanks). When reservoirs, ponds, rivers, and other similar bodies of water are used to supply the sprinkler system, consider and evaluate any unusual conditions (e.g., droughts, freeze-ups, etc.).
- Meet with the local fire department to familiarize them with special hazards and emergency procedures.
- Develop mutual aid agreements with other companies.
- Keep a list of all vendors' and key customers' telephone numbers and other important contact information available and secured.
- Provide an alert and warning system for all personnel on the premises.
- Plan fire evacuation routes, mark them clearly, and drill employees in using them.
- Inspect all evacuation routes daily.
- Practice your evacuation plan.

Emergency Response: During a Fire

- Identify the affected area and sound the alarm.
- Call the public fire department.
- Evacuate all visitors and employees.
- Position security staff at the front entrance of the building (or wherever appropriate) to meet, brief, and escort the fire department.
- When directed by the fire department, notify the electric company to cut off electric power to the facility.

Emergency Recovery: After a Fire

- Conduct a roll call of all personnel, including visitors.
- Assess the structure for damage.
- Inspect all utilities and turn off those that are damaged.
- Protect equipment and inventory against further damage from water or exposure to the elements.
- Restore fire detection and suppression systems.
- Arrange for security at the scene.
- Photograph and document the damage.
- Begin salvage operations.

This document is provided for information purposes only. It is not intended to be a substitute for individual legal counsel or advice on issues discussed within. Readers seeking resolution of specific legal issues or business concerns related to the captioned topic should consult their attorney and/or insurance representative.



Loss Control Department
Technical Information Paper Series

Life Safety: *Evacuation Planning*

Copyright © 1999 The Hartford Loss Control Department
TIPS Series S 970.022 Printed in U.S.A.

This document is provided for information purposes only. It is not intended to be a substitute for individual legal counsel or advice on issues discussed within. Readers seeking resolution of specific legal issues or business concerns related to the captioned topic should consult their attorney and/or insurance representative.

Life Safety: Evacuation Planning

Protecting the health and safety of individuals is the first priority during an emergency. *Evacuation planning* is one common means of protecting individuals. Evacuation plans will vary depending on the facility and the nature of the emergency. In the case of a fire, an immediate evacuation to a predetermined area away from the facility may be necessary. In the event of a hurricane, evacuation could involve the entire community and might take place over a period of days.

When developing evacuation plans, consider the needs of employees, emergency responders, visitors, and others. Include provisions for facility shut-down, and coordinate plans with the local emergency management office and various outside agencies. Establish procedures for assisting persons with disabilities. Consider elevators, evac chairs, buddy systems, and areas of refuge.

Consider these general requirements for Evacuation Planning:

Designate Roles and Responsibilities

- Establish a clear chain of command. Identify personnel who have the authority to order and direct an evacuation.
- Designate wardens to assist others in an evacuation and to account for personnel and visitors.
- Designate personnel to continue or shut down critical operations while an evacuation is underway.

Establish Evacuation Routes

- Designate primary and secondary evacuation routes and exits.
- Install emergency lighting in case of a power outage during an emergency.
- Ensure that evacuation routes and emergency exits are:
 - clearly marked and well lit.
 - wide enough, clear, and unobstructed at all times, and unlikely to expose evacuating personnel to additional hazards.

Provide Evacuation Information

- Establish, document, post, and distribute evacuation policies and procedures.
- Provide emergency information, such as checklists and evacuation maps. Post evacuation maps in strategic locations.
- Consider the information needs of customers who visit the facility.

Provide Evacuation Training

- Train employees in evacuation procedures. Hold sessions at least annually, or when:
 - Employees are hired.
 - Wardens and other special assignments are designated.
 - New equipment, materials or processes are introduced.
 - Procedures are updated or revised.
 - Exercises show that employees performance must be improved.

Consider Special Situations

- Establish procedures for assisting persons with disabilities. Consider elevators, evac chairs, buddy systems, areas of refuge, signs, alarms, and means of communication. Be familiar with the relevant requirements of the Americans with Disabilities Act.
- Establish procedures to assist those who do not speak English.

Community Needs

- Coordinate plans with the local emergency management office and various outside agencies.
- Consider employees' transportation needs for community-wide evacuations.

After an Evacuation

- Obtain an accurate head count after an evacuation.
 - Designate assembly areas where personnel should gather after an evacuation.
 - Take a head count after the evacuation. Determine the names and last known locations of personnel not accounted for.
 - Establish a method of accounting for non-employees (customers, vendors).
 - Establish procedures for further evacuation in case the incident expands.

References

1. *Code for Safety to Life from Fire in Buildings and Structures..* (Life Safety Code) (National Fire Codes, NFPA 101). Quincy, MA: National Fire Protection Association, c1994.
2. *Employee Emergency Plans and Fire Prevention Plans.* 29 CFR 1910.38 Department of Labor. Occupational Safety and Health Administration.
3. *How to Prepare for Workplace Emergencies.* (OSHA 3088) Washington, DC: Occupational Safety and Health Administration, 1995.
4. *Recommended Practice for Disaster Management.* (National Fire Codes, NFPA 1600). Quincy, MA: National Fire Protection Association, c1995.

This document is provided for information purposes only. It is not intended to be a substitute for individual legal counsel or advice on issues discussed within. Readers seeking resolution of specific legal issues or business concerns related to the captioned topic should consult their attorney and/or insurance representative.



Loss Control Department
Technical Information Paper Series

Lightning Prevention and Protection

Copyright © 1999 The Hartford Loss Control Department
TIPS Series S 970.009 Printed in U.S.A.

This document is provided for information purposes only. It is not intended to be a substitute for individual legal counsel or advice on issues discussed within. Readers seeking resolution of specific legal issues or business concerns related to the captioned topic should consult their attorney and/or insurance representative.

Lightning Prevention and Protection

What is Lightning?

Lightning is the atmospheric discharge of electrical energy from one charged area to another area of different charge. This current flow can occur between cloud and cloud, or between the earth and a cloud. During the initial lightning flash, current flows exceed 140,000 amperes 99 percent of the time, with multiple strokes of reducing current flow intensity.

Lightning causes property damage directly from the hit and through induced electrical surges; it can also start fires. Parts of a structure most likely to be struck are chimneys, flagpoles, towers, deck rails, or other objects that project above the surrounding area. On buildings which have flat roofs, the roof edge is most likely to be struck. Lightning is also a very serious personal threat.

Lightning protection is accomplished by providing the means by which a lightning strike can enter or leave the earth (for example, through a lightning rod) without causing property damage or loss of life. The path must be of low impedance so that excessive heat is not generated; this heat can start fires.

Emergency Preparedness: Before Lightning Storms

- Establish an Emergency Preparedness Plan (EPP) that takes prevention, emergency response, and disaster recovery into consideration. If an EPP is already in place, review and update it as needed for lightning readiness.
- Designate an Emergency Coordinator and an EPP Team. Assign responsibility to specific employees for advance arrangements to initiate the plan.
- When a severe storm is approaching, listen to the radio or TV for updated weather information. An AM radio is sensitive to electrical disturbances that are detected by background static. This static will alert people that there is an electrical storm in the area.
- Consider installing a lightning protection system that is capable of intercepting a lightning strike and conducting it to ground.
- Install lightning arrestors on incoming telephone and power lines to protect against electrical surges generated by lightning.
- Install surge protectors to protect electronic equipment from electrical surges generated by lightning.
- Educate people about the hazards of lightning and stray extraneous electrical current flows.
- Have people trained to administer CPR if someone is hit by lightning.

Emergency Response: During Lightning Storms

- When the storm approaches, it becomes a personal threat to anyone outside the lightning-protected area. Seek shelter in a substantial building. Avoid metal-roofed buildings.
- Discontinue any wet operations where people come in contact with wet or highly conductive environments.
- If you are caught outside, avoid high areas. Do not stand near open water, metal fences, wire, or other horizontal conductors. Do not stand near trees, poles, flagpoles, or other vertical conductors. Put down metal tools, golf clubs, or poles.
- If, during the storm, your hair stands on end, drop to your knees, bend forward, and place your hands on your knees. Do not lie flat on the ground.
- If someone is hit by lightning and loses consciousness, start CPR. Once consciousness is regained, seek medical help immediately. Anyone who is stunned by lightning, even if consciousness is not lost, should also seek medical help.

Emergency Recovery: After Lightning Storms

- Check the area for fires and/or electrical damage that may have occurred.
- Inspect the lightning arrest system for any damage that may have occurred from a direct lightning hit. Repair damage.
- Check all main electrical equipment and circuits if a direct hit is suspected, and before energizing equipment that was shut down.

This document is provided for information purposes only. It is not intended to be a substitute for individual legal counsel or advice on issues discussed within. Readers seeking resolution of specific legal issues or business concerns related to the captioned topic should consult their attorney and/or insurance representative.