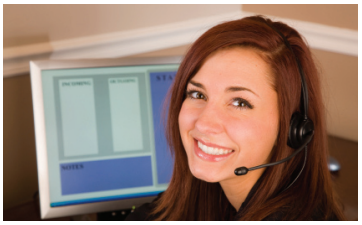
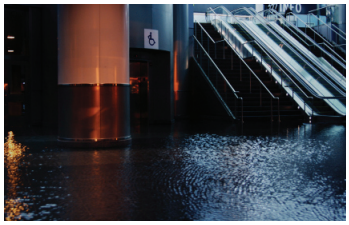
Florida Business Disaster Survival Kit





Prepared by the Tampa Bay Regional Planning Council in association with the Business Continuity Planning Alliance and the State of Florida Division of Emergency Management.

Funded through a grant from the Florida Emergency Management, Preparedness and Assistance Trust Fund

Florida
Business Disaster Survival Kit

BUSINESS DISASTER PLANNING GUIDEBOOK

Prepared by the Tampa Bay Regional Planning Council
in cooperation with the Business Continuity Planning Committee
funded through a grant from the Florida Emergency Management,
Preparedness and Assistance Trust Fund

JUNE 2008

Tampa Bay Regional Planning Council

FLORIDA EMERGENCY PREPAREDNESS ASSOCIATION

FRCA
Florida Regional
Councils Association
Partnerships for the Future

STATE EMERGENCY
FLORIDA
SERT
RESPONSE TEAM

The Tampa Bay Regional Planning Council (TBRPC) wishes to acknowledge the assistance of the following persons, agencies, associations and businesses in the development and update of the ***Florida Business Disaster Survival Kit*****:**

Susan Mueller, Emergency Manager, TECO Energy
Steve Elliot, Elliot Consulting, Inc.
Rebeca Searcey, Tampa Bay WorkForce Alliance
Stacey Swank, Pinellas County Economic Development
Robert Wabbersen, Publix Supermarkets
Holley Wade, CEM, Business Contingency Program, Hillsborough County Emergency Management
Bill Hastings, Elliot Consulting, Inc.
Mark Hendrickson, Tampa Bay Chapter, American Red Cross
Don Hermey, Manatee County Emergency Management
Thomas Iovino, Pinellas County Communications Department
Doug Blackwell, Pinellas County Emergency Management
Sally Bishop, Director, Pinellas County Emergency Management
Ron Barnwell, Executive Director, Clearwater Chamber Business Assistance Corporation
William G. Babcock, Vice President of Administrative Services, Eva-Tone, Inc.
Leslie Chapman-Henderson, CEO, FLASH
Jerry Custin, Business Assistance, Oldsmar Chamber of Commerce
Janet Double, Pinellas County Communications Department
Laurie Feagans, Director, Manatee County Emergency Management
Diane Fojt, MISC, REMT-P, Field Traumatologist, Medical Education Consultants of America, Inc.
Larry Gispert, Director, Hillsborough County Emergency Management
Larry Hibbs, Owner, Servpro of Bradenton, Florida
Jim Martin, Director, Pasco County Emergency Management Department
Doug Meyer, Coordinator, Pinellas County Emergency Management
Katie McLean, Manatee County Planning Department
Mary Jane Stanley, CED, Executive Director, Pasco Economic Development Council
Charlie Reese, Institute for Business and Home Safety (IBHS)
Jerry Ross, Executive Director, Disney Entrepreneur Center
Missy Rudd, Florida Department of Business and Professional Regulation
Quinton Williams, Florida Division of Emergency Management

A special recognition is extended to
WTSP-TV Tampa Bay's 10 and the late Dick Fletcher, Chief Meteorologist, for narration, content contribution and video segments.

Tampa Bay Regional Planning Council Staff:
Betti C. Johnson, AICP, Principal Planner
Kim Williams, Communications/Graphics Coordinator

Margarita Laughlin, Spanish Translator

Recent hurricanes including the hurricane season of 2004 when an unprecedented four hurricanes hit the state of Florida and the horrific events of Hurricanes Katrina and Rita in 2005, flooding, tornadoes, wildfires and the tragic events of September 11, 2001, have emphasized the need for everyone–families and businesses–to be prepared.

The Florida Business Disaster Survival Kit is part of the official state disaster preparedness and mitigation program, Florida Prepares!

The Florida Business Disaster Survival Kit includes this Guidebook, the **Florida Business Continuity Planning (BCP) Wizard©**, an interactive planning assistance tool and a Business Continuity Model Plan, online training exercises and a library of resources, websites and contacts to assist you in your planning efforts. The Kit is available on the Internet in English or Spanish. (www.fldisasterkit.com).

The "Kit" was prepared by the Tampa Bay Regional Planning Council (TBRPC) and the Business Disaster Planning Steering Committee that includes the Emergency Management, Communications and Economic Development agencies of Hillsborough, Manatee, Pasco and Pinellas counties, the Florida Division of Emergency Management, the American Red Cross and qualified, interested professionals in private industry. The Florida Regional Planning Councils (FRCA) with their emergency management agencies and business continuity planning partners from around the state contributed valuable local information and reviewed information and helped to promote awareness for this statewide project.

This guide is intended to be used by small to medium size businesses, although we hope all businesses find it useful to ensure their business continuity plan are viable and to increase the safety of their employees, vendors and customers/clients as well as their financial security.

You are busy and your eye must be on the bottom line. However, becoming familiar with the contents of this guide and going through this planning process will increase the odds that your business will make it through the next disaster.

The guide is divided into four sections:

The first section introduces the **Business Continuity Planning Process**. It explains why disaster planning is so important for all businesses in Florida, and highlights what you can do–step by step–to prepare your business and your employees and reduce your vulnerability to disasters.

Section Two, the **Hazard Analysis and Response Guide**, provides an overview of the hazards that businesses in the State of Florida may face. This expanded section includes natural hazards, technological hazards and other hazards that may result in business interruption and significant loss. This section references Response Checklists for specific events in the Appendix.

The third section relates to **Recovery and Mitigation**. The recovery actions portion describes re-entry teams, repairs and the relocation of essential operations, if necessary. The mitigation strategies are initiatives designed to minimize your risk of loss due to specific hazards. This part presents risk assessment and cost-benefit analyses. The strategies include policies, strategies and investments to protect your human resources, your facility and both tangible and intangible assets.

The fourth section is **Resources: Preparedness Info Center.** It provides a resource list, links to websites where you can obtain critical local information, publications and contact information. Defining Destruction: A BCP Glossary, provides a glossary of terms relating to hazards, weather and contingency planning.

Section I:

Business Continuity Planning Process

As a business owner or manager, you have invested a lot of time and resources into making your business work. Now imagine that all you have worked for goes up in smoke, literally. Every year emergencies take their toll on business and industry, in lives and dollars. But something can be done. Business and industry can limit injuries and damages and return more quickly to normal operations.

This guide is not intended to be restrictive, exhaustive, definitive or overly detailed. It is designed to provide the basic knowledge necessary to help you protect your business from the adverse effects of disasters, large or small. You do not need to have an in-depth knowledge of emergency management or business continuity management to begin. What you need is the authority to create a plan and a commitment from the highest level of management to make emergency management part of your corporate culture. If you already have a plan, use this guide as a resource to assess and update your plan.

There is no hard and fast definition of what constitutes a disaster. Sometimes a disaster develops quickly, hitting you full-force with little or no warning (an Incident). Other times a disaster looms on the horizon for weeks until it becomes large enough to be a threat (an Event). However, the word disaster takes on a new meaning depending on the industry in which you work. A simple water pipe break could spell disaster if you are in the communications business and the break is in your electronic telephone switching area. If you are a business that depends on refrigeration, a power outage could spell disaster. Disasters by definition cannot be planned for, but a clear well thought-out plan can greatly enhance the chances for survival.

WHAT IS BUSINESS CONTINUITY PLANNING?

Business Continuity Planning (BCP) is the act of anticipating incidents which will affect mission critical functions of the company and ensuring that the business and its employees respond to any emergency in a safe, planned and rehearsed manner. BCP is not just about disaster recovery, crisis management, insurance or Information Technology (IT). It is a business issue. It presents you with an opportunity to review the way your organization performs its processes, to improve procedures and practices and increase resilience to interruption and loss.

WHAT IS EMERGENCY MANAGEMENT?

Comprehensive Emergency Management consists of four phases:

- Preparedness requires understanding the effects of disasters or emergencies, the actions that must be taken to respond to and recover from these events, as well as what can be done to mitigate future losses. Preparedness is taking the steps to ensure your business and employees are ready for the "unexpected" and know what needs to be done in an emergency situation.
- Mitigation involves taking the steps to prevent an emergency or disaster or, at least reduce your business' vulnerability.
- Response is handling the threat or the occurrence of an emergency or disaster.
- Recovery is restoring all aspects of business operations damaged or interrupted by an event.

Figure 1
Comprehensive Emergency Management

WHERE DO YOU BEGIN?

TOP LEVEL COMMITMENT

Management must be committed at the highest level for the plan to be successful. The plan must be part of the strategic business plan and the company must budget appropriately and separately for the program. A top-level policy statement should be issued that affirms the value of planning, acknowledges and accepts the associated costs, documents management responsibilities and includes the goals and expectations of the plan, as well as any organizational assumptions or parameters.

BUILDING THE PLANNING AND MANAGEMENT TEAM

The first step in your Continuity Planning Process is to build a Planning and Management Team. This team is responsible for creating, implementing, updating and maintaining the plan.

To demonstrate management's commitment and promote cooperation, a statement authorizing the planning team to take steps necessary to develop the plan should be issued. A team leader should be selected and a clear line of authority between the group members and group leader should be established. Team members should also be prepared to view this task as a continual process, rather than a one-time event.

The size of your team depends on the size of your business. The team should be representative of the entire organization. Planning cannot be accomplished in a vacuum. You will need the feedback from every department as well as their support in the development and implementation of the plan. If appropriate, the team should be comprised of key management employees from each business unit. Once the team is formed, it is important to set up a work schedule and deadlines. Some items to consider are:

- Timeline for key deliverables,
- Budget,
- Assignment of specific tasks, and
- Formation of an Emergency Management/Crisis Management Team.

UNDERSTANDING YOUR BUSINESS: DEFINING YOUR MISSION ESSENTIAL FUNCTIONS

The team should conduct an analysis of the operational aspects of the business and determine what is critical for continuance.

- When identifying your critical products, services and operations you should distinguish the following:
- What are the key business objectives of the organization? What is this business about?
- What are the products and services of the business?
- Who is involved (both internally and externally) in the achievement of the business objectives?
- What facilities and equipment are needed to produce our products and services?
- What administrative operations, equipment and personnel are vital to the continued functioning of the business?
- What products and services are provided by suppliers, especially sole source vendors?
- What are the necessary lifeline services such as electrical power, water, sewer, gas, telecommunications and transportation?

Remember to identify those key internal (i.e., personnel, IT, etc.) and external groups and resources (i.e. customers, suppliers, etc.) upon which the business objectives rely. Consider external influences that may impact on the critical processes and functions. Input from these groups or individuals can greatly enhance the planning process.

The purpose of this exercise is to determine the mission essential functions for your business, those activities necessary for your business to operate. It is worthwhile to begin the selection process with the mission statement, organizational charts, list of daily responsibilities and activities, and staff rosters. The following are steps necessary for the selection of "Mission Essential Functions":

1. List all organizational functions;
2. Determine criteria for selecting critical activities;
3. Identify Mission Critical Activities;
4. Determine minimum acceptable level you need to operate to provide mission critical activities to stay in business;
5. Prioritize those Activities and Functions;
6. Identify minimum personnel needed to complete those functions based on skills and knowledge;
7. Assess alternate facility capacity and resource needs based on functions and personnel; and
8. Determine requisite resources and equipment needed.

The following form was developed to help you define your company's "mission essential functions," the critical time period for the operation, minimum staff requirements, special equipment or supplies necessary, space needs and the contact person for each operation.

TABLE 1 - MISSION ESSENTIAL FUNCTIONS

1 Mission Essential	2 Time Period	3 Minimum Staff	4 Special Equipment/ Supplies	5 Space Needs	6 Business Unit Manager

HAZARD IDENTIFICATION AND RISK ASSESSMENT

The next step is to identify hazards and assess the risk. This step entails gathering information about current capabilities and possible hazards and emergencies, and conducting an analysis to determine your capacity to handle them.

To identify the potential hazards/emergencies faced, list all the hazards/ emergencies that could affect your business. (Your local Emergency Management Agency can assist you.) Typically these fall into one of three categories: natural hazards, technological hazards, and other types of hazards. Be imaginative. Consider all emergencies that could occur in your community, areas adjacent to your facility and those that could occur in your facility. If you determine some hazards do not present a threat to your business, you can eliminate them in the process. Other factors to consider are below:

- Historical – What types of events have occurred in the past?
- Human Error – What emergencies can be caused by employee error? Are employees trained to work safely? Do they know what to do in an emergency?
- Physical – What types of emergencies could result from the design or construction of the facility? Are there adequate and appropriate facilities for storing combustibles? Are evacuation routes and exits clearly identified and free of obstructions?

Once you have identified all the possible hazards, you need to rate the probability of the events considering the frequency and severity. When rating the hazards, use a simple system such as low, medium or high, or a scoring system of 1 to 5.

For the next part of the analysis you need to evaluate and rate the potential human impact, property impact and business impact of each of the identified hazards, taking into account any capabilities, resources, plans, policies or procedures you already have in place. When evaluating the human impact you are considering the possibility of injury or death to your employees, customers, clients or suppliers. The property impact involves the potential loss or damage to the physical structure and equipment, taking into consideration the costs to replace, repair or lease/rent facilities and equipment. Finally, when reviewing the business impact you need to evaluate the impact of the event to your critical operations and functions (i.e., employees unable to report to work, customers unable to reach the facility, interruption of critical supplies or product distribution, imposition of fines, penalties or legal costs, etc.). The Hazards and Vulnerability Analysis Form is provided to assist you in your risk assessment.

TABLE 2 - HAZARDS & VULNERABILITY ANALYSIS

HAZARD	PROBABILTY	HUMAN IMPACT	PROPERTY IMPACT	BUSINESS IMPACT	TOTAL
	Low Probability 1 - High Probability 5	Low Impact 1 - High Impact 5			
Tropical Storm					
Category 1-2 Hurricane					
Category 3-5 Hurricane					
Flooding					
Thunderstorm, Lightning, Hail					
Tornado					
Wildfire					
Sinkhole					
Drought					
Extreme Heat					
Emergency Water Shortage					
Winter Storms & Extreme Cold					
Agricultural Disease & Pests					
Hazardous Materials					
Building Fire					
Power Service Disruption					
Environmental Health					
Pandemic Flu					
Terrorism					
Bomb Threat					
Explosions & Detonation					

HAZARD	PROBABILTY Low Probability 1 - High Probability 5	HUMAN IMPACT	PROPERTY IMPACT	BUSINESS IMPACT Low Impact 1 - High Impact 5	TOTAL
Building System Failure/ Collapse					
Bio Terrorism					
Cyber-Attack					
Radiological Emergencies					
Violence in the Workplace					
Sabotage, Fraud and Theft					
Loss of Key Staff					
Civil Unrest					
Workforce Disruption					
Adjacent Hazards					
Other					

Now that you have identified the hazards your business could face and ranked your vulnerability, you know for which hazards you need to plan and you can prioritize your planning efforts based on your vulnerability. Checklists for specific hazards have been developed and are included in this guidebook (see Appendix). Select those which are appropriate for your business to include in your Business Continuity Plan.

MITIGATION STRATEGY

Once you have completed your analysis and identified those areas where your business is most at risk, decisions have to be made.

What can be done to protect the business operation? Eliminate as many of the hazards as possible or mitigate the effects of hazards that cannot be eliminated.

This is your Mitigation Strategy. There are many possibilities, so it is likely that any strategy adopted will have a number of approaches. Some items may be completed through memos, policy changes or training. Other items may involve expenditures that must be budgeted for over time. Whichever is chosen, there are certain considerations to bear in mind. Benefits to businesses from mitigation are not limited to a reduction in facility damages. The truly cost-effective benefits include:

- Increased life safety for employees and customers,
- Reduced down-time in productions,
- Protected information systems,
- Reduced damages to facilities and nonstructural components,
- Reduced damages to vital equipment, and
- Enhanced insurance coverage or reduced insurance deductibles.

Section III discusses the benefits and elements in a Mitigation Strategy including the following:

1. Human Resources Policy and Procedures: Awareness and Reporting Policies;
2. Employee Training;

3. Employee/ Family Preparedness Programs;
4. Security Issues;
5. Protection of your Facilities/ Physical Property from Water, Wind or Fire Damage;
6. Protection of Data – Backups, Software and Policies; and
7. Business Insurance

RECOVERY STRATEGY

Section III also discusses the recovery phase of a disaster, i.e., how you get back to business after a major event. It includes a description of what to expect in both the short-term and long-term. This section focuses on re-entry and your advance recovery team, the restoration of mission essential functions, the implementation of the crisis communications plan, safety measures and immediate repairs.

CONTINUITY OF OPERATIONS

Both the public and the private sector are confronting what has been termed the "new paradigm of preparedness" for employees and organizations in the wake of the September 11th tragedy. Traditionally, we have spent time and resources preparing to get employees out of a building or area that may be in danger. This is the first step–a critical one–in preparing a Business Continuity Plan. There is now a critical second step: how to continue a level of productivity to meet customer/client needs after a disaster.

Imagine that the alarms are sounding and your employees are exiting the building due to some emergency (bomb scare, hazardous material incident, anthrax scare, security breach, etc.). As you gather at your designated area safely outside the building, you are informed that the building is inaccessible for 48 hours, or 72 hours or indefinitely. Following a hurricane you may not be able to get back into the area for several weeks. Are your employees prepared to accomplish work when the workplace is not available?

Typically, the "A Plan" is to send employees home. However, depending on the length of time and your business demands, this business disruption could be devastating. According to "Smart Business Magazine," two out of every five companies hit by a large disaster go out of business within five years. This statistic can be managed if employees and business teams are prepared with a "Plan B" to resume a level of productivity.

While the purpose of the Business Continuity Plan is to provide an overview, emergency procedures and checklists necessary to respond to an emergency, the Continuity of Operations (COOP Plan) defines how to respond to an emergency that directly affects your ability to continue normal operations. The consequence of a major emergency such as a hurricane, terrorist attack, or nuclear attack, could severely disrupt your ability to function. In addition, a small-localized emergency such as a fire, explosion, or contamination could make a building unusable for an extended period of time.

The COOP plan describes how you will resume business operations after a crisis or loss of resource. The capability of an organization to continue essential operations and reconstitute those operations prior to, during, and after an emergency that limits occupancy of the building or disrupts normal services, drives the successful recovery of the business as well as the local economy and entire community. This should be a key part of your Recovery Strategy.

DEVELOPING THE BUSINESS CONTINUITY PLAN

A comprehensive Business Continuity Plan will include the following:

1. The **Strategic Plan** which will define the vision, mission, goals and objectives of the program.
2. **Emergency Operations/Response** - identify the procedures which spell out how you will respond to emergencies. Whenever possible develop them as a series of checklists that can be quickly located. The plan should also list the roles

and responsibilities of internal and external agencies, organizations, departments and individuals. This shall also include an organization chart which will establish the line of authority for agency, organization, departments, and individuals.

3. The **Mitigation Strategy** which shall establish interim and long-term actions to eliminate hazards or to reduce the impact of those hazards that cannot be eliminated.
4. A **Recovery Strategy** which shall identify the short-term and long-term priorities, processes, vital resources, acceptable time frames and procedures for restoration of services, facilities, programs, and infrastructure. The Recovery Strategy should address the possibility of loosing access to one or more workplaces/facilities. This **Continuity of Operations Plan** identifies the critical and time-sensitive applications, processes and functions to be recovered and continued, as well as the personnel, resources and procedures necessary to do so.

Each component will have common elements. These elements are the foundation for the procedures that will be followed to protect personnel and equipment and resume operations. These core elements of emergency management are:

- **Direction & Control** – Someone must be in charge in an emergency. The system for managing resources, analyzing information and making decisions in an emergency is called direction and control.
- **Life Safety** – Procedures for protecting the health and safety of everyone during an emergency (i.e., evacuation planning, routes and exits, assembly areas, sheltering, etc.).
- **Property Protection** – Procedures for protecting facilities, equipment and vital records (i.e., fighting fires, containing material spills, shutting equipment down, moving equipment to a safe location, etc.).
- **Communications** – Specific methods and equipment will be needed to report emergencies, warn personnel and customers of the danger, keep employees and families informed about what's happening, coordinate response actions and keep in contact with customers and suppliers, keeping in mind that the normal communications systems could be unavailable.
- **Community Outreach** – You may involve outside organizations in your emergency management plan. This section should include a plan for public information and media relations.
- **Recovery & Restoration** – This section should include your critical operations and the plans for resuming operations, continuity of management and protection of the chain of command, insurance coverage, contracts and claim requirements, and employee support.
- **Administration & Logistics** - This section provides direction for the creation and maintenance of complete and accurate records to ensure a more efficient emergency response and recovery, keeping in mind that certain records may be required by your insurance carrier(s) or prove valuable in the case of legal action after an incident.

WRITING THE PLAN

1. Identify Existing Plans and Procedures - Chances are there are existing plans and procedures which address disaster planning already in existence. It is possible all that is necessary is to pull these documents together into a comprehensive plan. At a minimum, there are probably procedures already incorporated into the business practice which address many of the hazards your company may face. The challenge is bringing this information together, identifying what may be missing or incomplete and writing a clear, concise and viable plan.
2. Support Documents - The committee will need access to any documents that could be needed in an emergency such as:

- Emergency call lists for employees, clients, vendors and suppliers, contractors, insurance agent/companies, emergency response agencies
- Floor plans, Building and site maps that indicate utility shut-offs, water lines, gas lines, electrical cut-offs, electrical sub stations, hazardous materials (including cleaning supplies) storage, sewer lines, fire extinguishers, exits and designated escape routes, assembly areas, and restricted or high security areas

- Local government plans for community disasters (Evacuation Zones, procedures for re-entry, etc.)
- Insurance information and inventories
- Vital Records (paper and electronic formats, software, databases) and the procedures for backup and protection

3. Team Members to discuss and complete the (1) Strategic Plan (purpose, goals, objectives and policies), (2) Hazard and Vulnerability Assessment and (2) Mission Essential Functions Table (each department).
4. Use the BCP Template to generate a draft plan.
5. Assign each member of the planning team a section to review. Establish specific goals and milestones as well as an appropriate format. Ideally a schedule should be set for:

   - First draft,
   - Review,
   - Second draft,
   - Table-top Exercise,
   - Review of plan in relation to the exercise,
   - Final draft,
   - Printing,
   - Distribution and
   - Training and Testing schedules.

Once the plan is ready for distribution employees will need to be informed about the plan and the scheduled training.

IMPLEMENTING THE PLAN

Implementing a plan is more than simply exercising the plan during an emergency. It means acting on recommendations made during the planning process, integrating the plan into company operations, training employees, exercising and evaluating the plan.

Emergency planning must become part of the business culture. Look for opportunities beyond employee orientation to build awareness. Educate and train personnel, test procedures, and make emergency management a part of what employees do on a daily basis. Use opportunities already available, such as Florida Hazardous Weather Awareness Week, National Hurricane Awareness Week or National Fire Prevention Week to conduct training sessions or exercises.

All employees will require some form of education and training. General training for all employees should address:

- Individual roles and responsibilities
- Information about threats, hazards and protective actions
- Notification, warning and communications procedures
- Personal/family emergency plans
- Emergency response procedures
- Evacuation, shelter and accountability procedures
- Location and use of common equipment
- Emergency shutdown procedures

Keep in mind that training needs to be a continual effort. For the plan to be efficient and effective, employees need to be knowledgeable about the policies and procedures outlined in the plan as well as their roles and responsibilities.

PLAN TESTING, EVALUATION AND MAINTENANCE

No matter how well conceived a plan is, it is almost impossible to consider all of the events and possibilities that can be encountered in a real emergency or disaster. Deciding to create a plan is an important step toward ensuring the survival of your business after a disaster. But simply writing the plan is not enough. Turning thoughts into action is not an exact science. In order to be considered reliable, your plan must be tested. A proven plan increases your confidence in its workability and avoids having a false sense of security in a plan that may look good on paper but is deficient in reality. Testing also assists in training the participants and familiarizing them with their roles. It lowers the stress during the emergency and reduces the possibility of panic since people will have a basic familiarity with their roles.

In order to test your plan, you will need to think of scenarios in which you would have to put the plan, or components of the plan, into action. Basically, the threat scenario should be based on those items identified in your risk assessment. Some suggested scenarios include fire, loss of services (including water, wastewater and power), tornado, tropical weather, hazardous materials release and computer virus. You may also want to consider testing re-entry and recovery procedures after the emergency.

TEST LEVELS

Testing the plan can be as simple or complicated as you wish. While you may not want to conduct a full-scale exercise, orientation sessions and tabletop exercises can be very effective. The key is to always evaluate your plan after each training session or implementation and make the necessary changes from lessons learned.

There are seven types of exercises defined within the U.S. Department of Homeland Security (DHS) Exercise Guidance each of which is either discussions-based or operations-based.

Discussions-based Exercises familiarize participants with current plans, policies, agreements and procedures, or may be used to develop new plans, policies, agreements, and procedures. Types of Discussion-based Exercises include:

- **Seminar**. A seminar is an informal discussion, designed to orient participants to new or updated plans, policies, or procedures (e.g., a seminar to review a new Evacuation Standard Operating Procedure).
- **Workshop.** A workshop resembles a seminar, but is employed to build specific products, such as a draft plan or policy.
- **Tabletop Exercise (TTX).** A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. TTXs can be used to assess plans, policies, and procedures. It is an exercise that simulates an emergency situation in an informal, stress-free environment. The participants, usually people on a decision-making level, gather around a table to discuss general problems and procedures in the context of an emergency scenario. The focus is on training and familiarization with roles, procedures, or responsibilities. While this type of exercise lacks realism and provides only a superficial exercise of plans, procedures, and staff capabilities, it requires only a modest commitment in terms of time, cost and resources. It is a good way to acquaint key personnel with emergency responsibilities, procedures, and one another.
- **Games.** A game is a simulation of operations that often involves two or more teams, usually in a competitive environment, using rules, data, and procedure designed to depict an actual or assumed real-life situation.

Operations-based Exercises validate plans, policies, agreements and procedures, clarify roles and responsibilities, and identify resource gaps in an operational environment. Types of Operations-based Exercises include:

- **Drill.** A drill is a coordinated, supervised activity usually employed to test a single, specific operation or function within a single entity (e.g., a fire drill).
- **Functional Exercise (FE).** A functional exercise examines and/or validates the coordination, command, and control between various multi-agency/division/company coordination centers, if appropriate. The functional exercise simulates an emergency in the most realistic manner possible, short of moving real people and equipment to an actual site. As the name suggests, its goal is to test or evaluate the capability of one or more functions in the context of an emergency

event. Players practice their response to an emergency by responding in a realistic way to carefully planned and sequenced messages given to them by simulators. All decisions and actions by players occur in real time and generate real responses and consequences from other players. The guiding principle is to imitate reality. The atmosphere is stressful and tense due to real-time action and the realism of the problems. While this type of an exercise can test the same functions and responses as in a full-scale exercise without high costs or safety risks, it is lengthy and complex, requires careful scripting, careful planning, and attention to detail.

- **Full-Scale Exercises (FSE).** A full-scale exercise is as close to the real thing as possible; it replicates the disaster to the smallest detail. It is a lengthy exercise which takes place on location, using, as far as possible, the equipment and personnel that would be called upon in a real event. It differs from a functional exercise or "drill" in that a drill focuses on a single operation. Scenarios often include surprise events to test responses of the participants and to achieve realism as much as possible. (For example, people posing as casualties may be made up with wounds to test the reactions of the participants to events they may actually encounter in a disaster.) Full simulations normally are used by the military, police, fire/rescue and emergency management organizations and businesses with high exposure.

Ideally, everyone in your business and third parties (vendors, suppliers, customers, governmental agencies, etc.) who could possibly be involved in the event of a disaster should participate in the test. Obviously, this is not always practical or even possible, especially the third parties. Even if interested parties are unable to participate, they should be informed of their expected role in your plan and the team should simulate activities assigned to third parties unable to participate. Try to work with the third party in advance to find out how they intend to respond in a disaster. It is important to thoroughly document this portion of the exercise in case the third party's planned response is determined to be inadequate during the exercise. This documentation will be important when you present your results to them and ask for changes. If such an occasion arises, it will likely illustrate the need for the third party's active participation in subsequent exercises.

The building block approach focuses on exposing participants to a cycle of training and exercises that escalates in complexity, with each exercise designed to build upon the last, in terms of scale and subject matter. For example, a building-block series of exercises may include a seminar, which leads to a tabletop exercise (TTX), which leads to a full-scale exercise (FSE).

The plan should be tested at least annually. More frequent exercises may be required for high-risk operations. Seasonal exercises should be considered. These should be conducted far enough in advance of the season to incorporate revisions and possibly retest.

After an exercise, consider the lessons learned and make certain any necessary changes to the plan are incorporated into the document. Major changes may require another exercise. Occasionally, the results of an exercise may warrant not only another exercise. You may also discover a higher level of testing than originally thought was needed. For instance, a business that originally decided that a walkthrough was a sufficient exercise may discover that a partial or full simulation is now needed because the walkthrough was inadequate to thoroughly test the plan.

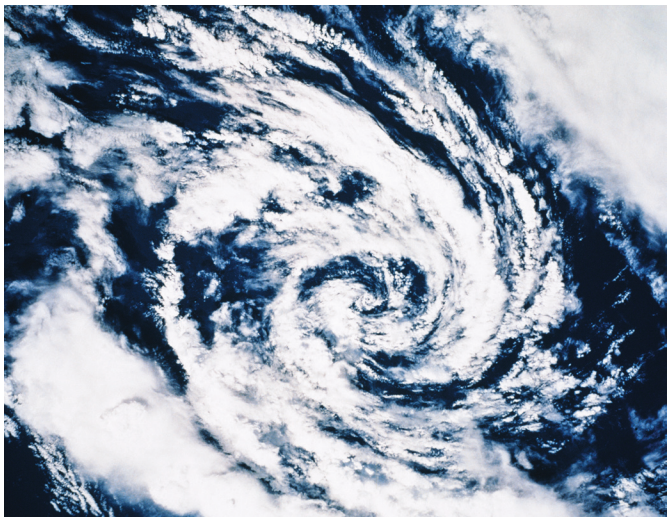
It is extremely important to document each exercise. The tests should have a script that describes each situation or scenario, who should participate, how it is to be conducted, the expected results, and a place to record the actual results. The expected results are compared to the actual results at the conclusion of the exercise. The extent to which the expected results match the actual results determines the level of success of the exercise.

Every business can encounter an emergency situation that could disrupt or cease operations. By taking the time and making the commitment to plan for the unexpected, you are not only protecting your business, employees and customers, you are helping to protect your community and local economy.

Section II:

Hazards Analysis and Response

NATURAL HAZARDS



This section provides information on natural hazards (geological, meteorological and biological) that may threaten businesses in Florida, including:

- Hurricanes and Tropical Storms
- Floods and flash floods
- Thunderstorms and Lightning
- Tornadoes and water spouts
- Wildfires
- Sinkholes and Seismic Events
- Drought
- Extreme Heat
- Emergency Water Shortage/ drought
- Winter Storms and Extreme Cold
- Agricultural Diseases and Pests; and
- Emerging Diseases (pandemic influenza)

HURRICANES AND TROPICAL STORMS

Hurricanes and tropical storms are among nature's most powerful forces because of their size and potential for destruction. Hurricanes are tropical cyclones–the general term for all circulating weather systems over tropical waters. Powered by heat from the sea, they are steered by the upper level winds and by their own sometimes ferocious energy.

Florida has experienced the greatest number of hurricane landfalls of any state in the nation because of its geographic location. Florida's flat topography also makes it susceptible to the full force of hurricane winds and powerful storm surge. There have been sixty-eight (68) landfalling hurricanes from1900 through 2006. of which 31 were major hurricanes (category 3 or higher). For more information regarding Florida hurricanes and their frequency, see Profiling Hazard Events, an excerpt from the State of Florida Hazard Mitigation Plan.

The Atlantic Hurricane season lasts from June 1st to November 30th with the peak season from mid-August to late October.

Tropical cyclones are classified as follows:

- **Tropical Depression:** A disturbance with a clearly defined low pressure area; highest wind speed is 38 miles per hour.
- **Tropical Storm:** A distinct low pressure area defined by a counterclockwise rotating circulation with winds of 39 to 73 miles per hour.
- **Hurricane:** Once a tropical storm's constant wind speed reaches 74 mph or greater, it is classified as a hurricane. In the western Pacific, hurricanes are called "typhoons," and similar storms in the Indian Ocean are called "cyclones."

HURRICANE CATEGORIES AND EVACUATION LEVELS

Hurricanes are categorized on a scale of 1 to 5 based on the strength (barometric pressure and wind speed) of the storm. The scale is called the Saffir-Simpson Hurricane Scale. Evacuation zones in coastal counties in Florida are based on the potential storm surge from the threatening hurricane, taking into account its projected strength on the Saffir-Simpson Scale, the expected track (landfalling, paralleling and exiting direction) and forward speed.

SAFFIR-SIMPSON SCALE

Category	Winds MPH	Damage	Storm Surge ft[1]
1	74-95	Minimal	4-5
2	96-110	Moderate	6-8
3	111-130	Major	9-12
4	131-155	Severe	13-18
5	Above 155	Catastrophic	Greater than 18

HURRICANE HAZARDS

The hurricane can combine storm surge, powerful winds, tornadoes and torrential rains into a devastating combination.

- **Storm surge** is an abnormal rise in sea level 50 to 100 miles wide that sweeps across the coast near where the "eye" of the hurricane makes landfall. The surge of high water, topped by waves, can be devastating. The stronger the hurricane winds and the shallower the offshore water, the higher the surge will be. Along the immediate coast, storm surge is the greatest threat to life and property.
- **Hurricane-force winds**, 74 mph or more, can destroy buildings and mobile homes. Debris can become flying missiles in hurricanes. Winds often stay above hurricane strength well inland. Even if your building is located outside of the coastal flood areas, it is extremely important to secure your facility before the storm.
- **Widespread torrential rains**, often in excess of 10 inches can produce destructive floods. This is a major threat to areas well inland. If your business is located in the 100-year flood prone area, it is extremely important that you have flood insurance, floodproof your facility to the extent feasible and have a plan to evacuate or move your operations, if necessary.
- Hurricanes also produce tornadoes, which add to the hurricane's destructive power.

WARNINGS AND ADVISORIES

As with all hazardous weather, it is important to keep informed and know the difference between "watches" and "warnings."

- **Tropical Storm Watch:** An alert for a specific area that a tropical storm may pose a threat within 36 hours.
- **Tropical Storm Warning:** An alert that tropical storm conditions, including sustained winds of 39 to 73 mph, are expected in specific areas within 24 hours.
- **Hurricane Watch:** An alert for a specific area that hurricane conditions pose a threat within 36 hours.
- **Hurricane Warning:** An alert that hurricane conditions are expected in a specified coastal area within 24 hours. All precautions should be completed immediately.
- **Evacuation Order:** The most important instruction you will receive. Once issued, an evacuation order is mandatory.

INLAND/FRESHWATER FLOODING FROM HURRICANES

Hurricanes can produce widespread torrential rains. Floods are the deadly and destructive result. Flash flooding can occur due to the intense rainfall. Flooding on rivers and streams may persist for several days or more after the storm.

[1] Storm Surge heights are based on a national average. Along the Gulf of Mexico and bay areas, storm surge may be significantly higher due to the shallow water and configuration of the bays.

The speed of the storm and the geography beneath the storm are the primary factors regarding the amount of rain produced. Slow moving storms and tropical storms tend to produce more rain.

Between 1970 and 2004, more people lost their lives from freshwater flooding associated with landfalling tropical cyclones than from any other weather hazard related to tropical cyclones. (On August 25, 2005, Hurricane Katrina became the costliest and one of the deadliest hurricanes in the history of the United States. It was the sixth strongest Atlantic hurricane ever recorded and the third strongest hurricane on record that made landfall in the United States. Most of the more than 1200 deaths associated with Katrina were victims of storm surge (Mississippi) and the flooding resulting from the storm surge inundation of the dikes and levee systems (New Orleans).

See the "Flooding" section for more specific information on flood related emergencies.

Determining your vulnerability to storm surge, freshwater flooding and high winds is critical in the development of your Business Continuity Plan. Evacuation or potential long-term structural damage and/or inaccessibility to your facility means you need to develop a crisis communication plan for your employees, clients or customers; develop a mitigation plan to reduce the physical damage to your facility or equipment and be prepared to identify an alternate workplace(s) to continue essential business operations.

A website has been developed by the State of Florida, Division of Emergency Management (www.floridadisaster.org). This site will guide you toward the state and local information for your area.

PREPAREDNESS CHECKLISTS FOR EMPLOYER AND EMPLOYEE

Protecting business facilities is not the entire solution to protecting business operations. Even if the facility survives a natural disaster such as a hurricane with little or no damage, the business cannot operate if the transportation or utility systems it relies upon are damaged, if employees cannot get to work and customers cannot buy products or services. A business is dependent on the resilience of its employees and the community to natural disasters.

Checklists have been prepared that provide a task list of what to do before, during and after a storm. See the Appendices for an Emergency Evacuation Checklist (Checklist 1) and listing of emergency supplies for the office, the Disaster Supplies Kit (Checklist 2). There is also a checklist for employees, the Employee Family Disaster Plan (Checklist 3) with critical information necessary in the aftermath of a disaster. From this information, the employer can build an emergency call-down list; see Emergency Call Down Procedures, to contact key employees, vendors and customers in the aftermath of a disaster.

FLOODING

Floods are one of the most common hazards in the U.S. and the State of Florida. While flooding does result from hurricanes, flooding can also occur during winter storms as well as prolonged summer thunderstorm activity.

All floods are not alike. Riverine floods develop slowly, sometimes over a period of days. Flash floods can develop quickly, sometimes in just a few minutes. Overland flooding occurs outside a defined river or stream, such as when a levee is breached. Flooding also can occur from a dam break, producing effects similar to flash floods.

Flooding also has become the most deadly hurricane impact in the last 30 years. Rainfall associated with hurricanes varies with hurricane size, forward speed and other meteorological factors. The rainfall associated with a hurricane is from 6 to12 inches on average, with higher amounts common. As warnings have increased and coastal evacuation plans have become more sophisticated, the deaths associated with storm surge have been reduced significantly. However between 1970 and 1999, more people lost their lives from freshwater flooding than any other tropical storm hazard.

Flooding, like drought, is a natural event, part of the normal water cycle. Flooding disasters, however, are another matter. They usually result from a failure to understand the natural systems of our environment. **In fact, flooding is the most common and expensive hazard facing the State due to our development in floodplains and the frequency of flooding events.**

Realizing that tax dollars could be saved and disasters avoided through adequate planning, the National Flood Insurance Program (NFIP) was established. The NFIP provides flood insurance to residents in communities that adopt appropriate standards and land use controls.

The Federal Emergency Management Agency (FEMA) through the National Flood Insurance Program (NFIP) has identified areas that have a 1% chance or greater of flooding in any given year, referred to as the 100-year flood plain. These areas have been delineated on Flood Insurance Rate Maps (FIRMs) for most flood-vulnerable jurisdictions in the country. The maps also identify the elevation of the flood waters from the hypothetical 100-year storm. Structures within the floodplain must be built at or above the Base Flood Elevation (BFE).

The big boom of development along the Florida's coastline in the early 1970's has left a legacy of existing coastal development built before the floodplain regulation of the NFIP and coastal management legislation. This has resulted in significant property losses for homeowners. Florida has more than 1,500 repetitive loss properties, properties that have had more than 4 flood losses in the last 10 years.

Most communities in the State of Florida (which contain floodplains) are participants in the NFIP. In addition, most of those communities participate in the Community Rating System (CRS) that encourages local governments to enact policy and procedures that further promote preparedness and mitigation. Floodplain managers, CRS Coordinators and LMS Coordinators meet through different committees to address common major issues relating to flood hazard mitigation.

First you must determine if your facility is located in flood vulnerable areas. Contact your community's flood plain management/planning office to determine if it is in the 100-year flood zone and if there is a history of flooding in the area. Local officials can give you valuable information on how to prevent flood damage through flood proofing, such as:

- Locating outside of the floodplain unless the facility and utilities are elevated above the BFE.
- Constructing barriers such as levees, berms, and floodwalls to stop floodwater from entering the building.
- Sealing walls in basements with waterproofing compounds to avoid seepage.

They will be able to tell you what the policies and regulations are regarding construction and redevelopment.

FLOODING MYTHS AND FACTS

MYTH: Flooding occurs only at low elevations along the coast.

FACT: Flooding is a result of elevation, drainage, soil type and surrounding development. It occurs along the coast and rivers as well as inland. More than 30% of the land in the State of Florida is in the flood plain.

MYTH: My property insurance policy will cover damage if we are flooded.

FACT: Flood damage is only covered under a separate flood insurance policy.

MYTH: Freshwater flooding is bothersome but not dangerous.

FACT: While traditionally riverine flooding was not considered life-threatening, over the past thirty years, it has become the leading cause of death from tropical storms and hurricanes. These deaths are primarily the result of driving through flooded roadways and children playing in flood waters.

If flood waters threaten, know the terms used to describe flooding:

- **Flood Watch** - Flooding is possible. Stay tuned to National Oceanic and Atmospheric Administration (NOAA) Weather Radio or commercial radio or television for information. Watches are issued 12 to 36 hours in advance of a possible flooding event.
- **Flash Flood Watch** - Flash flooding is possible. Be prepared to move to higher ground. A flash flood could occur without any warning. Listen to NOAA Weather Radio or commercial radio or television for additional information.
- **Flood Warning** - Flooding is occurring or will occur soon. If advised to evacuate, do so immediately.
- **Flash Flood Warning** - A flash flood is occurring. Seek higher ground on foot immediately.

EMERGENCY WARNING PROCEDURES

- Purchase a NOAA Weather Radio with battery backup and a tone-alert feature that automatically alerts you when a Watch or Warning is issued (a tone alert is not available in all areas).
- Purchase a battery-powered commercial radio and extra working batteries.
- Be prepared to evacuate. Learn your community's flood evacuation routes and where to find high ground. See the "Resources: Preparedness Info Center" for direction to this important information.

- Be prepared to be "on your own" for at least three days. Assemble a disaster supplies kit for each facility. Keep a stock of food and extra drinking water.

For more information, see the Appendices Flood Safety Checklist (Checklist 7) and Emergency Evacuation Procedures (Checklist 1).

TIPS ON FLOOD INSURANCE

- Consider purchasing flood insurance. Flood losses are not covered under standard property insurance policies.
- FEMA manages the National Flood Insurance Program, which makes federally backed flood insurance available in communities that agree to adopt and enforce floodplain management ordinances to reduce future flood damage.
- Flood insurance is available in most communities through insurance agents.
- There is a 30-day waiting period before flood insurance goes into effect, so don't delay.
- Flood insurance is available whether the building is in or out of the identified flood prone area.
- If your community participates in the NFIP, it has adopted a Flood Plain Management Ordinance that regulates development within the 100-year flood plain. This allows residents and businesses to purchase flood insurance through the federal government. The Flood Plain Management Ordinance requires new construction and reconstruction to elevate up to or above the Base Flood Elevation (BFE) to reduce the risk of flooding in the building itself. After a disaster, this can become a major challenge. The Rule requires structures damaged more than 50% of the value, to be rebuilt to current standards including elevating the structure above the base flood elevation. Your NFIP flood insurance policies automatically provide this coverage up to $20,000. However, this may not cover the amount necessary to rebuild to current codes. Many other commercial policies do not. Business owners in the flood plain should purchase additional "replacement" coverage in case the facility is damaged by wind or fire.

If you have questions about the program, contact your municipal government. If you work in an unincorporated area, call the County Planning or Building Department.

THUNDERSTORMS, LIGHTNING AND HAIL

Thunderstorms affect relatively small areas when compared with hurricanes and winter storms. The typical thunderstorm is 15 miles in diameter and lasts an average of 30 minutes. Nearly 1,800 thunderstorms are occurring at any moment around the world. That's 16 million a year! Despite their small size all thunderstorms can be dangerous. Every thunderstorm produces lightning that kills more people each year than tornadoes. Other associated dangers of thunderstorms include tornadoes, strong winds, hail and flooding.

FLASH FLOODS/ FLOODS

- Nearly 140 fatalities each year.
- Most flash flood deaths occur when people become trapped in their automobiles.
- Refer to the Flooding Section and the "Flooding Safety Checklist" (Checklist 7 in Appendix). You may also download the brochure, "Protecting Your Commercial Building from Flood" from the Florida Business Disaster Survival Kit or log onto www.ibhs.org.

TORNADOES

- Nature's most violent storms.
- Winds can exceed 200 mph. Result in an average of 80 deaths and 1,500 injuries each year.
- Refer to the Tornado Section and "Tornado Safety Checklist." (Checklist 8 in Appendix).

Straight-line winds are responsible for most thunderstorm wind damage. A small area of rapidly descending air beneath a thunderstorm can cause damaging winds in excess of 100 mph. The strong winds usually approach from one direction and

may be known as "straight-line" winds. One type of straight-line winds, the downburst, can cause as much damage as a strong tornado. For mitigation options, download the brochure, "Protecting your Commercial Building from Wind Damage" on the Florida Business Disaster Survival Kit or log onto www.ibhs.org.

HAIL

- Hail is precipitation in the form of balls or irregular lumps of ice which is always produced by convective clouds. The type of convective cloud is nearly always cumulonimbus, or more commonly, a thundercloud.
- An individual unit of hail is called a hailstone. Usually a hailstone begins as a frozen raindrop or snow pellet within a thunderstorm. The turbulent updrafts and downdrafts within the cloud send the hailstones up and down several times, where they gather layer upon layer of ice.
- When the ice becomes too heavy to be supported by the updraft it falls to the ground.
- A hailstone ranges in size from that of a pea to that of a grapefruit, or from about 1/5 inch to more than 5 inches in diameter.

LIGHTNING

- The ingredient that defines a thunderstorm is lightning.
- It occurs with all thunderstorms.
- It averages 93 deaths and 300 injuries annually in the U.S.
- It causes several hundred million dollars in damage.
- Florida leads the nation in number of lightning deaths and injuries.
- The action of rising and descending air within a thunderstorm separates positive and negative charges. Water and ice particles also affect the distribution of electrical charge. Lightning results from the buildup and discharge of electrical energy between positively and negatively charged areas.
- The average flash could light a 100-watt light bulb for more than 3 months. Most lightning occurs within the cloud or between the cloud and ground.
- The air in a lightning bolt is 50,000 F° - five times hotter than the surface of the sun!! The rapid heating of air in the lightning channel causes a shock wave that results in thunder.
- The potentials for fire and power outage are the primary concern of lightning for business operations. Refer to those sections and the disaster planning checklists for more specific information.

LIGHTNING MYTHS AND FACTS

MYTH: If it is not raining, then there is no danger from lightning.

FACT: Lightning often strikes outside of heavy rain and may occur as far as 10 miles away from any rainfall.

MYTH: The rubber soles of shoes or rubber tires on a car will protect you from being struck by lightning.

FACT: Rubber-soled shoes and rubber tires provide NO protection from lightning. However, the steel frame of a hard-topped vehicle provides increased protection if you are not touching metal. Although you may be injured if lightning strikes your car, you are much safer inside a vehicle than outside.

MYTH: People struck by lightning carry an electrical charge and should not be touched.

FACT: Lightning-strike victims carry no electrical charge and should be attended to immediately. Contact your local American Red Cross **Chapter for information on CPR and first aid classes.**

MYTH: "Heat lightning" occurs after very hot summer days and poses no threat.

FACT: What is referred to as "heat lightning" is actually lightning from a thunderstorm too far away for thunder to be heard. However, the storm may be moving in your direction.

WHAT TO DO BEFORE THUNDERSTORMS APPROACH

1. Know the terms used by weather forecasters:
   - Severe Thunderstorm Watch - Tells you when and where severe thunderstorms are likely to occur. Watch the sky and stay tuned to radio or television to know when warnings are issued.
   - Severe Thunderstorm Warning - Issued when severe weather

has been reported by spotters or indicated by radar. Warnings indicate imminent danger to life and property to those in the path of the storm.

2. Know thunderstorm facts:
   - Thunderstorms may occur singly, in clusters, or in lines.
   - Some of the most severe weather occurs when a single thunderstorm affects one location for an extended time.
   - Thunderstorms typically produce heavy rain for a brief period, anywhere from 30 minutes to an hour.
   - Warm, humid conditions are very favorable for thunderstorm development.
   - A typical thunderstorm is 15 miles in diameter and lasts an average of 30 minutes.
   - Of the estimated 100,000 thunderstorms each year in the United States, about 10 percent are classified as severe.
   - A thunderstorm is classified as severe if it produces hail at least three-quarters of an inch in diameter, has winds of 58 miles per hour or higher, or produces a tornado.
3. Know the calculation to determine how close you are to a thunderstorm:
   - Count the number of seconds between a flash of lightning and the next clap of thunder. Divide this number by 5 to determine the distance to the lightning in miles.
4. Remove dead or rotting trees and branches that could fall and cause injury or damage during a severe thunderstorm.
5. When a thunderstorm approaches, secure outdoor objects that could blow away or cause damage. Shutter windows, if possible, and secure outside doors. If shutters are not available, close window blinds, shades or curtains.

For more information, refer to the Lightning Safety Checklist #9

TORNADOES

A tornado is defined as a violently rotating column of air extending from a thunderstorm to the ground. The most violent tornadoes are capable of tremendous destruction with wind speeds of 200 mph or more.

In an average year, 800 tornadoes are reported nationwide, resulting in 80 deaths and over 1,500 injuries. Florida is #3 in number of tornadoes. Most are weak. However, strong ones do occur.

Tornadoes are classified by intensity and damage on the Fujita Scale similar to the Saffir-Simpson Hurricane Scale.

FUJITA SCALE

Category	Intensity	Wind Speed MPH
F-0	Gale	40-72
F-1	Moderate	73-112
F-2	Significant	113-157
F-3	Severe	158-206
F-4	Devastating	207-260
F-5	Incredible	261-318

Weak Tornadoes

69% of tornadoes

< 5% of tornado deaths

Lifetime 1-10+ minutes

Winds < 110 mph

Strong Tornadoes

29% of tornadoes

30% of tornado deaths

Lifetime: 20 min or longer

Winds 110-205 mph

Violent Tornadoes

Only 2% of tornadoes

70% of tornado deaths

Lifetime can exceed 1 hour

Winds > 205 mph

TORNADO MYTHS AND FACTS

MYTH: Areas near rivers, lakes and mountains are safe from tornadoes.

FACT: No place is safe from tornadoes. In the late 1980's, a tornado swept through Yellowstone National Park leaving a path of destruction on a 10,000 foot mountain.

MYTH: The low pressure in a tornado causes buildings to "explode" as the tornado passed overhead.

FACT: Violent winds and debris slamming into buildings cause most structural damage.

MYTH: Windows should be opened before a tornado approaches to equalize pressure and minimize damage.

FACT: Opening windows allows damaging winds to enter the structure. Leave the windows alone. Instead, immediately go to a **safe room**.

When a tornado threatens:

1. Know the terms used to describe tornado threats:
   - Tornado Watch - Tornadoes are possible. Remain alert for approaching storms. Listen to your battery-operated NOAA Weather Radio or local radio/television outlets for updated reports.
   - Tornado Warning - A tornado has been sighted or indicated by weather radar. Take shelter immediately.
2. Purchase a NOAA Weather Radio with a battery backup and tone-alert feature that automatically alerts you when a Watch or Warning is issued (tone alert not available in all areas). Purchase a battery-powered commercial radio and extra batteries as well.

For additional safety information and planning guidance, refer to the Tornado Safety Checklist, Checklist 8 in Appendix.

WILDFIRE

The wildfires of 1998 brought another harsh reminder to Florida residents of the power of natural hazards to destroy property, threaten safety and cause untold human hardship. Overall, after the firestorm was finally extinguished, the event had caused one of the worst wildfire disasters in Florida's history, resulting in nearly 2,300 wildfires with almost 500,000 acres burned. Well over 300 homes were damaged or destroyed. Over ten thousand firefighters from 47 different states were needed, along with more than 150 aircraft, to bring the fires under control. In their aftermath, they left the people of the State - who are perhaps more accustomed to the ravages of hurricanes, tornadoes, and floods - surprised at the power and severity of this fire storm. In 1999, Florida's drought continued. As a result, the State again was stricken with a severe wildfire outbreak. Even though drought conditions were worse, the 1999 wildfire season brought fewer losses because the emergency response and the public were more prepared.

The reasons for the wildland fire crisis are deceiving. Extremely dry weather conditions create a natural potential for disaster. But the increasing number of people living in or near wildlands means those firefighters must turn away from wildfires to protect lives and property.

- Fire facts about rural living include the following:
- Once a fire starts outdoors in a rural area, it is often hard to control. Wildland firefighters are trained to protect natural resources, not homes and buildings.
- Many rural businesses are located far from fire stations. The result is longer emergency response times. Within a matter of minutes, a building may be destroyed by fire.
- Limited water supply in rural areas can make fire suppression difficult.
- Buildings may be secluded and surrounded by woods, dense brush and combustible vegetation that fuel fires.

As a business owner considering building in an area where a wildfire can occur, you can take a few simple precautions which will protect your business and may well preserve the attractive environment.

1. **Choose a firewise location.**
   - Check with local officials to see what fire protection is available.
   - Evaluate the site. A level area is better than a sloped one.
   - Ensure that emergency vehicles will have easy access with at least 12 feet wide with turn-around space.
   - Don't forget to clearly mark your location so firefighters can find you.
2. **Design and build firewise structures.**
   - Work with architects, contractors and fire officials to create a design that is both aesthetically pleasing and firewise.
   - The number one cause of building losses in wildland fires is from untreated wood shake roofs.
   - Don't let sparks jump from your business to the wildland--or from a wildland fire to your business.
3. **Stay on guard with firewise landscaping and maintenance.**

   Tips for making your property fire resistant:
   - Keep lawns trimmed, leaves raked, and the roof and rain-gutters free from debris such as dead limbs and leaves.
   - Stack firewood at least 30 feet away from your building.
   - Store flammable materials, liquids and solvents in metal containers outside the home at least 30 feet away from structures and wooden fences.
   - Create defensible space by thinning trees and brush within 30 feet around your building. Beyond 30 feet, remove dead wood, debris and low tree branches.
   - Landscape your property with fire resistant plants and vegetation to prevent fire from spreading quickly. For example, hardwood trees are more fire-resistant than pine, evergreen, eucalyptus, or fir trees.
   - Make sure water sources, such as hydrants, ponds, pools and wells, are accessible to the fire department.
4. **Be prepared and have a fire safety and evacuation plan:**
   - Practice fire escape and evacuation plans.
   - Mark the entrance to your property with address signs that are clearly visible from the road.
   - Know which local emergency services are available and have those numbers posted near telephones.
   - Provide emergency vehicle access through roads and driveways at least 12 feet wide with adequate turnaround space.

SINKHOLES AND SEISMIC EVENTS

SINKHOLES

Sinkholes can be depressions in the land surface or may be hidden from view below the surface. Sometimes referred to as "sinks," they are widely distributed in Florida. They can be shallow or deep, small or large, but all are a result of the same general geologic processes.

Much of Florida's landscape is comprised of what's known as "karst." A karst terrain is a land surface produced by water dissolving the limestone bedrock and is characterized by sinkholes, cavern systems and springs. Sinkholes occur as a natural process of erosion of the limestone by water. Ancient cavities dissolved in the limestone need a triggering mechanism to cause the collapse. In pre-development times sinkholes were usually triggered by heavy rains or a flood that made the soil "roof" over the cavity very heavily, so that it eventually collapsed. Droughts also can lower the groundwater levels, reducing the buoyant support of a cavity roof and prompting a collapse.

Increased numbers of sinkholes can generally be attributed to changing or loading of the earth's surface with development such as retention ponds, buildings, changes in drainage patterns, heavy traffic vibrations or declining groundwater levels.

Sinkholes are of interest to Florida because they are one of the predominant land form features of the state. Their development may be sudden and may result in property damage or loss of life. Florida has more sinkholes than any other state in the nation. Florida's average sinkhole size is 3 to 4 feet across and 4 to 5 feet deep.

Based on historical evidence, the most vulnerable counties are located mostly in the center portion of the state and include: Hillsborough, Citrus, Pasco, Polk, Hernando, Marion, and Orange Counties. The least vulnerable counties, assumed by historical evidence, are in the panhandle, in the Northeast Jacksonville area and the Miami-Dade, Duval, Hendry, Holmes, Lafayette, Monroe and Walton counties.

Perhaps the most famous sinkhole in recent U.S. history is the one formed in May 1981, in Winter Park, Florida near Orlando. The sinkhole is roughly circular but elongated, (approximately 300 feet by 300 feet in size). It swallowed one house and shed, half of the municipal swimming pool, a Porsche sports car, several large oak trees, a section of the crossing street and adjoining street and an estimated 4 million cubic feet of soil. The sinkhole also damaged three other Porsche sports cars and a pick-up camper that slid into the crater, caused the rear of an auto shop to crack open and exposed the utility lines in the vicinity.

Lake Jackson in Tallahassee, a nationally known bass fishing lake, experienced a sinkhole on September 16, 1999. It suddenly drained more than half the lake of every last gallon of water, not to mention every fish and alligator.

On July 12, 2001, emergency officials for Hernando County investigated 18 confirmed sinkholes that hit in one day across the area, affecting a 15- to 16-block residential area and causing extensive damage to one house. It was one of the largest holes measured, between 50 and 100 feet deep.

The best way to find out whether there is sinkhole activity in your area is to refer to maps on the Florida Department of Environmental Protection web site (http://www.dep.state.fl.us/geology/geologictopics/sinkhole.htm).

What to do if a Sinkhole forms? Refer to the Sinkhole Action Checklist, Checklist 11 in Appendix.

EARTHQUAKES

Though earthquakes are not likely to affect Florida, their effects have been felt throughout history. Of the earthquakes felt in Florida, only six are thought to have had epicenters in Florida. (State Profile, Florida Division of Emergency Management, 2003))

LANDSLIDES

There is no historical evidence of landslide events in the state of Florida.

OTHER NATURAL HAZARDS

DROUGHT

A drought is a period of abnormally dry weather that persists long enough to produce serious effects (crop damage, water supply shortages, etc.). The severity of the drought depends upon the degree of moisture deficiency and the duration as well as the size of the affected area. A drought can affect vast territorial regions and large population numbers. This damaging phenomenon is rarely lethal but enormously destructive. Drought can ruin local and regional economies that are agricultural and tourism based. Drought also increases the risk of other hazards such as fire and flash floods.

Devastating impacts on businesses and the overall economy include the following:

- Decreased land prices
- Loss to industries directly dependent on agricultural production (e.g., machinery and fertilizer manufacturers, food processors, dairies)
- Unemployment from drought-related declines in production
- Strain on financial institutions (foreclosures, more credit risk, capital shortfalls)
- Revenue losses to federal, state, and local governments (from reduced tax base)
- Reduced of economic development
- Fewer agricultural producers (due to bankruptcies, new occupations)
- Rural population loss
- Loss to manufacturers and sellers of recreational equipment
- Losses related to curtailed activities: hunting, fishing, bird watching, boating, etc.

Costs and losses to agricultural producers are more direct and severe, including annual and perennial crop losses, damage to crop quality, income loss for farmers due to reduced crop yields, reduced productivity of cropland (wind erosion, long-term loss of organic matter, etc.), insect infestation, plant disease, wildlife damage to crops, increased irrigation costs, and the cost of new or supplemental water resource development (wells, dams, pipelines). These should be considered in the Business Disaster Plan.

Costs and losses to livestock producers also may be severe, including reduced productivity of rangeland, reduced milk production, forced reduction of foundation stock, closure/limitation of public lands to grazing, high cost/unavailability of water for livestock, cost of new or supplemental water resource development (wells, dams, pipelines), high cost/unavailability of feed for livestock, increased feed transportation costs, high livestock mortality rates, disruption of reproduction cycles (delayed breeding, more miscarriages), decreased stock weights, increased predation, and range fires.

Loss from timber production from drought is the result of wildland fires, tree disease, insect infestation, impaired productivity of forest land and direct loss of trees, especially young ones.

Loss from fishery production is the result of damage to fish habitat, loss of fish and other aquatic organisms due to decreased flow.

EXTREME HEAT

Heat kills by pushing the human body beyond its limits. Under normal conditions, the body's internal thermostat produces perspiration that evaporates and cools the body. However, in extreme heat and high humidity, evaporation is slowed and the body must work extra hard to maintain a normal temperature.

Most heat disorders occur because the victim has been overexposed to heat or has over-exercised for his or her age and physical condition. The elderly, young children and those who are sick or overweight are more likely to succumb to extreme heat.

Conditions that can induce heat-related illnesses include stagnant atmospheric conditions and poor air quality. Consequently,

people living in urban areas may be at greater risk from the effects of a prolonged heat wave than those living in rural areas. Also, asphalt and concrete store heat longer and gradually release heat at night, which can produce higher nighttime temperatures, known as the "urban heat island effect."

Businesses in Florida especially those related to tourism, recreation, or construction should address extreme heat from a life safety perspective. Employees should be aware of heat disorders, know how to recognize the danger signals and avoid over-exposure.

1. Know the terms associated with extreme heat:
   - Heat wave - Prolonged period of excessive heat, often combined with excessive humidity.
   - Heat index - A number in degrees Fahrenheit (F°) that tells how hot it feels when relative humidity is added to the air temperature. Exposure to full sunshine can increase the heat index by 15 degrees.
   - Heat cramps - Muscular pains and spasms due to heavy exertion. Although heat cramps are the least severe, they are often the first signal that the body is having trouble with the heat.
   - Heat exhaustion - typically occurs when people exercise heavily or work in a hot, humid place where body fluids are lost through heavy sweating. Blood flow to the skin increases, causing blood flow to decrease to the vital organs. This results in a form of mild shock. If not treated, the victim's condition will worsen. Body temperature will keep rising and the victim may suffer heat stroke.
   - Heat stroke - Heat stroke is life-threatening. The victim's temperature control system, which produces sweating to cool the body, stops working. The body temperature can rise so high that brain damage and death may result if the body is not cooled quickly.
   - Sun stroke - Another term for heat stroke.
2. Consider the following preparedness measures when faced with the possibility of extreme heat.
   - Install window air conditioners snugly, insulate if necessary.
   - Close any floor heat registers nearby and use a circulating or box fan to spread cool air.
   - Check air-conditioning ducts for proper insulation.
   - Install temporary reflectors, such as aluminum foil covered cardboard, to reflect heat back outside and be sure to weather-strip doors and sills to keep cool air in.
   - Cover windows that receive morning or afternoon sun with drapes, shades, awnings or louvers. Outdoor awnings or louvers can reduce the heat that enters a home by up to 80 percent. Consider keeping storm windows up all year.
3. See the Extreme Heat Safety Checklist (Checklist 12 in Appendix) and Disaster Supplies Kit (checklist 2 in Appendix) for more information.

EMERGENCY WATER SHORTAGE

An emergency water shortage can be caused by prolonged drought, poor water supply management or contamination of a surface water supply source or aquifer. Water conservation is very important during emergency water shortages. Water saved by one user may be enough to protect critical needs of others. A checklist for employers and employees is provided. It lists specific practices at the office to reduce water consumption and conserve this most valuable resource. (Water Conservation Checklist - Checklist 13 in Appendix)

WINTER STORMS AND EXTREME COLD

Winter storms and extreme cold immobilize an entire region. Even in areas that normally experience mild winters. it is possible to be hit with a major event with impacts such as flooding, storm surge, closed highways, blocked roads, downed power lines and hypothermia. Two industries that are most susceptible to economic loss from the extreme cold are agriculture and tourism.

Preparedness is key to protecting your business, customers and employees. Again, be prepared to evacuate if flooding is imminent and advised by local officials. Prepare a disaster supplies kit for your facility and call-down procedures for communicating with employees.

See Winter Storms Safety Checklist (Checklist 14 in Appendix A) for safety tips.

AGRICULTURAL DISEASES AND PESTS

- An outbreak of serious disease on crops or livestock can set off a chain reaction that would include:
- Direct economic losses (herd destruction, containment measures, disposal of dead animals).
- Rise in consumer prices for meat.
- Compensation to farmers.
- Agricultural industry layoffs and unemployment.
- Impact on retail food business and restaurant industries (both from increased prices and from loss of business because of consumer fear).
- Trade restrictions, loss of exports, and drop in international trade. (A very small outbreak can prompt international export restrictions.)

The largest recent animal disease outbreak in the United States occurred in 1983-84, when avian influenza swept through Pennsylvania and neighboring states. Poultry prices for consumers jumped by $350 million. A 6-month eradication plan cost the federal government $63 million.

American officials say that a food contamination scare similar to the one that hit the Belgium poultry industry in the late 1990s could jeopardize $140 billion in annual U.S. agricultural exports. Soybean rust could wipe out an $8 billion/year industry. Asian longhorn beetles could be used to kill maple trees and cripple syrup production in New England. Any targeted agricultural industry could suffer catastrophic losses.

In 1970 leaf blight destroyed about $1 billion worth of corn in the United States. Between 1993 and 1998 fusarium head blight affected successive wheat harvests in the Dakotas, Minnesota, and Manitoba. The disease spread over 10 million acres, probably with the help of abnormally wet weather and cost an estimated $1 billion in lost production.

Diseases that can be passed to humans would have an even greater impact. In 1988 the value of British beef and beef products was estimated at US $880 million. After bovine spongiform encephalopathy (BSE, or "mad cow disease") emerged, its value dropped considerably. After a 1996 announcement of a probable link between consumption of BSE-affected meat and a new variant of Creutzfeld-Jakob disease in humans, the value fell to zero.

DISEASE TRANSMISSION AMONG ANIMALS

Animal diseases can be spread in three primary ways.

- Airborne transmission - Some diseases (e.g., foot-and-mouth (FAM) disease, avian influenza, Newcastle disease) can travel in aerosol form very long distances in the air. (In 1981 FAM broke out in France and traveled 175 miles to Great Britain in 3 days.) Airborne diseases are extremely difficult to contain and would present an enormous challenge to

emergency responders in the event of an outbreak. These diseases can also be transmitted by direct contact.

- Direct contact - Some diseases (e.g., FAM, rinderpest, vesicular stomatitis, hog cholera, African swine fever) can be spread by direct contact among animals, contact with contaminated objects such as feed and water troughs, milking machines and other equipment, and people's clothes and shoes. This makes biosecurity measures, keeping animal facilities clean and restricting human and vehicle traffic around animals absolutely critical.
- Vectors - Some diseases (e.g., vesicular stomatitis, lumpy skin disease, Rift Valley fever, bluetongue, African swine fever) can be spread by other organisms, such as mosquitoes and ticks. In these cases, disease control depends on insect control.

TRANSMISSION OF ANIMAL DISEASES TO HUMANS

Some animal viruses are zoonotics; they can be transferred to another species including humans. Zoonotics usually do not affect humans in the same way they do animals. For example, FAM, vesicular stomatitis and Newcastle disease can be transmitted to humans, but the resulting illness is mild and not considered dangerous to human health. However, a few pathogens have been known to seriously harm humans. For example, people have died from avian influenza, and 74 cases of a new variant Creutzfeldt-Jakob disease (a fatal neurological disorder) have been linked to ingestion of BSE-infected beef products.

CROP DISEASES

Most crop diseases produce failed harvests rather than killing the plants outright. They do so by drastically reducing crop quality and quantity. Fungi present the biggest threat to crops. Crop diseases are caused by fungi, viruses and bacteria. These plant pathogens are transmitted by wind, water, or vectors. Because they depend heavily on environmental factors (e.g., temperature, humidity, rainfall, sunlight), the introduction of a pathogen does not necessarily result in widespread infection. There are three primary transmission modes of crop diseases.

- Airborne (Fungal Diseases) - Fungi produce dry spores, which are dispersed on the wind and can travel great distances. After a fungus has infected an area, it is very difficult to eliminate all of the spores. Although fungicides are helpful, fungi can persist in other hosts, allowing the disease to continue infecting plants for a long time.
- Vectors (Viruses and Bacteria) - Insects such as aphids are often virus carriers. When an aphid feeds on a leaf, it pierces cell walls and transmits the virus. Although viruses can be extremely damaging to crops, their ability to spread is limited by insect movement. Crop viruses are currently untreatable. Virus control depends on insect control and the use of virus-resistant crop strains. Insects also can transmit bacteria.
- Waterborne (Bacteria) - Bacteria require moisture for transmission. Although they cannot be transmitted on the wind, they can travel via wind-driven rain. Splashing rainwater can spread bacteria among individual plants, and irrigation runoff can spread bacteria over entire fields. Although bacteria can cause serious plant diseases, they generally cannot spread over vast areas.

CROP PESTS

Insects can damage crops directly. Infestations of particular insects can prompt export restrictions. (The Mediterranean fruit fly, or "Medfly," lays its eggs on many types of fruit on which the larvae later feed. If the Medfly became established in the United States, the USDA estimates that it would cost $1.5 billion per year in lost production and export restrictions.

The agriculture industry must be particularly vigilant in preparedness for natural disasters or intentional actions:

- Need for Surveillance

Surveillance is the first line of defense against a disease outbreak. U.S. agriculture relies

on ground surveillance, plant pathologists and field veterinarians for disease reporting. The greater the number of human monitors and the better trained they are to recognize diseases, the better the chance that serious diseases do not become widespread outbreaks. Disease outbreaks in wildlife also should be monitored because they can serve as early warning signs of agricultural outbreaks.

- Need for Quick Diagnosis

A fast diagnosis is critical in the case of a disease such as FAM, which can spread hundreds of miles during the time lag between when the disease is noticed and when a national lab confirms it. Currently there are no rapid screening tests for Foreign Animal Diseases (FADs). State labs do not routinely check for FADs because these diseases are so rare, and in some cases they do not have the resources to diagnose particular FADs. The samples have to be sent to a national lab. As a result, it can take several days for a FAD to be diagnosed.

PROTECTING AGAINST ANIMAL DISEASES

Bio-security is an important means of preventing the introduction of disease to farms, feedlots, and other livestock and poultry facilities. Bio-security should include the following.

- Keeping vehicles and people (e.g., non-business visitors) away from livestock and poultry buildings to prevent them from introducing or transmitting diseases.
- Isolating new animals from the rest of the herd for several days to let potential symptoms appear.

PROTECTING AGAINST PLANT DISEASES

Bio-security measures are unrealistic for crops. The primary protections against crop diseases include:

- Use of disease-resistant strains
- Herbicides and pesticides
- Crop Diversity

Review Steps to Protect Your Farm from Pests and Disease (Checklist 15 in the Appendix) to protect against a deliberate attempt to infect your crops or livestock.

EMERGENCY DISEASES AND PANDEMIC INFLUENZA

In 2005 the Avian Flu seemed poised to threaten the globe with millions of deaths, yet by 2007 our attention has been diverted by the war in Iraq, global warming and other pressing concerns and many feel there is no real threat of pandemic. However, the threat of a flu pandemic has hardly receded and world health experts are in agreement that a pandemic is inevitable (DRJ, Summer 2007). In the event of pandemic influenza, businesses and other employers will play a key role in protecting employees' health as well as mitigating the impact to the economy and the community. As with any disaster, preparedness is essential.

THE PANDEMIC SEVERITY INDEX

The US Department of Health and Human Services (HHS) has developed a Pandemic Severity Index, which uses case fatality ratio as the critical driver for categorizing the severity of a pandemic. Similar to the Saffir Simpson Hurricane Scale, future pandemics will be assigned to one of five categories of increasing severity (Category 1 to Category 5). The Pandemic Severity Index provides communities a tool for scenario-based contingency planning to guide local pre-pandemic preparedness efforts. Accordingly, communities facing the imminent arrival of pandemic disease will be able to use the pandemic severity assessment to define which pandemic mitigation interventions are indicated for implementation.

STRATEGIES TO MITIGATE THE IMPACT OF THE PANDEMIC IN THE COMMUNITY

The National HHS Pandemic Influenza Plan calls for community strategies that hopefully will significantly delay or reduce the impact of a pandemic (also called non-pharmaceutical interventions - NPI) until a vaccine is available. These community strategies could have a significant impact on business operations, employee health and welfare, the economy and the community as a whole. Communities, individuals and families, employers, schools, and other organizations will be asked to plan for the use of these interventions to help limit the spread of a pandemic, prevent disease and death, and lessen the impact on the economy and the functioning of society.

These interventions include the following:

1. Isolation and treatment (as appropriate) with influenza antiviral medications of all persons with confirmed or probable pandemic influenza. Isolation may occur in the home or healthcare setting, depending on the severity of an individual's illness and/or the current capacity of the healthcare infrastructure.
2. Voluntary home quarantine of members of households with confirmed or probable influenza case(s) and consideration of combining this intervention with the prophylactic use of antiviral medications, providing sufficient quantities of effective medications exist and that a feasible means of distributing them is in place.
3. Dismissal of students from school (including public and private schools as well as colleges and universities) and school-based activities and closure of childcare programs, coupled with protecting children and teenagers through social distancing in the community to achieve reductions of out-of-school social contacts and community mixing.
4. Use of social distancing measures to reduce contact among adults in the community and workplace, including, for example, cancellation of large public gatherings and alteration of workplace environments and schedules to decrease social density and preserve a healthy workplace to the greatest extent possible without disrupting essential services.

Refer to Checklist #29 for Strategies and Human Resource Policies to mitigate the impact of these community initiatives on your company operations, employees' health and your bottom line.

For more information:

The following provide information to guide business planning for a pandemic:

Business Pandemic Influenza Planning Checklist (www.pandemicflu.gov/plan/business/businesschecklist.html)

Pandemic Preparedness Planning for U.S. Businesses with Overseas Operations Checklist, (www.pandemicflu.gov/plan/business/businessesoverseaspdf.pdf)

Pandemic Influenza Preparedness, Response and Recovery Guide for Critical Infrastructure and Key Resources (www.pandemicflu.gov/plan/pdf/cikrpandemicinfluenzaguide.pdf)

In addition, recommendations for implementation of pandemic mitigation strategies are available at www.pandemicflu.gov. Reliable, accurate, and timely information on the status and severity of the pandemic also will be posted on www.pandemicflu.gov. Additional information is available from the Centers for Disease Control and Prevention (CDC) Hotline: 1-800-CDC-INFO (1-800-232-4636). This line is available in English and Spanish, 24 hours a day, 7 days a week. TTY: 1-888-232-6348. Questions can be e-mailed to cdcinfo@cdc.gov.

TECHNOLOGICAL HAZARDS

This section provides information on other hazards that may affect your business operations, including:

- Hazardous Materials
- Building Fire
- Power Service Disruption
- Environmental Health
- Terrorism
- Bomb threat
- Explosions and Detonation
- Building System Failure or Collapse
- Biological and Chemical Weapons
- Cyber-Attack
- Radiological Emergencies

HAZARDOUS MATERIAL INCIDENTS

Hazardous materials are substances that, because of their chemical nature, pose a potential risk to life, health or property if they are released. Affecting urban, suburban and rural areas, hazardous material incidents can range from a chemical spill on a highway to groundwater contamination by naturally occurring methane gas.

The good things chemicals bring into our lives are indispensable to us. From industrial chemicals to household detergents and air fresheners, hazardous materials are part of our everyday lives. Hazards can exist during production, storage, transportation, use or disposal.

Although major chemical emergencies are extremely rare, there always remains a chance that one will occur in the community despite the precautions that have been taken by the chemical users/producers and emergency responders. Knowing how to respond safely and appropriately to hazardous material emergencies greatly lessens the chance of serious injury and brings peace of mind. Many communities have Local Emergency Planning Committees (LEPCs) that identify industrial hazardous materials and keep the community informed of the potential risk.

The LEPC or your local emergency management agency can assist you in your planning efforts by providing the following information:

1. Warning Procedures in your local area, such as
   - Outdoor warning sirens or horns,
   - Emergency Alert System (EAS) - information provided via radio and television,
   - All-Call telephoning automated system for sending recorded messages,
   - News Media - radio, television, cable,
   - Residential route alerting - messages announced to neighborhoods from vehicles equipped with public address systems;
2. Community Plans for Response to a hazardous materials incident; and
3. Storage and use of hazardous chemicals in your local area.

Use this information to evaluate risks to your business. Determine how close you are to factories, freeways or railroads that may produce or transport toxic substances.

Be prepared to evacuate the building. An evacuation can last for a few hours or several days. See the Emergency Evacuation Procedures Checklist (Checklist 1 in Appendix) and Facility Disaster Supplies Kit (Checklist 2 in Appendix) for more important information.

Be prepared to Shelter in Place (Checklist 5 in Appendix). It may be determined by local officials that it is safer to stay indoors until the threat has dissipated rather than evacuate. If you are requested to stay indoors (shelter-in-place) rather than evacuate, follow the instructions given by emergency authorities.

An additional checklist has been provided to incorporate into your Business Continuity Plan: What to Do During and After a Hazardous Materials Incident (Checklist 16 in Appendix).

If your company uses, stores or generates potentially hazardous materials, you will need to comply with the requirements for the (1) safe handling, transport and disposal of all materials; (2) training of employees in safe practices and (3) development and exercise of emergency procedures. For specific information and guidance, contact your county emergency management agency or your local fire department.

All companies having hazardous chemicals must report annually to the State Emergency Response commission (SERC) for Hazardous materials and the Local Emergency Planning Committee (LEPC) under the Emergency Planning and Community Right-to-Know Act (EPCRA). For information on reporting requirements, go online to the SERC's website for the State's How-to-Comply Handbook, LEPC locations and all current reporting forms. (See Section IV. Resources: Preparedness Info Center, Website Links.)

BUILDING FIRE

Fire safety is important business. National Fire Prevention Week is intended to focus on the importance of fire safety in the home, in schools and at work. But workplace fire safety is the Occupational Safety and Health Administration's (OSHA) principal focus and saving lives and preventing injuries due to fire is a key concern.

According to National Safety Council figures, losses due to workplace fires in 1988 totaled $3.1 billion. Of more than 5,000 persons who lost their lives due to fires in 1988, the National Safety Council estimates 360 were workplace deaths.

When OSHA conducts workplace inspections, it checks to see whether employers are complying with these standards for fire safety. OSHA standards require employers to provide proper exits, fire fighting equipment, emergency plans and employee training to prevent fire deaths and injuries in the workplace.

1. **Building Fire Exits**
   - Each workplace building must have at least two means of escape remote from each other to be used in a fire emergency.
   - Fire doors must not be blocked or locked to prevent emergency use when employees are within the buildings.
   - Delayed opening of fire doors is permitted when an approved alarm system is integrated into the fire door design.
   - Exit routes from buildings must be clear and free of obstructions and properly marked with signs designating exits from the building.
2. **Portable Fire Extinguishers**
   - Each workplace building must have a full complement of the proper type of fire extinguisher for the fire hazards present.
   - Employees expected or anticipated to use fire extinguishers must be instructed on the hazards of fighting fire, how to properly operate the fire extinguishers available and what procedures to follow in alerting others to the fire emergency.
   - Only approved fire extinguishers are permitted to be used in workplaces, and they must be kept in good operating condition. Proper maintenance and inspection of this equipment is required of each employer.
   - Where the employer wishes to evacuate employees instead of having them fight small fires there must be written emergency plans and employee training for proper evacuation.

3. **Emergency Evacuation Planning**
   - Each employer needs to have a written emergency action plan for evacuation of employees that describes the routes to use and procedures to be followed by employees.
   - Also, procedures for accounting for all evacuated employees must be part of the plan.
   - The written plan must be available for employee review.
   - Where needed, special procedures for helping physically impaired employees must be addressed in the plan. The plan must include procedures for employees who must remain behind temporarily to shut down critical plant equipment before they evacuate.
   - The preferred means of alerting employees to a fire emergency must be part of the plan. An employee alarm system must be available throughout the workplace complex and must be used for emergency alerting for evacuation.
   - The alarm system may be voice communication or sound signals such as bells, whistles or horns. Employees must know the evacuation signal.
   - Training all employees in emergency procedures is required.
   - Employers must review the plan with newly assigned employees so they know correct actions in an emergency as well as with all employees when the plan is changed.
4. **Fire Prevention Plan**
   - Employers need to implement a written fire prevention plan to minimize the frequency of evacuation. This prevention plan complements the evacuation plan. Stopping unwanted fires from occurring is the most efficient way to handle them. The written plan should be available for employee review.
   - Housekeeping procedures for storage and cleanup of flammable materials and flammable waste must be included in the plan. Recycling of flammable waste such as paper is encouraged. However, handling and packaging procedures must be included in the plan.
   - A procedure for controlling workplace ignition sources such as smoking, welding and burning must be addressed in the plan. Heat producing equipment such as burners, heat exchangers, boilers, ovens, stoves and fryers must be properly maintained and kept clean of accumulations of flammable residues. Flammables are not to be stored close to those pieces of equipment.
   - All employees are to be apprised of the potential fire hazards of their job and the procedures called for in the employer's fire prevention plan. The plan shall be reviewed with all new employees when they begin their job and with all employees when the plan is changed.

5. **Fire Suppression System**
   - Properly designed and installed fixed fire suppression systems enhance fire safety in the workplace. Automatic sprinkler systems throughout the workplace are among the most reliable fire fighting means. The fire sprinkler system detects the fire, sounds an alarm and puts the water where the fire and heat are located.
   - Automatic fire suppression systems require proper maintenance to keep them in serviceable condition. When it is necessary to take a fire suppression system out of service while business continues, the employer must temporarily substitute a fire watch of trained employees standing by to respond quickly to any fire emergency in the normally protected area. The fire watch must interface with the employer's fire prevention plan and emergency action plan.
   - Signs must be posted about areas protected by total flooding fire suppression systems that use agents that are a serious health hazard, such as carbon dioxide or Halon 1211. Such automatic systems must be equipped with area pre-discharge alarm systems to warn employees of the impending discharge of the system and allow time to evacuate the area. There must be an emergency action plan to provide for the safe evacuation of employees from within the protected area. Such plans are to be part of the overall evacuation plan for the workplace facility.

Checklists to assist you in planning for building fires have been provided:

- Emergency Evacuation Procedures (Checklist 1)
- Fire Safety Checklist (Checklist 17)

POWER SERVICE DISRUPTION

Power Service Disruption can be the result of a weather event, an accident or a terrorist attack. There are some physical measures a business can take to be prepared for power service disruptions (i.e., surge protectors or backup generation for critical equipment). As in the case of any other emergency, the business owner needs to address liabilities, risks and response activities in advance.

An emergency plan can include some of the following measures:

1. Facility

   If your lights fail, first try checking your breakers or fuses. Re-setting the breakers or putting in new fuses may bring your lights back on. To reset a breaker, turn it to the OFF position, press firmly off, and then push to the ON position. If re-setting the breaker or replacing the fuses does not help, call your local electric utility. If using back-up generation, what are your procedures to avoid "backfeed"?

2. Medical Emergency

   In the case of a medical emergency during a power outage, employees should seek immediate care at the nearest appropriate health care facility. Please note that some telephones require electricity and may not be in service during an outage. Businesses are encouraged to have a back-up communication plan in case of such an event.

3. Facility Protection and Security
   - Determine your threat level and communicate to employees.
   - Employers are encouraged to develop a business security plan. Included in this plan should be security processes dealing with power outages/disruptions. For example, will you need security guards if your alarm system is not functioning?
   - Be on the alert for fires and call authorities if smoke or fire is spotted.
   - What to do if you have another emergency during the outage (e.g., material spill).
   - What to do if water enters your facility. What equipment could you use when the lights come back on?
   - Procedure for re-entering the building. (See Preparedness Brochure in Resource Section).

4. Employee Field Work
   - Inform personnel that any fallen wire is potentially hazardous.
   - Inform personnel how to deal with a fallen power line on their car.

5. Communications
   - Inform the employees how they will be communicating with their supervisor or employer if they are in the field during a large-scale power outage.
   - Publish a telephone number to be used by employees to call their supervisor and be prepared to provide reporting instructions.
   - Make appropriate communication to your customers.

ENVIRONMENTAL HEALTH

Indoor air quality has become a major concern for businesses as well as the insurance industry. Primary threats to the environmental health of your business will include mold.

Molds are small organisms found almost everywhere, inside and outside, on plants, foods and dry leaves. They can be nearly any color – white, orange, green or black. Molds are beneficial to the environment and are needed to break down dead material. Very tiny and lightweight, mold spores travel easily through the air.

Most building surfaces provide adequate nutrients to support the growth of mold. When mold spores land on material that is damp – for example, walls, floors, appliances (such as humidifiers or air conditioners), carpet or furniture – they can begin to multiply. When molds are present in large numbers, they may cause allergic symptoms similar to those caused by plant pollen.

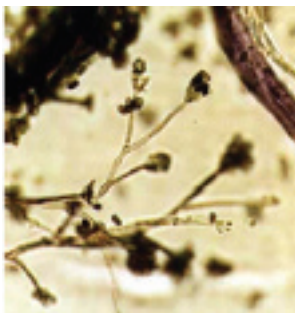
What does mold need to grow?

- A food source such as leaves, paper, wood or dirt,
- A source of moisture and a place to grow.

What are sources of moisture in your business?

- Flooding
- After a fire (fire suppression)
- Leaky roofs
- Humidifiers
- Damp basements or crawl spaces
- Constant plumbing leaks
- Clothes dryers vented indoors

You and your employees are exposed to some mold every day, usually by touching, eating or breathing it. When mold is growing on a surface, spores can be released into the air where they can be easily inhaled. A person who ingests or inhales a large number of spores may suffer adverse health effects.



Health Effects - Exposure to any mold could cause health effects (e.g., allergic symptoms such as watery eyes, a runny nose, sneezing, nasal congestion, itching, coughing, wheezing, difficulty breathing, headache and fatigue) under the right conditions. Similarly, the same amount of mold may cause health effects in one person, but not in another. Some people are more sensitive to molds than others, including infants and children, elderly persons, immune compromised patients (i.e., people with HIV infection, cancer, liver disease, etc., or who are under-going chemotherapy) and individuals with existing respiratory conditions, such as allergies and asthma.

When airborne mold spores are present in large numbers, they can cause skin irritation, allergic reactions, asthma episodes, infections and other respiratory problems for people. Exposure to high spore levels can cause the development of an allergy to the mold. Mold also can cause structural damage to your building(s).

Testing for molds is not difficult. Kits are sold at home improvement stores but it takes a trained professional to determine what kind of molds are present. Testing should be done under the following circumstances:

- When occupants are at risk: infants and young children, adults on certain medications, older adults with diminished immune systems, individuals with existing respiratory conditions;
- Occupants indicate current health problems: runny nose, burning eyes, sore throat, and headache;
- To locate hidden mold;
- To discover what is the exposure and how much of a building is contaminated;

- To establish effective containments;
- Anytime a lawsuit is a possibility; and
- To determine when remediation is successful. Even if initial testing is not performed, it is recommended that a Clearance Test be performed to assure the environment is safe.

CLEAN-UP

If you experience flooding, carpets, paper and other absorbent materials can grow mold after getting soaked. In general, it is best to throw out those items. Other items made of glass or metal should be cleaned and disinfected.

It is important to make sure that the source of moisture is stopped before the mold is cleaned up. If this is not done, the mold will grow again. How you clean up areas contaminated with mold depends on the surface where the mold is growing. A professional should be consulted if large areas (more than 10 square feet) are contaminated with mold.

If the surface is non-porous (varnished wood, tile, etc.), you can take the following steps:

- The surfaces first need to be cleaned with soap.
- Use non-ammonia soap or detergent in hot water and scrub the entire area affected by the mold twice. Never mix bleach with ammonia; the fumes are toxic.
- Use a stiff brush or cleaning pad on block walls or uneven surfaces.
- Rinse clean with water.
- Let disinfecting areas dry naturally. The extended time is important to kill all the mold spores.

During the cleanup of molds, many spores may be released into the air. Mold counts in air are typically 10 to 1,000 times higher than background levels during the cleaning and removal of mold-damaged materials. To prevent health effects, there are several ways you can protect yourself while cleaning up the mold.

- Anyone with a chronic illness, such as asthma or emphysema, should not do the cleanup.
- Use a HEPA filter respirator or N95 mask purchased from a hardware store to reduce the mold spores you breathe in.
- Wear protective clothing that is easily cleaned or discarded.
- Wear rubber gloves and goggles.
- Do not allow employees or bystanders to be present when you are doing the cleanup.
- Work over short time spans and take breaks in a fresh air location.
- Open the windows in your building during and after the cleanup.
- Shut off heat or air conditioning to prevent mold spores from being spread around the office.
- Tightly seal the air return vent with 6 millimeter plastic.
- Turn on an exhaust fan or place a fan in a window to blow air out of the affected room to the outside. (Make sure the air is being blown outside the home, not into another room.)
- Double bag materials with 6 millimeter plastic bags before you remove them from a contaminated area.

If you have any questions, there are websites that provide good information on this issue. The www.epa.gov/iaq gives the Environmental Protection Agency (EPA) position on indoor air quality for both commercial and residential properties. The Indoor Air Quality Association represents a majority of the industry's position and is located at www.iaqa.org . The IICRC, Institute of Inspection, Cleaning and Restoration Certification has written the Standard for Water Damage Restoration and provides guidance as to how and what can be restored. They are located at www.iicrc.org.

TERRORISM

In addition to the natural and technological hazards, Americans face threats posed by hostile governments or extremist groups. These threats to national security include acts of terrorism and acts of war.

Terrorism is the use of force or violence against persons or property for purposes of intimidation, coercion or ransom. Terrorists often use threats to create fear among the public, to erode the citizens' confidence in their government and to get immediate publicity for their causes.

Acts of terrorism range from threats of terrorism, assassinations, kidnappings, hijackings, bomb scares and bombings and cyber attacks (computer-based) to the use of chemical, biological and nuclear weapons.

High-risk targets include military and civilian government facilities, international airports, large cities and high profile landmarks. Terrorists might target large public gatherings, water and food supplies, utilities and corporate centers. Further, they may spread fear by sending explosives or chemical and biological agents through the mail.

In the immediate area of a terrorist event, you need to rely on emergency management, law enforcement, fire and other officials for instructions. However, you can prepare in much the same way you and your employees would prepare for other crisis events.

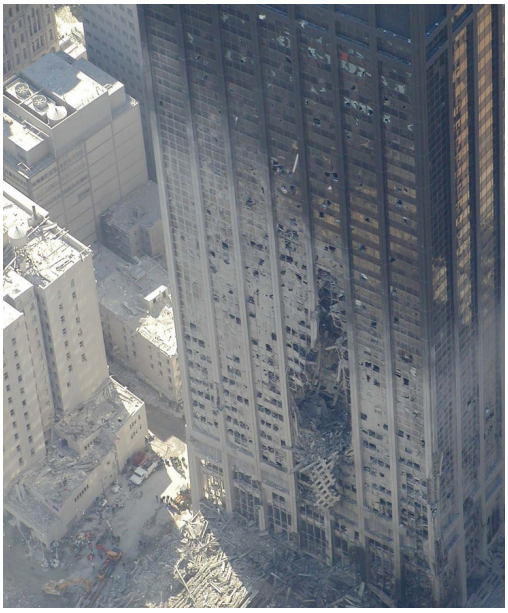
- Wherever you are, be aware of your surroundings.
- Take extra precautions when traveling.
- Notice where emergency exits are located. Plan how to get out of a building, subway or congested public area or traffic. Note where staircases are located.
- Assemble a disaster supply kit at work and at home.
- Training (e.g., be familiar with different types of fire extinguishers and how to locate them, first aid, CPR).
- Be prepared to do without services you normally depend on that could be disrupted - electricity, telephone, natural gas, gasoline pumps, cash registers, ATM machines and Internet transactions.
- Be prepared to respond to official instructions such as Evacuation of the Building or area or Shelter-in-Place.

BOMB THREATS

If you receive a bomb threat, get as much information from the caller as possible. Keep the caller on the line and record everything that is said. Then notify the police and the building management. See Bomb Threat Procedures Checklist (Checklist 20 in Appendix). Keep next to all employees who may answer the phones.

If you are notified of a bomb threat, do not touch any suspicious package. Clear the area around a suspicious package and notify the police immediately. When evacuating a building, do not stand in front of windows, glass doors or other potentially hazardous areas. Do not block sidewalk or streets to be used by emergency officials or others still exiting the building. See Handling Suspicious Parcels and Letters Checklist (Checklist 24 in Appendix).

BUILDING EXPLOSION



Explosions can collapse buildings and cause fires. People who work in a multi-level building can do the following:

1. Review emergency evacuation procedures. Know where all emergency exits are located. Insure that stairwells have working emergency lighting.
2. Keep fire extinguishers in working order, know where they are located, and learn how to use them. Learn first aid.
3. Contact the local chapter of the American Red Cross for information and training.
4. Building owners should keep the following items in a designated place on each floor of the building:

- Portable, battery-operated radio and extra batteries
- Several flashlights and extra batteries
- First aid kit and manual
- Several hard hats
- Tools to clear blockages to exits
- Fluorescent tape to rope off dangerous areas

Employees should be trained to follow the procedures in the checklist that call for the immediate evacuation of the building (See Checklist 1). Procedures should be in place to implement (1) an immediate warning of all personnel, (2) notification of local emergency officials and (3) verification of evacuation and safety of all employees.

BUILDING SYSTEM FAILURE OR COLLAPSE

See Emergency Evacuation Procedures (Checklist 1 in Appendix)

CHEMICAL AND BIOLOGICAL WEAPONS

Chemical Agents - Chemical warfare agents are poisonous vapors, aerosols, liquids or solids that have toxic effects on people, animals or plants. They can be released by bombs, sprayed from aircraft, boats or vehicles, or used as a liquid to create a hazard to people and the environment. Some are odorless and tasteless. They can have an immediate effect (a few seconds to a few minutes) or a delayed effect (several hours to several days). While potentially lethal, chemical agents are difficult to deliver in lethal concentrations. Outdoors, the agents often dissipate rapidly. Chemical agents are also difficult to produce.

There are six types of agents:

- Lung-damaging (pulmonary) agents such as phosgene,
- Cyanide,
- Vesicants or blister agents such as mustard,
- Nerve agents such as GA (tabum), GB(sarin), GD (soman), GF and VX,
- Incapacitating agents such as BZ, and
- Riot-control agents (similar to MACE).

Biological Agents

A terrorist incident involving a biological agent has the potential to cause a widespread medical emergency. The most likely bioterrorist scenario is a covert incident; that is, the biological agent will be released without warning or claim of responsibility.

Because many biological agents produce effects that initially appear to be normal flu symptoms, the true nature of an attack may go undetected for a while. In most cases, there probably will be no identifiable crime scene, no explosion and no fire.

In this scenario, detection of a bio-terrorism incident will occur as increasing numbers of infected people seek medical care, and alert medical personnel and public health practitioners recognize that an unusual event is happening and report it to their response partners. Thus, it is likely to be medical detection and diagnosis, with the emergence of unusual patterns of illness which will trigger an investigation into the possibility of a terrorist incident.

Meanwhile, the disease may spread well beyond the initial point of attack, either through contagion or through movement of the biological agent itself. If the release is overt, the event may unfold more quickly, but serious health effects and public requests for information and treatment may still overwhelm the system.

Biological agents are organisms or toxins that can kill or incapacitate people, livestock and crops. The three basic groups of biological agents which would likely be used as weapons are bacteria, viruses and toxins.

1. **Bacteria** – Bacteria are small free-living organisms that reproduce by simple division and are easy to grow. The diseases they produce often respond to treatment with antibiotics.
2. **Viruses** – Viruses are organisms which require living cells in which to reproduce and are intimately dependent upon the body they infect. Viruses produce diseases that generally do not respond to antibiotics. However, antiviral drugs are sometimes effective.
3. **Toxins** – Toxins are poisonous substances found in, and extracted from, living plants, animals or microorganisms. Some toxins can be produced or altered by chemical means. Some toxins can be treated with specific antitoxins and selected drugs.

Most biological agents are difficult to grow and maintain. Many break down quickly when exposed to sunlight and other environmental factors. Others, such as anthrax spores, are very long-lived. They can be dispersed by spraying them in the air or infecting animals which carry the disease to humans as well through food and water contamination.

- Aerosols – Biological agents are dispersed into the air, forming a fine mist that may drift for miles. Inhaling the agent may cause disease in people or animals.
- Animals – Some diseases are spread by insects and animals, such as fleas, mice, flies, and mosquitoes. Deliberately spreading diseases through livestock also is referred to as agri-terrorism.
- Food and water contamination – Some pathogenic organisms and toxins may persist in food and water supplies. Most microbes can be killed and toxins de-activated by cooking food and boiling water.
- Anthrax spores formulated as a white powder were mailed to individuals in the government and media in the fall of 2001. Postal sorting machines and the opening of letters dispersed the spores as aerosols. Several deaths resulted. The effect was to disrupt mail service and to cause a widespread fear among the public of handling delivered mail.
- Person-to-person spread of a few infectious agents is also possible. Humans have been the source of infection for smallpox, plague, and the Lassa viruses.

METHODS OF DISSEMINATION

Chemical and biological agents can be dispersed in the air we breathe, the water we drink or on surfaces we physically contact. Dispersion methods may be as simple as opening a container, using conventional (garden) spray devices, or as elaborate as detonating an improvised explosive device.

Chemical incidents are characterized by the rapid onset of medical symptoms (minutes to hours) and easily observed signatures (colored residue, dead foliage, pungent odor or dead insects and animals).

Biological incidents are characterized by the onset of symptoms in hours to days. Typically, there will be no characteristic signatures because biological agents are usually odorless and colorless. Because of the delayed onset of symptoms in a biological incident, the area affected may be wider due to the movement of infected individuals.

Potential targets include highly populated areas, enclosed public spaces (e.g., shopping malls, office buildings, sports/ entertainment arenas and mass transit), crops and livestock.

DISSEMINATION THROUGH THE WATER SUPPLY

Potential targets include municipal water supply, enclosed water supplies and bottled water processing plants. Your plan should consider the following relevant factors:

- Contaminating large municipal water supplies may be difficult because water purification and sterilization processes that typically use chlorine or ozone will kill most biological agents.
- Smaller targets (e.g., water supply in a building) can be attacked by introducing an agent directly into the water tank.

DISSEMINATION THROUGH THE FOOD SUPPLY

The intentional infection of a food supply (agri-terrorism) is a serious concern. For businesses related to agriculture there is information on the use of biological agents to infect the food supply, see Steps to Protect Your Farm for Pests and Disease (Checklist 15 in Appendix) .

- Potential dissemination devices include aerosols, sprays, crop dusters, and liquid additives.
- Potential targets may include food crops and livestock using food processing plants (e.g., dairies, meatpacking) imported foods and food additives and restaurants.

PREVENTION

Prevention is key to minimizing risk. Measures to prevent those who have been exposed from developing an infection include the following methods:

- Barrier protection (e.g., use of protective suits or sealed buildings to prevent the intake of contaminated air).
- Sterilization and disinfection (using chemicals, heat, irradiation, filtration to kill pathogens or reduce their numbers to safe limits).
- Public health hygiene and personal hygiene (e.g., soap and water).
- Processing food to kill pathogens or inactivate toxins.
- Vaccination to create immunity to the disease.

WORKER PROTECTION

In the event of a terrorist incident involving an infectious biological agent, certain workers may be at risk of infection.

- First Responders (police, fire, EMS) who transport ill patients to medical facilities.
- Health care workers who care for patients.
- Laboratory personnel who handle clinical specimens.
- Health department staff who visit patients during outbreak assessment or control.

Because bio-terrorism attacks may be covert, these workers may be unaware of the presence or nature of a biological agent. Therefore, workers need to use standard prophylactic precautions (disposable gloves and gown, immediate hand-washing and face shield) to protect themselves when in contact with broken or moist skin, blood or body fluids. Protective gear must be changed between patients to prevent transmission.

Persons affected by biological or chemical agents require immediate attention by professional medical personnel. If medical help is not immediately available, decontaminate yourself and assist others. Decontamination procedures are listed in the checklist, " Checklist to Prepare and Respond to a Chemical/ Biological Attack" (Checklist 23).

SUSPICIOUS PARCELS AND LETTERS

Be wary of suspicious packages and letters. They can contain explosives, chemical or biological agents. Be particularly cautious at your place of business.

Refer to the checklist "Handling Suspicious Parcels and Letters" Checklist 24 in Appendix.

CYBER-ATTACKS

Cyberterrorism is distinct from computer crime, economic espionage and "hactivism" although terrorists may employ any of these forms of computer abuse to further their agendas. Cyberterrorism is the "unlawful attacks and threats of attack against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or ...cause enough harm to generate fear." (Denning, Dorothy E. "Cyberterrorism" August 2000.)

In other words, the weapons of cyberterrorism and computers may differ from chemical, biological and explosives weapons in that they do not cause direct injury or death. They can cause serious consequences to individuals, businesses, industry, government and the public at large. Depending on how they are used, they can lead to injury and death (e.g., the ring leader of the 1993 World Trade Center bombing used encryption technology in his failed plot to blowup U.S. airliners in the Far East).

The following are some general types of cyberterrorism:

1. **Data destruction or corruption** - Using viruses, installation of malicious code, or other means to damage a system from within. This can include destroying or corrupting files, changing data in a database or corrupting software programs within the system.
2. **Penetration of a system to modify its output** - Embedding code (e.g., Trojan horses or "logic bombs") to perform unauthorized functions at a later time.
3. **Theft** - System penetration with the goal of stealing information or sensitive data (e.g., password cracking and theft, "packet sniffing").
4. **Disabling a system** - Disruption of information structures (e.g., using e-mail bombings, spamming, denial-of-service attacks, or viruses) to crash or disable a system.
5. **Taking control of a system** - Taking over a system (e.g., an air traffic system, a manufacturing process control system, a subway or train system, a 911 communications system) to use it as a weapon.
6. **Website defacement** - Hacking into a website and changing its contents to spread misinformation, incite to violence, generate fear, or create chaos.
7. **Terrorist groups** use of websites, chat rooms, and encrypted e-mail to plan physical acts of terrorism, raise funds for terrorism, provide instructions to fellow terrorists, provide instructions on how to build bombs, spread hate propaganda, and/or recruit members.

The following table describes some of the tools that can be used by cyberterrorists to cause disruption and damage.

Tool	Description
HERF Gun	The High Energy Radio Frequency Gun. Directs a blast of high-energy radio signals at a selected target to disable it, at least temporarily. A HERF Gun can shoot down a computer, cause an entire network to crash or send a telephone switch into electronic chaos. Any of these effects can create denial-of-service scenarios. A HERF Gun is simple and easy to build.

Tool	Description
EMP/T Bomb	Electro-Magnetic Pulse Transformer Bomb, operates similarly to a HERF Gun, but is many times more powerful and causes permanent damage. According to a 1980 FEMA report5, the following hardware would be most susceptible to failure from EMP: • Computers, computer power supplies and transistorized power supplies. • Semiconductor components terminating long cable runs (especially between sites). • Alarm systems and intercom systems. • Life support system controls. • Telephone equipment. • Transistorized receivers, transmitters and process control systems. • Power control systems. • Communications links. Detonated over a dense urban area, EMP/T Bombs could take out all communications and electronic equipment and cause a blackout.
System Intrusion	Unauthorized entry into a system (hacking) can be used for information gathering, information alteration, and sabotage.
Emissions Capture	Various tools are available for capturing vital information/secrets such as passwords or data. Packet sniffing (below) is one approach. Van Eck emissions enable hackers to capture the contents of computer screens from up to 200 meters away. Devices designed to capture these emissions can be developed at very low cost.
Virus	A program that can attach itself to legitimate files and propagate, spreading like an infectious disease from computer to computer as files are exchanged between them. The virus hides until a certain criterion is met, then attacks the system by erasing files, destroying hard disk drives or corrupting databases.
Worm	Operates much like a virus but can travel along a network on its own.
Trojan Horse	A program that pretends to be a benign program but is really a program of destruction. When the user runs the program, it can perform the same kind of destruction as a virus.
E-mail Bombing	Flooding a site with so many e-mails that the system becomes paralyzed.
Logic Bomb	Unauthorized code that creates havoc when a particular event occurs, such as upon a certain date.
Packet Sniffing	Installing a software program on a network that monitors packets sent through the system and captures those that contain passwords and user IDs.
Spamming	Flooding a system with massive numbers of a message.
Sustainable Pulsing	Repeated convergence, redispersion and recombination of small, dispersed, internetted forces against a succession of targets.
Swarming	Unleashing multiple attacks on a cyberspace target from all directions at once.
Denial-of-Service Attack	Causing internal damage to a server, or overloading a site with “hits,” to the extent that service is denied to authorized users.
Web Sit-in	Mass convergence on a website to overload the site (e.g., with rapid and repeated download requests).

Of greatest concern for emergency planners are terrorist attacks intended to interfere with national life support systems. Systems of greatest priority are below:

- Telecommunications
- Banking and finance
- Electrical power
- Oil and gas distribution and storage
- Water supply
- Transportation

- Emergency services
- Government services

Improving security involves:

1. Knowing what data and processes need to be protected,
2. Recognizing the threats and judging possible impacts,
3. Calculating the risks and deciding what level of risk is acceptable,
4. Developing/implementing countermeasures to reduce the risk to an acceptable level, and
5. Testing and tuning the countermeasure strategy to ensure security.

As with all other hazards,

1. Be prepared to do without services you normally depend on that can be disrupted—electricity, telephone, natural gas, gasoline pumps, cash registers, ATM machines and internet transactions.
2. Be prepared to respond to official instructions if a cyber-attack triggers other hazards requiring general evacuation, evacuation to shelter, or shelter-in-place, because of hazardous materials releases, a nuclear power plant incident, or a dam or flood control system failure.

Refer to Cyber-Security Checklist (Checklist 22 in Appendix) for more information.

RADIOLOGICAL EMERGENCIES IN THE WORKPLACE

Radiation cannot be recognized or detected through the use of our five senses. It is important that everyone in your business understand that some basic immediate precautions need to be followed when exposure to a radiation source is suspected or if they have been exposed to a container with the following marking.

CAUTION - RADIOACTIVE MATERIAL
The trefoil, or three-leaf, is the standard radiation symbol used on many radiological postings and labels: The symbol could also be black on yellow.

Many businesses use equipment and instruments that house radioactive sources. Plans should be developed to address hazards resulting from the use and disposal of this type of equipment. Florida businesses that use equipment that house a radioactive source need to be in compliance with the Department of Health (DOH) radiation control regulations. They may need a permit to operate the equipment.

IMMEDIATE PRECAUTIONS

1. Notify your Facility Radiation Safety Officer (if applicable), 911, the local authorities and Radiation Control Authority on Accident Conditions. Follow applicable permit and regulatory requirements.
2. Notify 911 of the possible presence of radioactive materials.
3. Isolate hazard area in accordance with your ALARA (As Low As reasonably Achievable) plan and restrict access.
4. Do not touch containers.
5. Upon arrival of Law Enforcement or Fire Department, inform the First Responder that radioactivity may be present.
6. In the case of fire, do not attempt to move containers out of fire zone. Retreat to a safe area and wait for local authorities. Please note, radioactivity does not change flammability or properties of other materials.
7. In the case of a medical emergency, use First Aid treatment according to the nature of the injury.
8. Advise medical personnel that victim may be contaminated with radioactive material.
9. Detain persons exposed to radioactive material until arrival or instruction of Radiation Control Authority. Potential route of exposure can include inhalation, ingestion or breaks in skin.
10. Include business specific information in your emergency plans. Inform the employees regarding radiation safety. Follow your ALARA plan. Publish a telephone number to be used by employees to call their supervisor and be prepared to provide reporting instructions.

RADIOLOGICAL EMERGENCIES IN THE CASE OF A TERRORIST ATTACK

There are many questions regarding the likelihood of whether terrorists would use radioactive materials in attacks. Radioactive materials are hard to handle and the impact to the public would not be as tangible or visible after an attack.

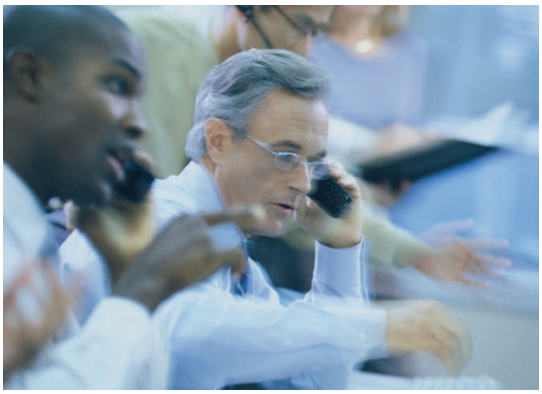
Different methods can be used in a radiological terrorist attack. A weapon can include explosion as a mechanism to disperse radiation as in the case of a dirty bomb or it could be more "passive" and include exposing the public to radioactive sources from gauges used in industry or radioactive waste.

IMMEDIATE PRECAUTIONS

1. As mentioned above, radiation cannot be seen, smelled, felt or tasted by humans. Therefore, if people are present at the scene of an explosion, they will not know whether radioactive materials were involved at the time of the explosion.
2. If people are not too severely injured by the initial blast, they should follow these steps.

    - Leave the immediate area on foot. Do not panic. Do not take public or private transportation such as buses, subways or cars. If radioactive materials were involved, they may contaminate cars or the public transportation system.
    - Go inside the nearest building. Staying inside will reduce people's exposure to any radioactive material that may be on dust at the scene.
    - Remove their clothes as soon as possible, place them in a plastic bag and seal it. Removing clothing will remove most of the contamination caused by external exposure to radioactive materials. Saving the contaminated clothing would allow testing for exposure without invasive sampling.
    - Take a shower or wash themselves as best they can. Washing will reduce the amount of radioactive contamination on the body and will effectively reduce total exposure.
    - Be on the lookout for information. Once emergency personnel can assess the scene and the damage, they will be able to tell people whether radiation was involved.
    - Even if people do not know whether radioactive materials were present, following these simple steps can help reduce their injury from other chemicals that might have been present in the blast. For more information go to the Center for Disease Control website (www.CDC.gov) or contact: Department of Health - Bureau of Radiation Control, P.O. Box 680069, Orlando, FL 32868-0069, Telephone: (407) 297-2095, or see link to www.CDC.gov.

OTHER BUSINESS INTERRUPTION HAZARDS



This section provides information on other hazards which may affect your business operations, including:

- Violence in the Workplace
- Sabotage, Fraud and Theft
- Loss of Key Staff
- Civil Unrest
- Workforce Disruption
- Adjacent Hazards

VIOLENCE IN THE WORKPLACE

The statistics on workplace violence are alarming. On average, one in six violent crimes is committed in the workplace. Studies also show that 20 people are murdered and 18,000 are assaulted at work each week. A 1996 survey by the Society of Human Resource Management found that about half of the managers surveyed knew of at least one violent incident at their organization in the past two years.

Beyond the loss of life and extreme emotional toll, workplace violence can generate significant legal costs. Many employees and third parties are suing employers for the effects of workplace violence. The National Safe Workplace Institute estimates that the average cost to employers of a single episode of workplace violence can amount to $250,000 in lost work time and legal expenses.

LIABILITY: HOW VIOLENCE IN THE WORKPLACE CAN AFFECT YOUR BUSINESS?

On May 4, 1999, a North Carolina jury concluded that the defendant-employers failed to take adequate precautions for the safety of their employees and awarded $7.9 million to the families of two men killed at work by an estranged employee. Allman v. Dormer Tools, No. 97CVS1161 (N.C. Sup. Ct., May 4, 1999); Knox v. Union Butterfield, No. 07CVS2012 (N.C. Sup. Ct., May 4, 1999).

On April 28, 1999, the Oregon Court of Appeals upheld a jury award for $1.25 million for punitive damages and $275,000 for compensatory damages to an injured employee whose supervisor knew of a patient's violent history and refused to return to work, instructing the plaintiff to remain alone at the facility, after she had been assaulted by a patient. MacCrone v. Edwards Center, Inc., 980 P.2d 1156 (Or. Ct. App. 1999).

Additionally, Allstate Insurance was sued by families of victims of workplace violence for failing to tell the Fireman's Fund in a reference check about a former employee's unstable mental condition and that he frequently brought guns to work. Carl Cronan, Workplace Violence Can be Costly in Many Ways, The Business Journal, December 21, 1998.

Florida recently enacted legislation to help employers decrease liability and the potential for workplace violence. Failure to take advantage of this new legislation may be costly, both in liability and harm to employees (Fla. Stat. § 768.096). This new law creates a presumption against negligent hiring if an employer conducts a reasonable background investigation.

While Florida courts have yet to clarify this law, in order to ensure compliance, the background investigation should include: (a) a criminal background investigation through the Florida Department of Law Enforcement, (b) a reasonable effort to contact an applicant's references and former employers, (c) a job application with questions about criminal convictions and several claims for intentional torts, (d) with written authorization, a check of his or her driver's license record if relevant to the work the employee will be performing and can reasonably be obtained, and (e) an interview of the prospective employee.

Employers conducting a criminal background check on a prospective employee can contact the Florida Department of Law Enforcement and receive a report of the individual's criminal history in Florida for only $15.

In conducting a reference check, Florida tort reform also establishes immunity for employers who provide information about a current or former employee to a prospective employer unless it is shown by clear and convincing evidence that the information disclosed was knowingly false or violated any civil rights of the employee. (Fla. Stat. § 768.095.)

In addition to maintaining strict hiring policies, employers also should establish a written workplace anti-violence policy and security procedures with zero tolerance for any incidents of workplace violence. Liability for workplace violence does not stop at just claims for negligent hiring, there is also potential for liability under the theory of negligent retention of an employee. Similar to employers who have procedures for investigating workplace harassment, employers should also have a system in place to deal with claims of workplace violence. The employer's written policies and security procedures that establish zero tolerance for this kind of behavior should list exactly what type of conduct is prohibited. In addition, employers should train supervisors and managers on how to recognize a problem and how to adequately resolve it. Remember to always maintain an environment that is both open to communication and respectful to all employees.

It is important to keep in mind that, while attempting to keep a workplace free from violence, an employer must balance this with a workplace that is also free of discrimination. Despite the protections of the Florida Tort Reform, employers should still be cognizant that the Federal Civil Rights Act of 1964, as amended, prevents an employer from discriminating against applicants or former employees for race, age, marital status, religion, ethnic background, or another protected category.

While implementing the new requirements under this legislation will not prevent all acts of workplace violence, with an average of 20 employees being killed each week in the workplace, employers cannot afford to risk a substantial verdict or, more importantly, lives, by failing to use these new protections. As an employer, you can help to minimize your risk by doing the following.

- Maintain strict hiring policies.
- Establish written workplace anti-violence policies and security procedures with zero tolerance for any instance of violence.
- List prohibited conduct.
- Monitor current employees' behavior.
- Train managers and supervisors how to recognize and resolve problems.
- Maintain a working environment that is open to communication and respectful to all employees.
- Balance a violence-free workplace with employee rights.

If you find yourself struggling to wade through these often complicated laws, you may want to consult an employment law attorney.

SABOTAGE, FRAUD AND THEFT

No company is immune to the threat of violence, sabotage, fraud and theft. It falls upon the owner(s) to ensure the security of their assets (tangible and intangible) and their employees.

The security of your business operations begins on your physical property. There are some physical design features you can employ to deter violence or theft in the workplace. Crime Prevention through Environmental Design (CPTED) is an urban planning design process, integrating crime prevention with neighborhood design and community development. For more information, see Section III Recovery and Mitigation.

Local law enforcement may have a CPTED or Neighborhood Watch Program which can assist you in developing a protection strategy to make your physical site a safer place to work and conduct business. Walk the perimeter of the property, walk up and down your halls, look at camera angles, visit with staff, check access controls and badge issuance policies. They are only a small part of your whole physical world.

Could an outsider gain access to your facility through the loading dock? Do you use water for fire suppression in the data center?

The previous section, Cyber-Attacks, provides more detailed information on how to protect your intangible assets. The checklists Cyber Security Threat Assessment and Cyber Security Checklist (Checklists 21 and 22 in the Appendix) also relate to this topic.

As an employer, you can help minimize your risk of sabotage, fraud and theft by doing the following:.

- Maintaining strict hiring policies.
- Establish written workplace anti-violence policies and security procedures with zero tolerance for any instance of violence.
- List prohibited conduct.
- Monitor current employees' behavior.
- Train managers and supervisors to recognize and resolve problems.
- Maintain a working environment that is open to communication and respectful to all employees.
- Balance a violence-free workplace with employee rights.

LOSS OF KEY STAFF

In this age of doing more with less, or with fewer employees, businesses tend to rely on key staff who, because of leadership, unique skills, and/or organizational memory hold a special position in the organization. However, loss of key staff due to unexpected death, illness or injury, can have a very negative impact on business operations and remaining staff. This loss can be mitigated by good internal communications, cross-training, sharing of information and records, and progress reports. However, it is key to ensure the mental health of surviving employees especially in a traumatic event.

Nowhere is this more obvious than the experiences of the September 11th tragedy and those businesses in the World Trade Center. While the loss experienced by the companies within the towers was traumatic, both for the organizations and individuals, the lessons learned involving compassion and recovery are appropriate for all businesses. Here there were two major concerns: (1) the mental health of the surviving employees and (2) the operational devastation. The people need to be functioning to get the operation back in gear. Without the operation, the company can no longer exist.

Support and validation go a long way in the initial phases of healing. A special part in Section III addresses Employee Support and Screening, a critical component when dealing with loss, especially an unexpected loss or one connected with violence or suicide.

Secondly, organizations must confront trauma and loss like individuals do. The first stage of recovery, safety and control, includes focusing on the job at hand. For businesses this means hiring new employees, finding temporary and then permanent quarters, re-establishing technical and client connections and getting back to work. Once control is established, the second stage is remembrance and mourning. People must mourn their colleagues and friends in order to be able to accept new employees and be ready to move forward. Leaders must help employees mourn by permitting it to occur.

The final stage of grief is reconnecting to normal life. It is during this stage here there is a potential challenge to become even stronger and better than before. Dr. Judith Herman, M.D., a noted trauma expert at Harvard University School of Medicine, suggests that as "individuals transform from victim to survivor, they may feel a new sense of pride and a healthy admiration of strengths and potential. Similarly, organizations can also find themselves transformed. A management that can build and sustain trust during a crisis will deepen employee connections."

CIVIL UNREST

Civil disturbances include riots, property damage, threatening individuals, or assemblies that have become significantly disruptive.

Demonstrations are visible actions designed to advocate a position on a particular issue. Most are peaceful and only occasionally cause an inconvenience. They become problematic when they obstruct business.

In Case of Civil Disturbance or Demonstration

1. Avoid provoking or obstructing demonstrators.
2. Secure your area (lock doors and safes, remove files, vital records and expensive equipment).
3. Avoid the area of disturbance.
4. Continue with normal routines as much as possible.
5. If the disturbance is outside, stay away from doors or windows. Stay inside.
6. If officers are not present, call 911 to alert them to the situation.

If an event may trigger a violent reaction within your community, it may be prudent to take additional precautions including evacuation or closing, initiating your call down procedures or heightening security precautions.

TOURISM IMPACT OF THE LOS ANGELES RIOTS

The tourism effects of civil disturbances can be devastating and long-lasting, perhaps permanent. The case studies show both an immediate loss in numbers of international tourists and long-term loses of 20% to 30% of visitor arrivals. This reflects impacts on independent travelers and group tourists:

Damage to "safety and security" and "friendly residents" perceptions are particularly difficult (and expensive) to correct. They are key considerations for site selection and evaluation by international travelers.

Temporary changes in the itineraries of tour operators become permanent (unless there is a reason to change back). The shifts in the itineraries of tour operators will have direct consequences to related destinations that typically tie in with a Los Angeles tour (including, particularly, Hawaii, Seattle, San Francisco, San Diego, and Las Vegas). The effects on Hong Kong tourism of the suppression in Tiananmen Square amply demonstrates this potential. Some international visitors will also project the Los Angeles experience as indicative of other U.S. cities and shift travel to other countries or regions.

Impacts can be substantially reduced through aggressive marketing and promotion efforts in key markets. However, this is generally not through the media. The key is having an extensive and reliable customer database that allows you to provide a personal and rapid response to allay customer concerns.

WORKFORCE DISRUPTION

Workforce disruption can be the result of management/employee miscommunication or differences concerning procedures or policies. Or it can result from a natural or technological hazard or a perceived threat of safety. A sound Business Continuity Plan will reinforce day-to-day communications as well as crisis communications to ensure your employees have the most up-to-date information during times of threat.

An interesting website provides an index to information relating to HR policies and procedures (Source: http://humanresources.about.com/cs/laborrelations/index). The Labor Relations links explore such topics as management-union relationships, remaining non-union, collective bargaining, the potential contribution of a union representative, the advantages of a represented work place, and grievances. Emphasis is placed on sites that focus on building an effective partnership among all parties.

ADJACENT HAZARDS

When assessing your vulnerability to natural, technological or other hazards, it is critical that you also look around your facility and adjacent areas.

1. For example, your new building may be elevated above an anticipated flooding event; however, you are located in a hurricane evacuation area. Therefore, you still will be mandated to evacuate your facility given a hurricane threat. You will not be able to return until officials give the "all clear." What is the potential impact on your operations?
2. The building adjacent to you houses a print shop which has specific chemicals identified as hazardous. An incident at that facility may force you to evacuate your building or shelter-in-place. Are you familiar with the businesses around you?
3. Some organizations or businesses are at a higher risk of violence or attack because of the nature of their operations, i.e., landmarks, large venues, family planning centers, religious centers, government agencies, etc. Your business continuity plan should recognize the impact of their increased vulnerability and the potential impact to your company.

Section III:

Recovery and Mitigation

RECOVERY OPERATIONS

After a disaster, facilities, equipment and stock may have been damaged or destroyed. You may be without power, water, sewer and phone services. The vendors and suppliers you rely on may not be operating. Your employees and customers may have experienced personal damage or loss. Damage to the area may limit access to your facility for an extended period of time.

This is when preparedness planning, training and exercise will pay off. This is also when you will be rewarded for the investments you have made in your facility to make it stronger and more resistant to flood, wind, fire and security breach.

An immediate return to normal day-to-day operations may not be possible. So your business must be prepared to be self-reliant and implement a continuity plan to carry it through the next several weeks or months. The survival of the business will depend on it.

The purpose of this section is to provide an overview of the concept of recovery operations. Knowing what to expect and planning ahead will minimize the financial impacts of the disaster and position your company to not only survive, but continue to provide a service to your community when it needs you the most. Preparedness can mean the difference between financial ruin and financial gain, victim or survivor, survivor or hero.

There are three overlapping periods of recovery.

- Immediate Emergency Period
- Short-Range Restoration Period
- Long-Range Reconstruction Period

The length of time required for each period will vary, depending on the severity of the disaster and the local capability to recover quickly. The following graph is illustrative to depict the overlapping nature of the various periods. It does not imply that there is a generally accepted, pre-determined length of each phase.

RECOVERY PERIODS

Period	Days After Disaster Strikes							Weeks After Disaster Strikes								
	1	2	3	4	5	6	7	2	3	4	5	6	7	8	9	10
Immediate Emergency	■	■	■	■	■	■	■									
Short-Term Restoration					■	■	■	■	■	■						
Long-Range Reconstruction									■	■	■	■	■	■	■	■

IMMEDIATE EMERGENCY PERIOD

The Immediate Emergency Period begins directly after the crisis. With a hurricane strike, for example, it begins when the sustained winds drop below tropical storm force (39 mph) and stretches through the first few days after landfall. This phase may extend up to one week for many activities, depending upon the severity of the damage. During the immediate recovery period, emergency recovery operation is the responsibility of each County Emergency Operations Center (EOC). The major activities of emergency response personnel during this period are intra-county recovery operations, damage assessment and inter-governmental resource distribution.

- Intra-County Recovery Operations focus on the missing, stranded, injured and homeless. The primary activities are search and rescue; emergency mass feeding, sheltering and transportation and medical care of the injured. The major resource needs are for sustenance supplies, such as water, food, medicine, ice, blankets, etc. Security of the damaged area, debris

clearance and efforts to restore essential public utilities begin. During this period, normal social and economic activities are disrupted. Emergency management officials begin to survey the affected areas for needed recovery resources.

- Damage Assessment Operations include the activation of Damage Assessment Teams at county and municipal levels, the development of a Preliminary Damage Survey and collection of information for the final Damage Assessment Report.
- Inter-Governmental Resource Distribution provides for coordination and distribution of resources through the establishment of County Staging Areas, municipal and Fire District Recovery Centers, local distribution points, and Regional Recovery Center and Regional Staging Areas.

1. Re-entry

First, **BE PATIENT**. Access to affected areas will be controlled. If the business is located in the affected are, you will not be able to return to your business until search and rescue operations are complete and safety hazards, such as downed trees and power lines, are cleared. Depending on the type and degree of destruction, it may take three days or longer for emergency crews to clear the area and establish security. (Note that, even in a contained event, such as a fire that affects only your facility, access may not be possible until officials conduct an investigation.)

As part of your planning process, you should designate an Advance Recovery Team that will be first on the scene to conduct a preliminary damage assessment of your facility, coordinate with emergency responders and determine the appropriate recovery strategy. The team will need photo identification and documentation of employment to gain access to the affected area. Coordinate with the county emergency management and local emergency response personnel to ensure your team has adequate identification.

The Advance Recovery Team should have the capability to communicate directly with management. Their preliminary Damage Assessment Report should consider damage to the facility, tangible and intangible assets and the surrounding community. Management can then implement the appropriate steps in its Business Continuity Plan.

2. Implementation of the Continuity of Operations Plan (COOP)

If your business is dependent upon Information Technology and downtime is not an option, the implementation of the COOP Plan must be a technically sophisticated project. Professional assistance in the development of your COOP may be sought to determine if the following options are required:

- Cold Site - A site (data center/work area) equipped with appropriate environmental conditions, electrical connectivity, communications access, configurable space and access to accommodate the installation and operation of equipment by key employees required to resume business operations.
- Warm Site - A site (data center/work area) that is partially equipped with hardware, communications interfaces, electricity and environmental conditioning capable of providing backup operating support.
- Hot Site - A site that serves as a Business Continuity Management facility with the relevant work area recovery, telecommunications and IT interfaces and environmentally controlled spaces capable of providing relatively immediate backup and data processing support to maintain the organization's Mission Critical Functions.
- Hot Standby - A term that is normally reserved for technology recovery. This is an alternate means of processing data which minimizes downtime so that no loss of processing occurs. It usually involves the use of a standby system or site permanently connected to business users and is often used to record and back up transactions in tandem with the primary system.Emergency Data Services - Remote capture and storage of electronic data, such as journal entries, electronic vaulting and database shadowing/mirroring.

3. Crisis Communications Plan – Crisis communications is essential. A framework should be established before an emergency and you may need to be creative.

First, determine the status of your employees. Are they safe and did they incur any damage to their home or belongings? Then communicate the plan regarding the restoration of essential functions. Employees, vendors, suppliers and customers/clients will need to hear from you very soon.

4. Safety Measures

- Again, have valid IDs or some kind of entry authorization for all vital employees. Security operations will include checkpoints into affected areas. It is also helpful if employees have a readily distinguishable shirt or uniform.

- Reduce any unnecessary driving, if possible. Roads may have debris that will puncture tires. Warn employees not to sightsee, especially at night.

5. Immediate Repairs

- If you are allowed back into your building and damage is minor, make temporary repairs to correct safety hazards and minimize further damage. This may include covering holes in the roof, walls or windows, bracing and debris removal.
- Contact your insurance agent immediately and make arrangements to meet the adjustor as soon as possible. Take photographs or videos of all damage before repairs are started and keep receipts for insurance purposes.
- Only hire licensed contractors certified by the local jurisdiction and State of Florida to do repairs. Check with the local Building Department to ensure the contractor is licensed. You may also refer to the Disaster Contractors Network (www.dcn.org) which monitors licensed contractors who also have special training in disaster recovery. (If the contractor requests you pull the permit, it may be an indication that he is not properly licensed and is not entitled to permitting privileges.)

SHORT-TERM RESTORATION PERIOD

The Short-Range Restoration Period begins a few days after a disaster and stretches several weeks, depending on the extent of the damage. Restoration activities focus on repair to slightly and moderately damaged structures. In general, they return the area to a relatively normal and economically viable state as services and utilities are restored and debris removal continues. More detailed surveys of damage continue. State and Federal disaster relief resources are distributed to victims needing assistance, such as temporary housing, loans, grants, food coupons, and legal/crisis counseling. Restoration of all public utilities takes place and reconstruction of damaged housing, commercial, industrial and public facilities begins.

1. Damage Assessment Operations continue. Contact should be made with your insurance agent and licensed contractors for any necessary facility repairs and replacement of equipment, furniture and inventory. Restoration of communications and information services is top priority.
2. Identification/ Passes. Each county has its own plan and procedures for re-entry after an evacuation / emergency situation. Some counties have instituted systems which include passes, bumper /windshield stickers or other means of identification. At the very least, your employees will need some sort of documentation that states their name, position and organization or agency with photo identification. If it is crucial that your employees get back to the work facility as soon as deemed safe by local officials, it is recommended that you contact your county emergency management agency and determine what documentation will be necessary to allow your employees to gain access into an affected area or your facility. For security reasons, it may be very beneficial to invest in ID badges, especially if you need to restrict access into your facility. Following Hurricane Andrew, many companies found that employees wearing company shirts with logos provided an additional security check from a distance. This can be important especially, if someone is moving equipment or supplies from your building.
3. Implement the Continuity of Operations Plan (COOP), if required. Based on the damage assessment report and the expected level of disruption, you may need to implement the COOP plan and either establish an alternate facility, transfer (outsource) mission essential functions to a third party and/or activate a telework option. Based on the damage assessment and estimate of time needed for repairs and restoration of services, implement the appropriate procedures to ensure that your mission essential functions are restored within the necessary timeframe. The alternatives should be identified in the Business Continuity Plan and be ready for such an event.
4. Restoration of Services. It may take 2 to 4 weeks before utilities are restored. If your operations are dependent on a power supply and/ or communications, you will need to bring in alternate power supply and communications equipment, i.e., generator, radios, cell phones, etc. These issues should be addressed, contractors identified and provisions made before a disaster occurs.
5. Employee Support. Employers and employees rely on each other after a disaster. Businesses should define a range of services that it can provide or arrange for, including:

- Cash advances
- Salary continuation
- Flexible or reduced work hours
- Telework
- Crisis Counseling, and;
- Dependent care

PAYROLL & CASH ADVANCES

If you want to ensure your employees have the resources to make repairs, take care of dependents and report back to work, as a business owner, you need to ensure your employees continue to receive paychecks. You must first consider your policies for payroll, especially if you are not open for a significant period of time. Depending on the circumstances – and if you want to retain your employees – policies should be developed which at least provide a minimum salary level even if you have an interruption in operations. The second step is then to make arrangements to continue to meet your payroll given a lack of power and/or loss of data.

- How is the payroll schedule going to be met?
- Will direct deposits be available?
- If computer functionality is down, how will employees be issued checks?
- Who is allowed to pick up employee payroll checks? Consider developing an authorization form for non-relative payroll check pick-up.
- Where can the payroll checks be cashed? Consider having a pre-established arrangement with a local bank for employee payroll check and personal check cashing.
- Can the business provide emergency cash advances with payroll deductions?
- How will emergency cash advances be processed?

FLEXIBLE / REDUCED WORK HOURS / TELEWORK

If the emergency or disaster affects the community as well as the business, employees may need flexibility and support from management in order to take care of added responsibilities at home as well as at work. There may be insurance agents or contractors to meet, dependents to care for or cleanup to accomplish. Typically, a little understanding in times of emergency is well rewarded in lower employee turnover and increased loyalty. Consider reduced or flexible work hours or, if appropriate and feasible, telework options.

LONG-RANGE RECONSTRUCTION PERIOD

The Long-Range Reconstruction Period may stretch over many months after a disaster, until all physical property, social and economic processes return to a stable and acceptable pre-disaster level. The visible activities are demolition of partially devastated structures and complete major reconstruction. Victims return to repaired/rebuilt structures from temporary housing and preventative mitigation measures are formulated and implemented.

STATE AND FEDERAL DISASTER ASSISTANCE OPERATIONS

Following a Florida Governor's disaster declaration, a Presidential disaster declaration may be requested. If granted, the State and Federal Emergency Management agencies are co-located into one facility, the Disaster Application Center. The Presidential Declaration will trigger federal disaster assistance programs including individual assistance (for employees) and low-interest loans through the U.S. Small Business Administration.

If you may apply for a disaster loan, it is very important that you have the necessary paperwork for the applications. That list is included in Checklist 28, The "Go Box".

TRAUMATIC STRESS: CRISIS COUNSELING

The better prepared the employee is, the less of an impact a critical incident will have on an individual and the more stable the workplace will be following an incident. Understanding the basics of traumatic stress and how it affects people can help an organization recover quickly and with limited chaos.

Humans have a fairly predictable and consistent response to trauma. These responses occur in stages over time. Within each stage there are signs and symptoms that are considered normal reactions to abnormal events. This is a very important concept for the employer because no one is immune, including the boss. Different people will have different reactions depending on previous life experiences, coping skills, home life stability, amount of personal losses and other factors. The normal signs and symptoms are often misinterpreted. Sometimes these normal reactions are seen as non-coping of the traumatized person and the tendency is to send them home, which may not be the wisest thing to do.

Ideally when developing a plan for disaster management, pre-incident education for at least the management team is highly recommended. If the management team understands what to expect in the way of signs and symptoms and how to optimally deal with people who have been traumatized, the return to normal operations may be accelerated. A three to eight hour annual in-service will be time well spent.

Some organizations rely on Employee Assistance Programs (EAPs). Traumatic Stress is a highly specialized field and requires a skill set that is developed only after specialized training and field experience in dealing with survivors of trauma. When searching for mental health assistance following a traumatic event, it is recommended to turn to the specialist in the field of Traumatology and Critical Incident Stress Management (CISM). The emerging field of Traumatology is a rapidly growing, relatively new concept in the mental health arena.

A team approach in Traumatology will consist of a diverse group of trained individuals, mental health, emergency work and faith-based backgrounds. A diverse group of experienced team members can provide the workplace with the greatest coverage of services to best meet the needs of all employees, especially those who might shy away from mental health professionals. When preventing long-term affects from trauma, the key is get in immediately and provide a safe, supportive environment to deal with the after effects of the event. The workforce can be educated on traumatic stress reactions and the means of coping. For more information go online to ICISF.org

Some organizations develop internal critical incident teams to deal with the small to medium incidents that occur in the workplace from time to time under mental health guidance. The internal teams have a great advantage. They know and understand the internal workings of the business and are familiar with the corporate culture.

MITIGATION STRATEGY

Things happen….Floods can inundate and submerge your critical equipment. Hurricane force winds can rip sections off the roof of your production facility. Fires can sweep through the office destroying records, data and hardware. Today, new threats such as incendiary devices, computer viruses and threats of violence can cause serious business interruptions. Protecting your business and your employees from damage and loss, mitigation or prevention, is the foundation of Business Continuity Planning.

A MARKET FOR MITIGATION

Recovery from a disaster was once the pinnacle of business wisdom. The context has now changed, however, from coming back quickly and effectively to never going down at all. With the highly competitive markets, slim profit margin, and tight overhead, losses due to natural and technological hazards can make the critical difference in a business' capacity to maintain profitability or even survive.

Fortunately, there are cost-effective strategies that can reduce or even prevent losses; for example, integrating mitigation in new construction may increase costs only between 1 and 5 percent. Rehabilitating or retrofitting an existing facility may cost more than the costs of improvements in new construction. Retrofitting existing facilities, though, may protect the facility from

damages that far exceed the cost. (Risk Management, v.44, n.5, May 1997).

The benefits to businesses from mitigation are not limited to a reduction in facility damages. The truly cost-effective benefits include:

- Increased life safety for employees and customers,
- Reduced down-time in production,
- Protected information systems,
- Reduced damages to facilities and nonstructural components,
- Reduced damages to vital equipment, and
- Enhanced insurance coverage or reduced insurance deductibles.

Business owners should also consider the opportunities to partner with the community in recovery. A prepared organization (including employees), that protects itself against possible structural damage, downtime, and loss of records and inventory, can move quickly from "victim" to "survivor." A business that has the capability to then respond with needed goods and services in a time of crisis can then move from "survivor" to "hero." The Southwest Florida Regional Planning Council (www.swfrpc.org) has developed a planning document for businesses, Profiting Through Disaster Preparedness, which includes case studies, guidance and how-to checklists.

RISK ASSESSMENT

The Hazard and Vulnerability Analysis is important to identify (1) what hazards pose the greatest risk to your business operations and (2) where to spend time and resources to mitigate those impacts.

There are three types of assets to consider. The first are human resources – your employees and customers or clients. Safety issues should always remain a top business priority from a human standpoint. When looking at the cost-benefit analysis, you must consider liability risk, potential damage to reputation in the community and business interruption.

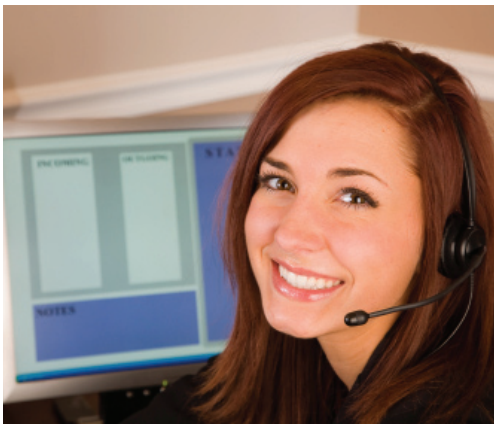
Secondly, and closely related, is protection of your facilities. There is a range of options for preventing damages in existing or new facilities. It is up to the business to determine the level of protection necessary for its operations and the right mitigation measure(s) to provide the protection. There are structural and non-structural mitigation strategies. Both should be considered.

Third, you must protect your tangible and intangible assets. Tangible assets include office furniture, work equipment, supplies, computers, desks, etc. Intangible assets include the information and data base systems that allow you to provide your services or manufacture your materials. They include your communications systems and client lists and other information. The protection of these resources is crucial for many business operations. Failure to protect client information may, in fact, represent a significant liability for the company.

PROTECTING YOUR HUMAN RESOURCES

As described in the previous sections, to respond efficiently during an emergency situation, a business needs to have an established Business Continuity Plan or program. Emergency planning should be an ongoing effort. There should be at least an annual test of emergency response plans and additional training / tests of procedures and policies.

Every employee is essential to the continuity of a business. For that reason, employers need to determine how the workforce will be managed prior, during and after an emergency. Managing the workforce includes having employer strategies and having prepared employees.



AWARENESS AND REPORTING POLICIES

A first step in preventing disasters is management and staff who are aware of their surroundings, the hazards to which they are vulnerable, and the necessary communication among them allowing concerns to be voiced and addressed. Americans have become much more aware of potential threats to our homeland. Probably most people, however, do not expect an emergency to affect their business, home or community. However, no business, home or community is immune to natural or technological disasters or acts of violence.

The best defense is a good offense. Employers and employees must be aware of potential problems, unusual occurrences, suspicious activity, and/or security risks. The BCP should address awareness and reporting policies. Management and employees should be trained in how to recognize potential threats and how to report them.

An example of awareness training may include how to recognize warning signals of potentially violent employees. Below is an excerpt from the Violence in the Workplace Fact Sheet on recognizing the warning signals.

"Potential warning signals may alert you to any employee or person in the workplace who could become violent. Changes in behavior are important to note in most cases. Look for patterns of changing behavior. No single warning signal in isolation is a reliable predictor of violence. Some factors may include:

- Major changes in personal appearance, attitude or behavior
- Change in personal relationships
- Reduction in job efficiency or productivity
- History of violent, reckless or antisocial behavior
- Unusual interest in or unexplained preoccupation with weapons or bringing weapons to work
- Serious stress in the employee's life
- Substance abuse
- Unexplained signals of physical injury
- Agitation
- Unexplained interest in what you do at work."

Awareness and reporting policies should not only cover violence, but any breach of security that can compromise safety or business operations. A safe workplace should also be free of the threat of theft or sabotage. Employees also should report any activity including unauthorized access to property or building without an owner's or manager's permission, duplication of keys or access cards, threats of retaliation. The BCP, in addition to the Employee Manual, should reflect the policies and reporting procedures for all concerns that can have an impact on safety, security and business operations.

EMPLOYEE TRAINING

All employees will require some form of preparedness training. This should include periodic employee discussions, staff meetings or desk and tabletop exercises to review safety procedures, evacuation plans, and recovery plans. Most importantly, employees should know what their individual roles and responsibilities are in an emergency situation. The Business Continuity Plan (BCP) should address the following elements that should be conveyed to employees in writing (such as the Employee Manual) and covered in staff meetings/training.

- Individual roles and responsibilities.
- Information about the hazards most likely to affect your business.
- Awareness and reporting policies.

- Security issues.
- Notification and warning procedures.
- Post-disaster communication procedures.
- Emergency Response Procedures (see Checklists in Appendices).
- Evacuation procedures.
- Location and use of emergency equipment, such as fire extinguishers.
- Emergency shutdown procedures.
- Re-entry.
- Recovery.

EMPLOYEE PREPAREDNESS

Employers should recognize and understand that employees are concerned foremost about the safety and well-being of their families during an emergency situation. Although the employer is responsible for assuring business continuity, employees have the responsibility of working together during an emergency situation to ensure that the business is restored efficiently. For that reason, it is critical that every employee develop a family emergency plan before an emergency situation arises. It is the employee's responsibility to develop a personal emergency plan. However, an employer needs to communicate expectations in regards to employee performance before, during and after a disaster and provide emergency preparedness guidance to their employees.

Guidance should include information on how to develop and promote personal preparedness. Information brochures are available to citizens from numerous agencies to help guide home and family preparations. This information should be relayed back to management so that they understand the plans of their employees. Potential conflicts should be resolved before the disaster strikes.

There are numerous sources of guidance available on government web sites such as www.fema.gov and www.floridadisaster.org. Local information is also available through the Florida Regional Councils, the local emergency management agencies and the local chapters of the American Red Cross. Florida companies also have extensive programs to better prepare their employees including the Tampa Electric Company's Get Ready! (See Employee Family Disaster Plan, Checklist 3 in Appendices).

Before developing a personal preparedness plan, an employee should learn about the emergency management plans and activities in their community in order to know:

- How the local government is protecting them from possible hazard,
- How to coordinate their emergency plan with those of the community, and
- How to use resources available in the community.

An Employee Disaster Preparedness Plan should include the following information:

1. Home and Family Preparation

   Alternate shelter for the employee and dependents ("dependents" are defined as those for whom the employee is directly responsible.). Each plan should have two additional contingency plans. Early evacuation to emergency shelters is strongly recommended.

2. Protection of Personal Property

   - Advance arrangements for home preparation and protection of personal property. The plan needs to address all but the most

severe damages.

- In the event my home is damaged, what am I required to do to protect/secure my home until it can be properly repaired?
- Can I make repairs to my home prior to an inspection by the claims adjuster?
- Are there any restrictions or requirements for the company that will repair my home, i.e., licensed, bonded, prior approval by insurance company, etc.?
- A schedule to inspect homes before hurricane season and to make necessary repairs/arrangements to reduce the risk of exposure to severe damage.
- Additional materials, equipment, and arrangements should be considered to expedite repairs after a hurricane.

3. All emergency planning information distributed by emergency agencies should be taken into consideration before a plan is formulated. Some of these considerations include, but are not limited to:
   - Home preparedness (i.e., current maintenance needs, repair supplies, storage area, etc.);
   - Evacuation zones and flood zones;
   - Geographic conditions that may affect the home (i.e., trees, rivers, creeks, remote area, etc.); and
   - Road conditions between home and the work location (i.e., the amount of trees on the route that may block transportation, the flood zones along evacuation route, etc.).
4. Dependent Care

   Plan for emergency dependent care in advance for children and elderly dependent(s) or ill family members. One plan with two additional contingency plans for dependent care needs. The plan should include family emergency meeting location (primary and secondary).

5. Contact numbers up to date and programmed in cell phones.
6. Medical/Dental
   - Information regarding primary care. Determine which substitute physician, if any should be contacted in an emergency situation if the primary physician i is unavailable.
   - Medical Supplies/Special Medical Needs - Employees with special medical needs or those who are taking prescription drugs should consult with their physician or pharmacist for such details as storage of prescription or non-prescription medications (i.e. baby formula, insulin, heart medication, etc.) in the event of an emergency situation.
     - A copy of medical records for each family member. Records should include current prescription dosages.
     - Address and telephone number of the nearest hospital.
7. Cash and Scarce Resources

A plan to obtain cash. Automatic teller machines (ATMs) may not work. Cash requirements may greatly increase for everyone during an emergency situation. The potential exists for the local economy to resort to a "cash basis society."

8. Missing Persons

   The Red Cross handles requests for locating missing persons in the event of an emergency. Direct employees to contact their local Red Cross Chapter if a family member or friend needs to be located.

9. Pet Care
   - Specify special pet needs.
   - Provide information, if possible, regarding Animal Services and what services could be expected.
   - List boarding houses that could be contacted for pet shelter information.
   - Have one plan with two additional contingency plans for pet care needs.
10. Personal Transportation

    Make advanced arrangements to prepare vehicles and consider alternatives if the primary means of transportation are eliminated. Insurance company can provide information about the requirements and restrictions of the policy after an emergency. This inquiry should include questions such as:

- In the event my vehicle is damaged by the event, what am I required to do to protect/secure the vehicle until it can be properly inspected and repaired?
- Can I use and/or make repairs to my vehicle prior to an inspection by the claims adjuster?
- Are there any restrictions or requirements for the repair company (i.e., licensed, bonded, prior approval by insurance company, etc.) that will repair my vehicle?

Transportation after a major event will be difficult because of road conditions and other limitations brought on by the emergency. Employees in remote areas are encouraged to take into consideration the road conditions between their homes and work locations, the amount of trees on the route that may block transportation, and their personal vehicle availability and readiness. Special plans can be made in advance to minimize the potential of being stranded.

11. Communications
    - Repair of electric lines takes precedence over phone line repair; cellular phone service may be restored first and may become a primary means of communication.
    - How will you communicate with your family if separated?

SECURITY ISSUES

1. Handling mail, visitors and deliveries

   Letters containing Bacillus anthracis (anthrax) have been received by mail in several areas in the United States. In some instances, anthrax exposures have occurred, infecting several persons. To prevent such exposures and subsequent infection, all persons should learn how to recognize a suspicious package or envelope and take appropriate steps to protect themselves and others. See Checklist 24 in Appendix Handling Suspicious Parcels and Letters. Train employees and post procedures where mail is handled.

2. Restricting Access

   As discussed previously, Crime Prevention through Environmental Design (CPTED) incorporates strategies that have been demonstrated to reduce the vulnerability to crime / violence. These same strategies should be employed to provide security and safety for employees, clients and customers.

   While no one wants to feel confined and business typically does not want to present an inaccessible or unwelcome environment, every business needs to be aware of its vulnerability to the outside world. Each business must assess its risk to crime and violence and then balance that risk with the need to project a welcoming atmosphere for customers and clients as well as the general community. Some degree of security is required for every business to ensure the safety of employees.

3. In assessing your risk and the opportunities to increase security without inconveniencing your staff or customers, consider the four CPTED Strategies:
    - **Natural Surveillance** promotes features that maximize visibility of people, parking areas and building entrances, e.g., doors/windows oriented toward streets and parking areas, streets/sidewalks that are pedestrian friendly, and adequate night lighting.
    - **Territorial Reinforcement** is well-defined property lines that distinguish private spaces from public spaces through the use of landscaping, pavement design, gateways and fences, art, and other elements. This can give the property users a better sense of control over their surrounding environment and a sense of ownership, which can discourage potential criminals.
    - **Natural Access Control** is attained through highlighting building entrances, streets and sidewalks, and neighborhood entrances/gateways as clearly public areas, and utilizing structural elements to limit access to private spaces.
    - **Target Hardening** is the use of security devices to increase the perception of risk in an offender by inhibiting their access to certain areas, e.g., window locks, dead bolts, interior door hinges, security lights, cameras, etc.

PROTECTING YOUR FACILITY

PROTECTING YOUR COMMERCIAL PROPERTY FROM WATER DAMAGE

Water may be essential to life, but as a destructive force, water can diminish the value of your commercial building. Commercial buildings, as well as manufacturing facilities, can suffer water damage that results in increased maintenance costs, a decrease in the value of the facility, lowered productivity and potential liability associated with a decline in indoor air quality. The best way to protect against this potential loss is to ensure that the building components, which enclose the structure, known as the building envelope, are water resistant. Also, you will want to ensure that manufacturing processes, if present, do not allow excess water to accumulate. Finally, make sure that the plumbing and ventilation systems, which can be quite complicated in commercial buildings, operate efficiently and are well maintained.

Flood Protection Checklist:

1. Determine if your building is located in a Special Flood Hazard Area. Start by checking with your community floodplain management (or FEMA) official, mortgage lender, or insurer or insurance agent to find out the flood zone. If a Flood Insurance Rate Map (FIRM) indicates that your facility is in flood zone A, AE, A1-A30, AH, AO, AR, V, VE or V1-V30, then the building is in a Special Flood Hazard Area.
2. Find out from your local floodplain management official the base flood elevation (BFE) for your property.
3. Consult your community's records or your property survey for the elevation of your building's lowest floor. If the community records and the property survey do not indicate the elevation of the lowest floor, you will need to hire a licensed surveyor to determine it. The lowest floor is the lowest enclosed area.

If the lowest floor is below the BFE, consider the following retrofit options:

- Relocation out of the floodplain provides the greatest protection from future flooding. A building that is structurally sound can be relocated although this is an expensive option. If the structure has had repetitive losses, it may be eligible for assistance from FEMA.
- Elevation of an existing structure provides the owner an opportunity to retrofit the structure by raising it above the anticipated base flood elevation level. It may be elevated by using fill, solid extended foundation walls, columns or piles. The technique used will depend largely on the flood, site and building characteristics, as well as cost.
- Floodproofing involves preventing floodwaters from entering a structure (dry floodproofing) or allowing floodwaters to enter a structure and flow through reducing the impact on the structure walls (only recommended for basements). Dry floodproofing involves completely sealing the exterior walls of the structure to prevent entry of floodwaters. Dry floodproofing provides an excellent vehicle for owners of existing flood-prone non-residential structures to bring them into compliance with the standards of the National Flood Insurance Program. It tends to be affordable and effective and should be considered if your facility is subject to flooding.

4. Identify and repair all leaks and cracks.

The following are common building-related sources of water intrusion:

- **Windows and Doors**. Check for leaks around your windows, storefront systems and doors.
- **Roof**. Improper drainage systems and roof sloping reduce roof life and become a primary source of moisture intrusion. Leaks are also common around vents for exhaust or plumbing, rooftop air conditioning units or other specialized equipment.
- **Foundation and Exterior Walls**. Seal any cracks and holes in exterior walls, joints and foundations. These often develop as a naturally occurring byproduct of differential soil settlement.
- **Plumbing**. Check for leaking plumbing fixtures, dripping pipes (including fire sprinkler systems), clogged drains (both interior and exterior), defective water drainage systems and damaged manufacturing equipment.
- **Ventilation, Heating and Air Conditioning (HVAC) Systems**. Numerous types, some very sophisticated, are a crucial component to maintaining a healthy, comfortable work environment. They are comprised of a number of components (including chilled water piping and condensation drains) that can directly contribute to excessive moisture in the work environment. In addition, in humid climates, one of the functions of the system is to reduce the ambient air

moisture (relative humidity) level throughout the building. An improperly operating HVAC system will not perform this function.

5. Prevent water intrusion through good inspection and maintenance programs

   You can help prevent water intrusion and excessive moisture levels by regularly inspecting the following elements of your building to ensure they remain in good condition.

   - **Flashings and Sealants**. Flashing, which is typically a thin metal strip found around doors, windows and roofs, is designed to prevent water intrusion in spaces where two building materials come together. Sealants and caulking are specifically applied to prevent moisture intrusion at building joints. Both must be maintained and in good condition.
   - **Vents**: All vents should have appropriate hoods, exhaust to the exterior and be in good working order.
   - Review the use of manufacturing equipment that may include water for process or cooling. Ensure wastewater drains adequately away with no spillage. Check for condensation around hot or cold materials or heat transfer equipment.
   - **HVAC**. Heating, ventilation and air conditioning systems are much more complicated in commercial buildings. Check for leakage in supply and return water lines, pumps, air handlers and other components. Drain lines should be clean and clear of obstructions. Ductwork should be insulated to prevent condensation on exterior surfaces.
   - **Humidity**: Except in specialized facilities, the relative humidity in your building should be between 30% and 50%. Condensation on windows, wet stains on walls and ceilings, and musty smells are signs that relative humidity may be high. If you are concerned about the humidity level in your building, consult with a mechanical engineer, contractor or air conditioning repair company to determine if your HVAC system is properly sized and in good working order. A mechanical engineer should be consulted when renovations to interior spaces take place.
   - **Moist Areas**. Regularly clean off, and then dry all surfaces where moisture frequently collects.
   - **Expansion Joints**. Expansion joints are materials between bricks, pipes and other building materials that absorb movement. If expansion joints are not in good condition, water intrusion can occur.
   - **Interior Finish Materials**. Replace drywall, plaster, carpet and stained or water damaged ceiling tiles. These are not only good evidence of a moisture intrusion problem, but can lead to deterioration of the work environment, if they remain over time.
   - **Exterior Walls**. Exterior walls are generally comprised of a number of materials combined into a wall assembly. When properly designed and constructed the assembly is the first line of defense between water and the interior of your building. It is essential that they be maintained properly (including regular refinishing and/or resealing with the correct materials).
   - Storage Areas: Storage areas should be kept cleaned with air allowed to circulate to prevent potential moisture accumulation.

6. Act Quickly If Water Intrusion Occurs
   - Label shut-off valves so that water supply can be easily stopped in the event of a plumbing leak. If water intrusion does occur, you can minimize the damage by addressing the problem quickly and thoroughly.
   - Immediately remove standing water and all moist materials, and consult with a building professional.
   - Should your building become damaged by a catastrophic event such as fire, flood or storm, take appropriate action to prevent further water damage once it is safe to do so. This may include boarding up damaged windows, covering a damaged roof with plastic sheeting or removing wet materials and supplies. Fast action on your part will help minimize the time and expense for repairs, resulting in a faster recovery.

For more information about protecting your business or home from water intrusion, check these sources:

- APA - THE ENGINEERED WOOD ASSOCIATION www.apawood.org
- ENERGY & ENVIRONMENTAL BUILDING ASSOCIATION www.eeba.org
- GLE ASSOCIATES, INC. Architects/Engineers/ Environmental Consultants www.gleassociates.com

- THE NATIONAL CENTER FOR ENVIRONMENTAL HEALTH www.cdc.gov
- THE UNITED STATES ENVIRONMENTAL PROTECTION AGENCY www.epa.gov
- Source: The Institute for Business and Home Safety (IBHS) is an initiative of the insurance industry to reduce deaths, injuries, property damage, economic losses and human suffering caused by natural disasters. It is at 4775 E. Fowler Avenue Tampa, FL 33617 1(866) 657-4247(IBHS) Fax: (813) 286-9960 www.ibhs.org
- See also Department of Community Affairs, Division of Emergency Management, Retrofitting and Flood Mitigation in Florida, January 1995.

PROTECTING YOUR COMMERCIAL BUILDING FROM WIND DAMAGE

First, find out if your building meets current building code requirements for high-wind regions. Experts agree that structures built to meet or exceed current model building codes and include provisions for high-wind have a much better chance of surviving violent windstorms.

Structural Improvements

Work involving building improvements may require a building contractor or a registered design professional, such as an architect or engineer.

1. Roofs: If you are replacing your roof, take steps to ensure that both the new roof covering and the sheathing to which it attaches will resist high winds. Your roofing contractor should:
   - Remove old coverings down to the bare wood sheathing.
   - Remove enough sheathing to confirm that rafters and trusses are securely connected to the walls.
   - Replace damaged sheathing.
   - Refasten existing sheathing according to the proper fastening schedule outlined in the current model building code for high wind regions.
   - Install a roof covering that is designed to resist high winds.
   - Seal all roof sheathing joints with self-stick rubberized asphalt tape to provide a secondary moisture barrier.
   - If you want to give your roof sheathing added protection, but it's not time to reroof, glue the sheathing to the rafters and trusses. Use an adhesive that conforms to Performance Specification AFG-01 developed by APA, the Engineered Wood Association. The adhesive is available at a hardware store or home improvement center.
2. Gables. Make certain the end wall of a gable roof is braced properly to resist high winds. Check the current model building code for high wind regions for appropriate guidance, or consult a qualified architect or engineer.
3. Connections. The points where the roof and the foundation meet the walls of your building are extremely important if your house can resist high winds and the pressures they place on the entire structure.
   - Anchor the roof to the walls with metal clips and straps (most easily added when you replace your roof).
   - Make certain the walls are properly anchored to the foundation. A registered design professional can determine if these joints need retrofitting. A qualified contractor can perform the work the design professional identifies.
   - If the building is over one story, make certain the upper story wall framing is firmly connected to the lower framing. The best time to do this is when you remodel.
4. Outside Maintenance
   - Replace gravel/rock landscaping material with shredded bark.
   - Keep trees and shrubbery trimmed. Cut weak branches and trees that can fall on your building.
5. When Building or Remodeling

- Windows. If you are replacing your existing windows, install impact-resistant window systems, which have a much better chance of surviving a major windstorm. As an alternative to new window systems, install impact-resistant shutters that close over window openings to prevent flying debris from breaking glass panes.
- Entry Doors. Make certain your doors have at least three hinges and a dead bolt security lock with a bolt at least one inch long. Anchor door frames securely to wall framing.
- Patio Doors. Sliding glass doors are more vulnerable to wind damage than most other doors. If you are replacing patio doors or building a new facility, consider installing impact-resistant door systems made of laminated glass, plastic glazing or a combination of plastic and glass. When a hurricane threatens, a temporary and effective step is to cover large windows and doors with shutters made of plywood or oriented strand board (OSB).
- Garage Doors. Because of their size, garage doors are highly susceptible to wind damage. A qualified inspector can determine if both the door and the track system can resist high winds or need to be replaced with a stronger system. Garage doors more than eight feet wide are most vulnerable. Install permanent wood or metal stiffeners. Or contact the door manufacturer.

Source: The Institute for Business and Home Safety (IBHS) is an initiative of the insurance industry to reduce deaths, injuries, property damage, economic losses and human suffering caused by natural disasters. It is located at 4775 E. Fowler Avenue Tampa, FL 33617 1(866) 657-4247(IBHS) Fax: (813) 286-9960 www.ibhs.org

PROTECTING YOUR PROPERTY FROM FIRE DAMAGE

If you are not sure whether your building is at risk from wildfires, check with your local fire marshal, building official, city engineer, or planning and zoning administrator. They can tell you whether you are in a wildfire hazard area. Also, they usually can tell you how to protect your property and personnel from wildfires and structural fires.

Fire protection can involve a variety of changes to your building and property - changes that can vary in complexity and cost. You may be able to make some types of changes yourself. But complicated or large-scale changes and those that affect the structure of your building or its electrical wiring and plumbing should be carried out only by a professional contractor licensed to work in your state, county, or city. One example of fire protection is replacing flammable roofing materials with fire-resistant materials. This is something that most owners would probably hire a contractor to do.

Here are the most important considerations to make sure you business is Fortified against Wildfire damage. (Refer to the Wildfire Safety Checklist (Checklist 10 in the Appendix) for more information.

- A noncombustible street number at least four inches high, on a contrasting background, at each driveway entrance, visible from both directions of travel.
- Eaves of noncombustible materials. A roof assembly with a Class A Fire rating. Wood shakes and wood shingles do not qualify regardless of rating.
- Multi-layered glazed panels in exterior windows, glass doors and skylights or solid, exterior shutters.
- Gutters and downspouts of noncombustible materials.
- LP gas containers must be located within defensible space.
- Defensible space of 100 feet minimum.
- Exterior wall material must have one hour fire resistive rating.
- Driveways must be provided at least 12 feet wide with at least 13.5 feet of vertical clearance. Driveways longer than 150 feet shall have turnarounds. Driveways longer than 200 feet shall have both turnouts and turnarounds.
- If the driveway is gated, the gate opens inward and has an entrance at least two feet wider than the driveway and at least 30 feet from the road. If secured, the gate must have a key box of a type approved by the local fire department.

A WORD ABOUT ROOFING MATERIALS

Some roofing materials, including asphalt shingles and especially wood shakes, are less resistant to fire than others. Keep this in mind if you plan to have your existing roofing materials replaced.

- Tile, metal, and slate are more expensive roofing materials, but if you need to replace your roofing anyway, it may be worthwhile to pay a little more for the added protection these materials provide.
- Slate and tile can be much heavier than asphalt shingles or wood shingles. If you are considering switching to one of these heavier coverings, your roofing contractor should determine whether the framing of your roof is strong enough to support them.

PROTECTING YOUR ASSETS (TANGIBLE AND INTANGIBLE)

PROTECTION OF DATA – BACKUPS, SOFTWARE AND POLICIES

According to Strategic Research Corp., the primary causes of data loss within companies are:

- Hardware system - 44%
- Human error - 32%
- Software - 14%
- Virus - 7%
- Natural disaster - 3%

Unlike tangible property, computer data are intangible information. However, stored information is more often than not, the lifeblood of the organization. Protecting your data and information is extremely important. As you can see, human error and hardware failure are major factors; however, the growing threat of viruses and malicious attacks further emphasize the need to protect your files and computer systems as closely as possible. Depending on office size and resources, many procedures can be chosen to effectively safeguard your data and even your hardware.

Some of the effective strategies to protect tangible assets:

- **Hardware Planning and location** – It may seem fairly straightforward, yet many offices may not have planned out their IT infrastructure with various disasters in mind. A small office with a room "in the back" that has a server or two on the floor may be vulnerable to flood incursion or even sprinkler system flooding from fire suppression. Server racks or shelves that hold the servers and battery backup devices at least a foot off the ground can make the difference between destroyed infrastructure and recoverable damage. Clean room or dry fire suppression systems are more expensive, but will not damage your IT equipment with water. Central location for server rooms/closets in the office work best for network infrastructure as well as minimizing damage from wind during tornadoes and hurricanes.
- **Paper fire safes** - Fire safes for protecting papers reduce the flash point of the documents. This is accomplished by a cement-like material in the walls of the safe that evaporate vapor into the safe to dampen the paper. This allows the temperature to rise to the 300-400+ degree range without igniting the paper. Important papers to be stored should also include software license numbers since they are often required if a software product is to be reinstalled.
- **Magnetic media fire safes** - Fire safes for tapes and diskettes differ from fire safes designed to protect paper. Condensing moisture can damage magnetic media, so these safes typically do not contain vapor-inducing materials. Tapes, disks, and other media should be kept in safes that insulate against fire heat to keep internal temperatures below 125 degrees. Safes should not be opened for at least 24hrs after fire exposure to allow the internal temperatures to stabilize gradually. It is important to keep the original installation diskettes for software packages should the need arise to reinstall a given program.

Magnetic media - Ironically, as organizations transfer documents to magnetic media for long-term storage, they may actually be shortening the storage life of the information. Properly stored, paper can last for decades or even centuries. However, diskettes have a shelf life of 1-2 years, tapes/drives 3-5 years, and CDs 10+ years. For irreplaceable information it is best to have backup documentation in hard (paper) copy or to ensure that the media (tapes, VHS, etc.) is in a format which can still be read.

Hot-site - Disasters that destroy data and software can also destroy the computer hardware that runs the software. A hot-site is an alternate location where the software can be installed on compatible hardware and facilities.

- *Location* - The location of a potential hot-site should be considered. In a hurricane or earthquake for instance, the disaster area could be tens to hundreds of miles wide. If widespread disasters are identified in a risk assessment then the hot-site location should be distant enough to be unaffected by the same disaster.
- *Equipment* - The computer hardware and other equipment should be compatible with that of the original system. Other office equipment such as phone systems, fax machines, and employee workspaces should also be examined.

Some of the effective means of protecting intangible assets:

Backups - Creating a mirror image of the intangible data onto tangible media (disk, tape, CD, etc.) provides a backup of this information. When the original data are rendered useless, the backups can be used to re-create the data. With client-host and distributive processing becoming more popular it is important to backup critical workstations, since certain data and cache files may be important to the system as a whole. Technology is changing rapidly. Most businesses have replaced external hard drives for their tape drives. Where tapes are referenced below, portable hard drives may be substituted. Backups you would want to pay attention to:

- **System** - System backups provide a spare copy of all the information on a computer system. The operating system (Windows, Server 2000-2008, Linux, etc.), application software, and volatile data are all backed-up. This should be done both on host servers and individual workstations (if resources allow).
- **Data Only** - Unlike system software, which typically doesn't change often, user data changes daily. Making backups of data is like having tangible insurance in that the hours of work a computer user has done have been protected.
- **Create bootable disk of operating system (Windows, Mac, Linux etc.)** - After a damaged computer has been repaired or replaced the operating system needs to be restored. For this restoration to take place the computer needs to be powered-up or "booted" using the operating system (OS). This typically means that a diskette, diskettes, or CD replicating the original OS need to be used. Some Local Area Networks (LANs) use a Network Operating System (NOS) that can be restored using diskettes, CDs, and tapes created from more elaborate backup software packages. Another option is a Pre-installed Environment (PE) like Windows PE or BartPE that has utilities and backup restoration programs installed. These are abbreviated operating systems that boot and run on a CD or DVD. Linux has a boot operating system as well. It is even possible with network features turned on to run a bare minimum file server with data disks attached internally or with USB, Firewire, or eSATA connections.

SCHEDULING OF BACKUPS

- **Daily** - System backups usually only need to be done on a monthly, or at most a weekly, basis. However, business critical PCs and servers should have their data backed up on a daily basis.
- **Monday-Friday** - Each day of the workweek should have its own data set backup. In other words if the work-week is Monday through Friday and it takes two tapes each day to do a data backup then a total of (10) tapes should be used on a rotational basis.
- **Weekly** - In addition to the daily backup sets a separate data backup set should be done weekly. This backup is then archived in case past information needs to be retrieved.
- **Monthly** - Separate data backup sets should also be done on a monthly basis. These backups should be kept even after data is purged from the system for later referral. Data is typically not purged for at least (1) year.

STORAGE LOCATION

- **On-site** – Tapes, DVDs, portable hard drives that are used to back up software should be kept in a dry, fire-resistant metal storage container. Access to the backup media should be restricted to authorized personnel for security purposes.
- **Off-site** - At least (2) system and data backup sets should be kept off-site from the location of the computer systems. If a large scale disaster occurs at the computer system locations the on-site backups may be destroyed. The geographic distance needed for off-site locations depends on the anticipated threats; across town is sufficient for building fires, for hurricanes the distance should be 30+ miles, for earthquakes it may require locating in a different area of the country.

Many companies are investigating the virtues of online data backup - a process that involves transferring backups over the

Internet and storing them in secure, redundant servers geographically distributed. Systems should be evaluated based on the following benefits:

1. Ease of data transfer – A system that mitigates the amount of work that must be done in order to transfer data to a secure location – but still does its job properly
2. Security – A system that ensures data, even if stored offsite, is always protected.
3. Easy Access and fast retrieval – access within minutes.

BUSINESS INSURANCE KNOW-HOW

You have invested so much time and money building your business. Isn't it worth a few minutes to learn how to protect that investment? This section provides a quick overview of the various types of commercial insurance you may need for your small business.

A major fire at your worksite or even a minor fall by a visitor can have a devastating impact on your business. So how can you protect your small business from big financial losses? You can start with two critical kinds of commercial insurance that are often packaged together in a Business Owner's Policy (BOP): property insurance and liability insurance.

Property insurance covers your physical assets: your building, equipment, furnishings, fixtures, inventory, computers, valuable papers, records, and more. But property insurance also can provide income if your business is forced to suspend operations after a covered loss.

For example, if your building is destroyed or damaged in a fire, you may not only be covered for that property loss, but also you may be able to collect income while you are regrouping.

Business liability insurance is specifically designed to protect your business assets if your company is sued for something it did or even did not do that resulted in bodily injury or property damage to someone else.

For example, a liability insurance policy may cover expenses if someone claims to be injured by a product you sell or it can pay for defense costs if a competitor sues you for trademark infringement.

Many insurance providers bundle the primary property and liability insurance coverages you need into an economically priced business owner's policy. You can then tailor your insurance package by extending the coverage limits in specific areas or adding options to cover risks that are inherent to your industry.

FLOOD INSURANCE

A flood policy protects you from flood, meaning a general and temporary condition of partial or complete overflowing of inland or tidal waters, the unusual and rapid accumulation or runoff of surface waters from any source, and mudflows caused by flooding which are related to a river of liquid and flowing mud on the surface of normally dry land areas.

According to the Federal Emergency Management Agency, floods result in over $1 billion of property damage each year. Yet only one-third of Americans living in heavy flood zones have the insurance to handle it. (Homeowners insurance doesn't cover floods.)

FLOOD INSURANCE FREQUENTLY ASKED QUESTIONS

1. Is my business at risk?

Ninety percent of all disasters in the United States are flood related. You are four times more likely to experience a flood than a fire. The Federal Emergency Management Agency estimates that between seven and eight million U.S. households and hundreds of thousands of businesses are exposed to the risk of flooding.

2. Is flood insurance provided by your property insurance policy?

Probably not. Most property insurance policies do not offer protection against flood damage. You will need a special policy for flood loss.

3. Is flood insurance required by law?

Maybe. Congress passed the Flood Disaster Protection Act of 1973 and the National Flood Insurance Reform Act of 1994 mandating that all federally insured or regulated lenders require flood insurance for mortgages and other loans on buildings and manufactured (mobile) homes located in Special Flood Hazard Areas.

4. What structures can be protected by flood insurance?

Almost any building with at least two walls and a roof may be insured if it is principally above ground and located in a community participating in the National Flood Insurance Program (NFIP). Coverage is also available for businesses and buildings under construction.

5. Will flood insurance cover the contents of my building?

The contents of a fully enclosed, insurable building may be covered by a separate policy, making flood insurance available to renters.

6. How much does flood insurance cost?

The average premium for an NFIP flood insurance policy is $300 per year for approximately $85,000 worth of coverage. For those not in a Special Flood Hazard Area, but still exposed to flood risk, there is a low cost policy available for as little as $106 per year. Nearly one-third of all flood claims come from these lower risk areas.

7. Where is flood insurance available?

Flood insurance is available for buildings in communities that have agreed to adopt and enforce sound flood plain management practices. Currently, these are over 18,000 communities participating in the NFIP throughout the United States and overseas territories.

8. When can I purchase flood insurance?

You can buy flood insurance at any time. There is normally a 30-day waiting period between the time flood insurance is purchased and the time the coverage is effective.

9. What if I've had a flood loss before?

If you have already received a grant for a flood loss, you must have flood protection. If not, you will be denied most kinds of government assistance if a flood should happen again.

COMMERCIAL AUTO INSURANCE

You would not dream of driving your personal automobile without insurance. It's just as important to protect your company vehicles. Even if you have personal auto insurance, you still need commercial auto insurance. That is because vehicles involved in an accident while engaged in company business may not be covered by your personal insurance. To make matters worse, you could be charged with misrepresentation if you have placed a vehicle you use for commercial purposes under your personal auto policy.

There are a variety of coverages for your commercial autos, and your agent or broker can help you choose the right one. The discussion should include business-use autos, pickups, vans, trucks and non-owned and rented vehicles. You may also want to include a conversation about "non-owned" vehicles (when employees use their own vehicles to run errands) and rented vehicles (when an employee travels and needs to rent a car).

WORKERS' COMPENSATION INSURANCE

As soon as you hire your first employee you need the protection of workers' compensation insurance. Not only do many state laws require it, but also the financial security of your business depends on it.

In general, workers' compensation represents a compromise between employers and employees regarding employment-

related injuries or illnesses. In short, employees relinquish their right to sue employers if they suffer some job-related injury or illness. But in return, employers agree to provide state-mandated benefits if employees suffer some job-related injury or illness. And to ensure employers have the money to pay these mandated benefits, most states require that employers demonstrate that they have the financial ability to pay any claims that may arise. Typically this financial ability is demonstrated through the purchase of workers' compensation insurance. Laws regarding workers' compensation insurance vary by state, so check with your independent insurance agent or broker to find out exactly what you need and how it's purchased.

Most workers' compensation insurance policies actually provide two types of coverages:

- Workers' Compensation Coverage. This type of insurance provides benefits for injured workers as required by state law regardless of who is at fault for the injury or illness. In other words, whatever benefits your state requires, your workers' compensation policy would provide.
- Employers' Liability Coverage. This additional coverage protects employers in case they are ever sued for damages arising from employment related accidents or diseases. However, to collect benefits provided by employer's liability coverage, both the employee as well as anyone else not covered by workers' compensation laws (i.e., spouses and dependents) would have to prove that the employer was actually legally responsible for the employee's injury or disease.

ERRORS & OMISSIONS INSURANCE (E&O)

Regardless of what kind of business you own, customers can claim that something you did on their behalf was done incorrectly, and that this error cost them money or caused them harm in some way.

In the litigious world we live in today, many business owners protect themselves with errors and omissions insurance (E&O). This type of insurance may be appropriate for anyone who gives advice, makes educated recommendations, designs solutions or represents the needs of others, such as teachers, consultants, software developers, ad copywriters, web page designers, placement services, telecommunication carriers or inspectors.

Although formalizing a contract with your clients can help limit your liability, the big expense in an errors and omissions claim is the legal defense needed to prove liability or innocence. Errors and Omissions policies are designed to cover many of these defense costs and ultimately the final judgment if the business owner does not win the case.

UMBRELLA INSURANCE

No one really expects a disaster to strike his or her business. But every small business is vulnerable to a major catastrophe or a huge lawsuit. Think about some of the devastating losses you have heard about recently or the large settlements that are awarded in courts these days. Some of these losses could exceed your primary insurance coverage unless you protect your business with umbrella insurance.

As its name implies, umbrella insurance extends your coverage beyond the limits of your basic business insurance. Umbrella insurance is important because it covers unexpected events. It is not expensive and, in certain instances, it could literally save your business.

Umbrella insurance policies provide additional liability insurance coverage after the limits of your underlying policy are reached.

For example, if several people were injured on your property and required $1.5 million in medical treatment but the liability limit of your underlying policy is $1 million, your umbrella insurance policy would cover the additional $500,000 (if you're found liable).

- Cost of Medical Treatment $1,500,000
- Your Basic Liability Limit $1,000,000
- Umbrella Policy Would Cover the Gap $500,000

SPECIALIZED COMMERCIAL INSURANCE

Some commercial insurance companies offer specialized packages for certain types of small businesses as well as optional coverages for certain types of risks. Your insurance agent is the one person most qualified to help you evaluate all the commercial coverages you may need for your specific business.

Source: The Hartford Insurance Company (www.thehartford.com/sb)

Section IV:

Resources: Preparedness Info Center

PUBLICATIONS AND BROCHURES

There are numerous documents available to help you develop a viable business continuity plan for your company. We have provided examples of some of the best of these available on the website (www.fldisasterkit.com). You will need Adobe Acrobat Reader to download and read these documents.

Guidebooks

Business Disaster Planning Guidebook (TBRPC, 2008)

Business Disaster Plan Template (TBRPC, 2008)

South Florida Hurricane Survival Guide for Small Businesses (SFRPC, 2000)

Emergency Management Guide for Business and Industry (FEMA)

Getting Back to Business (IBHS, 2004)

Open for Business (Florida DEM, 2000)

Documents and brochures which provide specific guidance for particular sections of your Business Continuity Plan or particular hazards are also available. Examples include:

- After the Flood: Safety Tips for Business Owners
- Against the Wind
- Automatic Sprinkler Systems - Testing Can Minimize Water Damage
- Cost-Benefit Estimates
- Cyberspace Strategy
- Protect Your Home Against Damage from Freezing Weather
- Emergency Action Plans and Fire Protection Plans: OSHA Regulation 29 CFR 1910.38
- EPA Guide to Protecting Building Environments
- Emergency Response to Terrorism: Self-Study Guide (ERTSS)
- Fact Sheet: Rolling Blackouts
- FDA Food Code/Hazard Analysis Critical Control Point Plan (HACCP)
- Fire Drill and Evacuation Guidelines for Health Care Facilities
- Is Your Home Protected From Hail Damage?
- Halon 1301-Fire Extinguishing Agents for New/Existing Installations
- Hometown Security
- Life Safety--Evacuation and Accessibility Planning for the Disabled
- Life Safety--Evacuation Planning
- Lighting Prevention and Protection
- Mold Remediation in Schools and Commercial Buildings
- Mold Resources
- Natural Hazards
- Preparing for and Responding to Bomb Threats and Letter Bombs
- Recovery
- Reviewing Potential Workplace Hazards
- Telecommuting
- Understanding the Life Safety Code
- Workplace Violence Awareness

- Workplace After a Disaster
- Workplace Violence Prevention Program

EMPLOYEE HANDOUTS

There are even more documents and brochures to assist your employees prepare their family disaster plans. Employee personal preparedness will be critical to the success of your business disaster survival so heed the advice of those companies who have dealt with disasters and support an active preparedness program for your employees. Here are some of the documents and brochures we found most helpful.

- Family Disaster Planning
- FEMA: Are You Ready? An In-depth Guide to Citizen Preparedness
- Is your home protected from a Wildfire Disaster?
- Ready New York Series

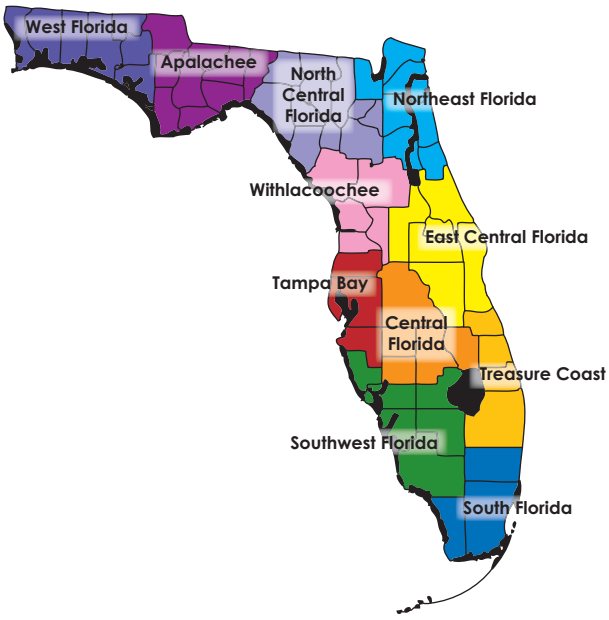
  Series provides general preparedness information for citizens in several languages.

  - Emergency Preparedness Guide
  - Beat the Heat Guide
  - Ready New York for Kids
  - Ready New York for Seniors and People with Disabilities
  - Hurricanes and NYC
  - Ready New York for Business
  - Ready New York For Pets
  - Pocket Guide

For more resources, go to the web site for the Capital Area Chapter of the American Red Cross, www.tallytown.com/redcross/.

CONTACT INFORMATION

In order to complete the Business Continuity Plan, you will need key information regarding vulnerability to specific hazards (i.e., hurricane evacuation zones, flood zones, locations of storage of extremely hazardous materials, etc.) in your county and/or region. In this section you will find the contact information for county emergency management, regional planning councils and local state agencies to assist you.



REGIONAL PLANNING COUNCILS

West Florida Regional Planning Council
4081 E. Olive Rd., Suite A
Pensacola, Florida 32514
www.wfrpc.dst.fl.us
(850) 332-7976

Apalachee Regional Planning Council
29776 Central Ave. E., Suite 1,
Blountstown, FL 32424
www.thearpc.com
(850) 674-4571

North Central Florida Regional Planning Council
2009 N.W. 67th Place, Ste. A,
Gainesville, Florida 32653-1603
www.ncfrpc.org
(352) 955-2200

Northeast Florida Regional Council
6850 Belfort Oaks Place
Jacksonville, Florida 32216
www.nefrpc.org
(904)279-0880

Withlacoochee Regional Planning Council
1241 S.W. Tenth Street
Ocala, Florida 34474-2798
www.wrpc.com
(352) 732-1315

East Central Florida Regional Planning Council
631 N. Wymore Rd., Suite 100, Maitland, FL 32751
Winter Park, Florida 32789
www.ecfrpc.org
(407) 623-1084

Central Florida Regional Planning Council
P. O. Drawer 2089
Bartow, Florida 33831-2089
www.cfrpc.org
(863) 534-7130

Southwest Florida Regional Planning Council
1926 Victoria Ave.,
Ft. Myers, Florida 33901
www.swfrpc.org
(239) 338-2550

Tampa Bay Regional Planning Council
4000 Gateway Centre Boulevard, Suite 100
Pinellas Park, FL 33782
www.tbrpc.org
(727) 570-5151

Treasure Coast Regional Planning Council
421 SW Camden Avenue
Stuart, FL 34994
www.tcrpc.org
(772) 221-4060

South Florida Regional Planning Council
3440 Hollywood Boulevard, Suite 140
Hollywood, Florida 33021
www.sfrpc.com
(954) 985-4416

COUNTY EMERGENCY MANAGEMENT AGENCIES

Comprehensive Emergency Management is the primary responsibility of local government. When a disaster threatens or incident occurs, it is your county emergency management, your local fire department, law enforcement and government who are on the scene and provide the incident command and control.

State and federal agencies serve in a support role to the local government during the times of crisis. When the crisis situation exceeds the resources of the local government, state and federal agencies provide and coordinate the distribution of needed resources to the local operation.

Each county in the State of Florida has an emergency management program which will coordinate response and recovery operations in a disaster. They can provide you with information concerning local emergency plans, evacuation zones, etc. However, do NOT contact them for planning information during an emergency. Obviously, your planning should be conducted before an emergency occurs. When a hurricane threatens, you should already know if and when you would have to evacuate. Your plans should be in place. Your employees should be aware of the plan, trained and prepared at home and at work.

Contact information for your county emergency management is available on the web sites listed below or in your local telephone directory.

WEBSITE LINKS

A central source is the State of Florida Emergency Management web site: www.floridadisaster.org. This site can direct you to federal, state, regional and local agencies which can provide support, resources and guidance.

Federal Entities	
Department of Homeland Security	http://www.tallytown.com/redcross/
Federal Emergency Management Agency	http://www.fema.gov/
FEMA Region IV	http://www.fema.gov/regions/iv/index.shtm
FEMA National Flood Insurance Program	http://www.fema.gov/nfip/
FEMA for Kids	http://www.fema.gov/kids/
US Fire Administration	http://www.usfa.fema.gov/
DisasterHelp.gov	https://disasterhelp.gov/portal/jhtml/index.jhtml
Citizen Corps	http://www.citizencorps.gov/
Small Business Administration (SBA)	http://www.sba.gov/
SBA Disaster Assistance	http://www.sbaonline.sba.gov/DISASTER/
Small Business Development Centers (SBDC)	http://www.sba.gov/sbdc/
Florida SBDC Network	http://www.floridasbdc.com/
State Entities	
Florida Division of Emergency Management	http://www.floridadisaster.org/
Florida State Emergency Response Commission (SERC)	http://state.fl.us/CPS/SERC/SERC.htm
Florida Emergency Operation Center	http://www.floridadisaster.org/eoc/
Florida DEM/ Domestic Preparedness	http://www.floridadisaster.org/bpr/EMTOOLS/Severe/terrorism.htm
Florida DEM/ Hurricane Awareness	http://www.floridadisaster.org/hurricane aware/
Florida Citizen Corps	http://www.floridadisaster.org/directoroffice/citizen corps/
Florida Department of Community Affairs	http://www.dca.state.fl.us/
Florida Department of Health	http://www.doh.state.fl.us/
Florida Department of Law Enforcement	http://www.fdle.state.fl.us/

Regional Planning Councils	
Central Florida Regional Planning Council	http://www.cfrpc.org/
North Central Florida Regional Planning Council	http://www.ncfrpc.org/
SFRPC South Florida Regional Planning Council	http://www.sfrpc.com/
SWFRPC Southwest Florida Regional Planning Council	http://swflorida.com/swfrpc/
Tampa Bay Regional Planning Council	http://www.tbrpc.org/
East Central Florida Regional Planning Council	http://www.ecfrpc.org/
Withlacoochee Regional Planning Council	http://www.wrpc.cc/
Northeast Florida Regional Planning Council	http://www.nefrpc.org/
Apalachee Regional Planning Council	http://www.thearpc.com/
Treasure Coast Regional Planning Council	http://www.tcrpc.org/
West Florida Regional Planning Council	http://www.wfrpc.dst.fl.us
Non-Profit/Educational	
Federal Alliance for Safe Homes	http://www.flash.org or http://blueprintforsafety.org
Institute for Business & Home Safety	http://www.ibhs.org
Florida County Emergency Management Web Sites	
Florida Emergency Preparedness Association	http://www.fepa.org
Alachua County Emergency Management	http://www.alachua em.org/
Baker County Emergency Management	http://bakercountyfl.org/
Bay County Emergency Management	http://bcem.co.bay.fl.us/
Bradford County Emergency Management	http://bradcoem.org/
Brevard County Emergency Management	http://embrevard.com/
Broward County Emergency Management	http://www.co.broward.fl.us/disaster.htm
Charlotte County Emergency Management	http://www.charlottecountyfl.com/emerg.htm
Citrus County Emergency Management	http://www.sheriff.citrus.fl.us/
Clay County Emergency Management	http://www.claycountygov.com/
Collier County Emergency Management	http://www.collierem.org/
Columbia County Emergency Management	http://www.isgroup.net/ccem/
DeSoto County Emergency Management	http://www.co.desoto.fl.us/dcem.html
Duval County Emergency Preparedness	http://www.ci.jax.fl.us/pub/emergency/
Escambia County Emergency Management	http://www.escambia emergency.com/
Flagler County Emergency Services Department	http://www.flagleremergency.com/
Franklin County Emergency Management	http://www.tallytown.com/redcross/franklin/
Gadsden County Emergency Management	http://www.tallytown.com/redcross/gadsden/
Gilchrist County Emergency Management	http://www.co.gilchrist.fl.us/em/
Gulf County Emergency Management	http://www.gulfcountygovernment.com/emd.html
Hamilton County Emergency Management	http://www.hamcoem.com/
Hardee County Emergency Management	http://www.hardeecounty.net/start.html
Hendry County Emergency Management	http://www.hendryfla.net/
Hernando County Emergency Management	http://www.co.hernando.fl.us/em/
Highlands County Emergency Management	http://www.hcbcc.net/
Hillsborough County Emergency Management	http://www.hillsboroughcounty.org/emer mgt/

Indian River County	http://www.indian river.fl.us/government/ems/disaster.html
Jackson County Emergency Management	http://www.emergencymanager.org/
Jefferson County Emergency Management	http://www.tallytown.com/redcross/jefferson/
Lake County Emergency Management	http://www.co.lake.fl.us/emergenc mang.htm
Lee County Public Safety	http://www.lee county.com/publicsafety.htm
Leon County Emergency Management	http://lcso.leonfl.org/em.htm
Levy County Emergency Management	http://www.levyeoc.com/
Liberty County Emergency Management	http://www.tallytown.com/redcross/liberty/
Madison County Emergency Management	http://www.tallytown.com/redcross/madison/
Manatee County Emergency Management	http://www.co.manatee.fl.us/
Marion County Emergency Management	http://www.sheriff.marioncountyfl.org/adsupport/emgt
Martin County Emergency Management	http://www.martin.fl.us/GOVT/depts/esd/EMA/
Miami Dade County Emergency Management	http://www.co.miami dade.fl.us/oem/home.htm
Monroe County Emergency Management	http://www.co.monroe.fl.us/pages/psd/
Nassau County Emergency Management	http://www.nassaufl em.com/
Okaloosa County Emergency Management	http://www.co.okaloosa.fl.us/emergencymanagement.html
Okeechobee County Emergency Management	http://home.okeechobee.com/okeeeoc/
Orange County Office of Emergency Management	http://www.ocoem.com/
Osceola County Emergency Management	http://www.osceola.org/index.cfm/sDepartment
Palm Beach County Emergency Management	http://www.co.palm beach.fl.us/eoc/
Pasco County Office of Emergency Management	http://pascocountyfl.net/oem/index.asp
Pinellas County Emergency Management	http://www.pinellascounty.org
Polk County Emergency Management	http://www.polk county.net/Public Safety/
Putnam County Emergency Management	http://www.putnam fl.com/brd/PCPS/EmergencyService.htm
Santa Rosa County Emergency Management	http://www.santarosa emergency.com/
Sarasota County Emergency Operations Center	http://www.sarasotaeoc.net/
Sarasota County Emergency Management	http://www.co.sarasota.fl.us/es em/
Seminole County Emergency Management	http://www.seminolepublicsafety.org/em.htm
St. Johns County Emergency Management	http://www.co.st johns.fl.us/BCC/emgcymngmt/index.html
St. Lucie County Emergency Management	http://www.stlucieco.gov/eoc/index.htm
Sumter County Emergency Management	http://bocc.co.sumter.fl.us/index.html
Taylor County Emergency Management	http://www.perryfl.com/tcem/
Union County Emergency Management	http://www.lake butler.com/em.htm
Volusia County Emergency Management	http://www.volusia.org/emergency/
Wakulla County Emergency Management	http://www.tallytown.com/redcross/wakulla/
Walton County Emergency Management	http://www.wcso fl.com/eoc.htm
Washington County Emergency Management	http://home.digitalexp.com/%7Ejbrock/wc11.htm

Relief Agencies	
American Red Cross	http://www.redcross.org/
Alachua County Chapter, Gainesville	http://alachua.redcross.org/
Brevard County Chapter, Melbourne	http://brevardcounty.redcross.org/
Broward County Chapter, Ft. Lauderdale	http://www.arcbcc.org/
Capital Area Chapter, Tallahassee	http://www.tallytown.com/redcross/
Central Panhandle Chapter, Panama City	http://centralpanhandle.redcross.org/
Central Florida Chapter, Orlando	http://centralflorida.redcross.org/
Charlotte County Chapter, Port Charlotte	http://www.sunline.net/redcross/
Coast to Coast Chapter, Daytona	http://www.daytonaredcross.org/
Columbia County Chapter, Lake City	http://www.cccarc.org/
Florida Coast to Coast Chapter, Daytona Beach	http://www.daytonaredcross.org/
Greater Miami &The Keys, Miami	http://www.miamiredcross.org/
Indian River Chapter, Vero Beach	http://www.redcross.org/fl/indianriver
Lee County Chapter, Fort Myers	http://www.arclcc.org/
Manatee County Chapter, Bradenton	http://www.manateeredcross.org/
Martin County Chapter, Stuart	http://martincountyfl.redcross.org/
North Treasure Coast Chapter, Vero Beach	http://northtreasurecoast.redcross.org/
Northeast Florida Chapter, Jacksonville	http://www.nefloridaredcross.org/
Northwest Florida Chapter, Pensacola	http://www.westfla redcross.org/
Palm Beach County Chapter, West Palm Beach	http://www.redcross pbc.org/
Polk County Chapter, Winter Haven	http://polkcountyfl.redcross.org/
Southwest Florida Chapter, Sarasota	http://southwestflorida.redcross.org/
Tampa Bay Chapter, Tampa Bay	http://www.redcrosstbc.org/
Salvation Army	http://www1.salvationarmy.org/
Florida Salvation Army Disaster Services	http://www.salvationarmyflorida.org/
Catholic Relief Services	http://www.catholicrelief.org/
Church World Service	http://www.churchworldservice.org/index.html
Citizen Corps	http://www.citizencorps.gov/
Humane Society Disaster Center	http://www.hsus.org/ace/11661
Florida Interfaith Networking in Disaster	http://www.findflorida.org/
Catholic Charities USA	http://www.catholiccharitiesusa.org/disaster
Church of the Brethren	http://www.brethren.org/genbd/ersm/disaster.htm
Church World Service Emergency Response	http://www.cwserp.org/
Christian Church (Disciples of Christ)	http://www.weekofcompassion.org/
CRWRC Christian Reformed World Relief Committee	http://www.crwrc.org/
Florida Council of Churches	http://www.floridachurches.org/
Florida Voluntary Organizations Active in Disaster	http://www.flvoad.org/
Lutheran Disaster Response	http://www.elca.org/dcs/disaster
Mennonite Disaster Services	http://www.menno disaster service.org/
NVOAD National Organizations Active in Disaster	http://www.nvoad.org/
Presbyterian Disaster Assistance	http://www.pcusa.org/pcusa/wmd/pda/index.html
United Church of Christ Wider Church Ministries	http://www.ucc.org/global/disaster
Habitat for Humanity	http://www.habitat.org/

Weather Links	
Florida State Weather Roundup	http://iwin.nws.noaa.gov/iwin/fl/hourly.html
The Weather Channel Florida	http://www.weather.com/weather/us/states/Florida.html
Weather Underground: Florida	http://www.wunderground.com/US/FL/
Florida Regional Weather	http://www.flausa.com/cgibin/sm40i.xe?docid=20135:2708
Yahoo! Weather Florida	http://weather.yahoo.com/regional/US/FL.html
Weather Online: Florida Local Weather	http://www.weatheronline.com/FLwx.html
Florida Weather Bureau	http://www.weatheronline.com/localwx/FL/
Florida Weather Monitor	http://www.floridaweather.com/
Florida State Information (NWS)	http://floridaweather.tierranet.com/
The Florida Weather Bureau	http://iwin.nws.noaa.gov/iwin/fl/fl.html
Florida Weather Center	http://www.weathercenter.com/
Florida Forecasts and Warnings	http://www.rsmas.miami.edu/environment/florida weather.html
AccuWeather State Radar Image	http://www.accuweather.com/msnbc/
Florida Disasters Info and Files	http://www.nsis.org/disasters/disasters files.html
Skywarn Storm Spotter Network	http://www.marine.usf.edu/nws/skywarn.html
Weather Information Network W.I.N.	http://www.gate.net/~hughesl/win/
Geostationary Satellite Server: Hurricane	http://www.goes.noaa.gov/g8hu.html
National Hurricane Center	http://www.nhc.noaa.gov/
National Weather Service (NWS)	http://www.nws.noaa.gov/
NWS Severe Weather Awareness	http://205.156.54.206/om/severeweather/index.shtml
NOAA	http://www.noaa.gov/
NOAA Hurricanes site	http://hurricanes.noaa.gov/
FEMA Storm Watch	http://www.fema.gov/fema/trop.htm
FEMA Hurricane Info	http://www.fema.gov/hu98/hurinfo.htm
NASA GOES Satellite Imagery	http://wwwghcc.msfc.nasa.gov/GOES/
NOAA GOES Satellite Server	http://www.goes.noaa.gov/g8hu.html
NRL Monterey Tropical Cyclone Images	http://kauai.nrlmry.navy.mil/sat bin/tc home
Current Watches and Warnings	http://www.spc.noaa.gov/products/wwa/
NOAA	http://www.noaa.gov/
NOAA Imagery	http://www.osei.noaa.gov/

DEFINING DESTRUCTION: A BCP GLOSSARY

BUSINESS-RELATED TERMS

ALTERNATE SITE: A site held in readiness for use during a Business Continuity E/I/C to maintain the business continuity of an organization's Mission Critical Activities. The term applies equally to office or technology requirements. Alternate sites may be "cold," "warm" or "hot." This type of site is also known as a Recovery Site. See: Cold Site, Warm Site, Hot Site, Recovery Site

ASSESSMENT: The evaluation and interpretation of measures and other information to provide a basis for decision-making.

BACKUP: A process by which data, electronic or paper based, is copied in some form to be available if the original data is lost, destroyed or corrupted.

BUSINESS CONTINUITY PLANNING: The overall process of developing an approved set of arrangements and procedures to insure your business can respond to a disaster and resume its critical business functions within a required time frame objective. It is an ongoing process to plan, develop, and implement disaster recovery procedures to ensure the optimum availability of the critical business functions. The primary objective is to reduce the level of risk and cost to you and the impact on your staff, customers and suppliers.

BUSINESS INCOME COVERAGE: The insurance company agrees to pay your loss of business income that results in a suspension of your business operations because of damage to your building or personal property caused by a covered cause of loss insured in your property policy. Business Income includes net profit or loss that would have been earned if the suspension of operations had not occurred and normal operating expenses including payroll that would have continued during the suspension. Coverage begins with the date of the loss to your property and ends when the damage or destroyed property could have been restored with reasonable speed and like quality.

BUSINESS INCOME FOR DEPENDENT PROPERTIES: Coverage is provided for you loss of business income because of damage to the building or personal property at another business that you are dependent on for your operations. The four types of dependent properties are businesses that furnish materials or services to you, businesses that purchase material or services from you, businesses that manufacture products for your customers, and a leader location, for example, an anchor store that attracts customers to your business.

CALL TREE: A structured cascade process (system) that enables a list of person, roles and/or organizations to be contacted as a part of an information or plan invocation procedure.

See: Contact List, Cascade System, Reverse Cascade System

CASCADE SYSTEM: A system whereby one person or organization calls out/contacts others who in turn initiate further call-outs/contacts as necessary.

See: Contact List, Call Tree and Reverse Cascade System.

CIVIL AUTHORITY INSURANCE: Business Income insurance pays for the loss of income if access to your business is prohibited by civil authorities because of damage to other property as a result of a covered cause of loss insured in your policy. Coverage is provided for up to two consecutive weeks from the date of the civil authority action.

CONTINGENCY PLAN: A specific planned response to an event which is possible, but uncertain, to occur.

COLD SITE: A site (data center/work area) equipped with appropriate environmental conditioning, electrical connectivity, communications access, configurable space and access to accommodate the installation and operation of equipment by key employees required to resume business operations.

COMMAND, CONTROL AND COORDINATION: A Crisis Management process: Command means the authority of an organization or part of an organization to direct the actions of its own resources (both personnel and equipment).

Control means the authority to direct strategic, tactical and operational operations in order to complete an assigned function and includes the ability to direct the activities of others engaged in the completion of that function, i.e., the crisis as a whole or a function within the crisis management process. The control of an assigned function also carries with it the responsibility for the health and safety of those involved.

Coordination means the harmonious integration of the expertise of all the agencies/roles involved with the objective of

effectively and efficiently bringing the crisis to a successful conclusion.

CONTACT LIST: See Call Tree and Cascade System, Reverse Cascade System.

COORDINATE: To advance systematically an exchange of information among principals who have or may have a need to know certain information in order to carry out their role in a response.

DAMAGE ASSESSMENT: The process of assessing the financial/non-financial damage following a Business Continuity E/I/C. It usually refers to the assessment of damage to physical assets, e.g., vital records, building, sites, technology to determine what can be salvaged or restored and what must be replaced.

DATA MIRRORING: A process whereby critical data is copied instantaneously to another location so that it is not lost in the event of a Business Continuity E/I/C.

DENIAL OF ACCESS: Inability of an organization to occupy its normal working environment; often due to Emergency Services policy.

DECISION POINT: The latest moment at which the decision to invoke the emergency procedures has to be taken in order to ensure the continued viability of the organization.

DENIAL OF ACCESS: The inability of a organization to access and/or occupy its normal working environment. Usually imposed and controlled by the Emergency and/or Statutory Services.

DESKTOP EXERCISE: See Table Top Exercise

DISASTER: A sudden, unplanned calamitous event that causes great damage or loss. In the business environment, it is an event that creates an inability on an organization's part to provide the critical business functions for some predetermined period of time. A disaster is any event that impairs your organization's ability to provide critical business functions for some predetermined period of time.

DISASTER MITIGATION: Activities taken to eliminate or reduce the level of risk to life and property from hazards.

DISASTER PREPAREDNESS: Activities, programs, and systems developed prior to a disaster that are used to support and enhance mitigation, emergency response, and recovery.

DISASTER PREVENTION: Measures employed to prevent, detect, or contain incidents, which, if left unchecked, could result in disaster.

DISASTER RECOVERY: The portion of a Business Continuity Plan (BCP) that addresses restoration of Information Technology and Telecommunication capabilities.

E/I/C: The acronym for Emergency(ies), Event(s), Incident(s) or Crisis(es).

ELECTRONIC VAULTING: The transfer of data to an offsite storage facility using a communications link.

EMERGENCY: Any natural or man-caused situation that results in, or may result in, substantial injury or harm to the population or substantial damage to or loss of property.

EMERGENCY OPERATIONS CENTER (EOC): The site from which civil government officials (municipal, county, State and Federal) exercise direction and control in an emergency.

EMERGENCY PUBLIC INFORMATION: Information that is disseminated primarily in anticipation of an emergency or at the actual time of an emergency and in addition to providing information, frequently directs actions, instructs, and transmits direct orders.

EMERGENCY RESONSE PROCEDURES: The initial response to any E/I/C and is focused upon protecting human life and the organizations assets.

EMERGENCY SUPPORT FUNCTION: A functional area of response activity establishes to facilitate coordinated Federal delivery of assistance required during the response phase to save lives, protect property and health, and maintain public safety. These functions represent those types of Federal assistance that the State likely will need most because of the overwhelming impact of a catastrophic event on local and State resources.

ESSENTIAL SERVICE: A service without which a building would be disabled. Often applied to utilities (water, gas, electricity, etc.) it may also include standby power systems, environmental control systems or communication network.

EQUIPMENT: The computer hardware and other equipment should be compatible with that of the original system. Other office equipment such as phone systems, fax machines, and employee workspaces should also be examined.

EVACUATION ORDER: The most important instruction you will receive from local government officials, relayed over local radio and television stations. Once issued, an evacuation order is mandatory under law in the State of Florida.

EXERCISE: An announced or unannounced execution of the business continuity plan intended to implement existing plans and/or highlight the need for additional plan development. A way of testing part of a BCP, an exercise may involve invoking the BCP procedures but is more likely to involve the simulation of an emergency or crisis in which participants role-play in order to assess what issues may arise, prior to a real invocation.

EXTENDED PERIOD OF INDEMNITY: You may purchase, as an option, an endorsement to extend the time of recovery after you resume operations to cover the reduction in income when you require additional time to return to normal levels of revenue.

EXTRA EXPENSE COVERAGE: The insurance company provides coverage for the necessary additional expenses needed to continue business when a covered loss damages or destroys your property. Examples include extra pay for overtime work to speed the restoration of the business, the extra cost of moving your operations to a temporary location, and rental of substitute equipment.

EVACUATION: Organized, phased and supervised dispersal of civilians from dangerous or potentially dangerous areas, and their reception and care in safe areas.

FIRST RESPONDER: Local police, fire, and emergency medical personnel who first arrive on the scene of an incident and take action to save lives, protect property, and meet basic human needs.

HOT SITE: A site (data center, work area) provides a BCM facility with the relevant work area recovery, telecommunications and IT interfaces and environmentally controlled space capable of providing relatively immediate backup data process support to maintain the organization's Mission Critical Activities.

HOT STANDBY: A term that is normally reserved for technology recovery. An alternate means of process that minimizes downtime so that no loss of process occurs. Usually involves the use of a standby system or site that is permanently connected to business users and is often used to record transactions in tandem with the primary system.

INFORMATION TECHNOLOGY DISASTER RECOVERY (ITDR): An integral part of the organization's BCM plan by which it intends to recover and restore its IT and telecommunications capabilities after an E/I/C.

KEY EMPLOYEES: The employees absolutely necessary to perform the tasks mandatory for an organization's continued operation.

LEAD AGENCY: The federal department or agency assigned lead responsibility under U.S. law to manage and coordinate the Federal response in a specific functional area. For the purposes of the CONPLAN, there are two lead agencies, the FBI for Crisis Management and FEMA for Consequence Management. Lead agencies support the overall Lead Federal Agency (LFA) during all phases of the response.

LIAISON: An agency official sent to another agency to facilitate inter-agency communications and coordination.

LOCAL GOVERNMENT: Any county, city, village, town, district, or political subdivision of any State, and Indian tribe or authorized tribal organization, or Alaska Native village or organization, includes any rural community or unincorporated town or village or any other public entity.

MANUAL PROCEDURES: An alternative method of working following a loss of IT systems. As working practices rely more and more on computerized activities, the ability of an organization to fall back to manual alternatives lessens. However, temporary measures and methods of working can help mitigate the impact of a E/I/C and give staff a morale boost.

MAXIMUM ACCEPTABLE OUTAGE (MA0): This is the timeframe during which a recovery must become effective before an outage compromises the ability of an organization to achieve its business objectives and/or survive.

MISSION CRITICAL ACTIVITIES (OR FUNCTIONS): The critical operational and/or business support activities (either provided

internally or outsourced) without which the organization would quickly be unable to achieve its business objectives(s), e.g., services and/or products.

MOBILE STANDBY: A transportable operating environment – often a large trailer – complete with office facilities and computer equipment that can be delivered and set up at a suitable site at short notice.

OFFSITE LOCATION: a site at a safe distance from the primary site where critical data (computerized or paper) and /or equipment is stored from where it can be recovered and used at the time of a Business Continuity E/I/C if original data, material or equipment is lost or unavailable.

OUTSOURCING: The transfer of business functions to an independent (internal or external) third party supplier.

PERIOD OF TOLERANCE: The period of time in which a Business Continuity E/I/C can escalate to a potential disaster without undue impact to the organization.

POST TRAUMATIC STRESS DISORDER (PTSD): PTSD is caused by a major traumatic E/I/C where a person experienced, witnessed or was confronted with a crisis that involved actual or threatened death or serious injury or threat to the physical integrity of self or others, and the person's response involved intense fear, helplessness or horror.

See: Trauma Counseling and Trauma Management.

PRE-POSITIONED RESOURCE: Material (i.e., equipment, forms and supplies) stored at an offsite location to be used in business recovery operations.

PUBLIC INFORMATION OFFICER: Official at headquarters or in the field responsible for preparing and coordinating the dissemination of public information in cooperation with other responding Federal, State, and local agencies.

RECOVERY: Recovery, in this document, includes all types of emergency actions dedicated to the continued protection of the public or to promoting the resumption of normal activities in the affected area.

RECOVERY PLAN: A Plan developed by each State, with assistance from the responding Federal agencies, to restore the affected area.

RECOVERY TIME OBJECTIVE (RTO): RTO is the maximum acceptable length of time that can elapse before loss of a business function severely impacts the business entity. The RTO is the time before a disaster is declared, during which time the impact begins, is recognized and is identified, and the time to perform the tasks documented in the disaster recovery plan for resumption of the critical business functions.

RENDEZVOUS POINT (RVP): A secure and safe location (point) to which all Emergency Services resources arriving at a Recovery Center outer barricade are directed for logging, briefing, equipment issue and deployment.

RESPONSE: Those activities and programs designed to address the immediate and short-term effects of the onset of an emergency or disaster.

REVERSE CASCADE SYSTEM: A reversal of the cascade system that enables the whereabouts and safety of personnel to be established.

RISK: The chance of something happening, measured in terms of probability and consequences. The consequence may be either positive or negative. Risk in a general sense can be defined as the threat of an action or inaction that will prevent an organization's ability to achieve its business objectives. The results of a risk occurring are defined by the impact.

RISK ANALYSIS: The process of identifying the risks to an organization, assessing the critical functions necessary for an organization to continue business operations, defining the controls that are in place to reduce organization exposure, and evaluating the cost for each such control. The risk analysis often includes an evaluation of the probabilities and likely impact of a particular event.

RISK ASSESSMENT: The overall process of risk identification, analysis and evaluation.

RISK CATEGORIES: Risks of similar types are grouped together under key headings, otherwise know as "risk categories." These categories include reputation, strategy, financial, investments, operation infrastructures, business, regulatory compliance, people, technology and knowledge.

RISK MANAGEMENT: A management approach designed to prevent and reduce risks and to lessen the impact of their occurrence. The objective is to identify the risks and mitigate to an acceptable level while considering the risk impact, probability and cost of mitigation implementation options.

RISK MITIGATION: Measures taken to reduce exposures to risks.

ROLL CALL: The process of ensuring that all employees, visitors and contractors have been safety evacuated and accounted for following an evacuation of a building or site.

SOCIAL IMPACT: The affect and effect of a E/I/C on the overall well-being of a population or community.

STANDBY SERVICE: the provision of the relevant recovery facilities.

TABLETOP EXERCISE: A paper feed scenario based method of testing plans, procedures and people.

TRAUMA COUNSELLING: The provision of assistance to staff, customers and others who have suffered mental or physical injury through being involved in an E/I/C.

TRAUMA MANAGEMENT: Trauma Management involves helping employees deal with trauma in a systematic way following a disaster through the delivery of appropriate support systems and coping strategies with the objective of restoring employees' psychological wellbeing.

UNINTERRUPTIBLE POWER SUPPLY (UPS): used for ensuring clean electrical power is delivered to sensitive or critical equipment in the event of a power loss or surge.

UTILITIES: Companies/organizations providing essential services; e.g., gas, water, electricity.

VIRUS: An unauthorized program that inserts itself into a computer system and then propagates itself to other computers via networks or disks. When activated, it interferes with the operation of the computer systems.

VITAL RECORD: Computerized or paper record which is considered to be essential to the continuation of the business following an E/I/C.

VITAL RECORD LOCATION: A designated storage location for holding Vital Records. Must be away from the normal site and be secure.

WARM SITE: A site (data center/ work area) which is partially equipped with hardware, communication interfaces, electricity and environmental conditioning capable of providing backup operating support.

WORK AREA FACILITY: A pre-designated space provided with desks, telephones, PCs, etc. ready for occupation by business recovery teams at short notice. May be internally or externally provided. See Cold Site, Hot Site, Warm Site, Alternate Site.

Source: The Business Continuity Institute 2002, Version BCI DJS 1.0 01/12/02.

WEATHER-RELATED TERMS

AIR MASS: A large body of air with relatively uniform characteristics, such as temperature and humidity.

ATMOSPHERE: The air surrounding the Earth.

BAROGRAPH: A device for recording air pressure.

BAROMETER: A device used to measure air pressure.

CLIMATE: Average weather of an area over a long time, usually 30 years.

CLIMATE MODEL: Mathematical model containing equations that describe climatic interactions.

COASTAL FLOOD WARNING: A warning that significant wind-forced flooding is eminent along low-lying coastal areas.

COASTAL FLOOD WATCH: An alert that wind-forced flooding is expected along low-lying coastal areas.

COLD FRONT: A warm cold air boundary with the cold air advancing.

CONDENSATION: The change of a vapor to liquid.

CONDUCTION: Transfer of heat within a substance or from one substance to another by inter-molecular action.

CONTINENTAL AIR MASS: An air mass that forms over land, making it generally dry. It may be warm or cold.

CONVECTION: Transfer of heat by the movement of the heated material. In meteorology, the up and down air motions caused by heat.

CORIOLIS EFFECT: The apparent curving motion of anything, such as wind, caused by Earth's rotation. It was first described in 1835 by French scientist Gustave Gaspard Coriolis.

CYCLONE: An area of low atmospheric pressure with winds blowing around it, counterclockwise in the Northern Hemisphere, clockwise in the Southern Hemisphere.

DOPPLER RADAR: Radar that measures speed and direction of a moving object, such as wind.

DOWNBURST: Wind blasting downward through the air. It may be due to a thunderstorm or shower.

DRIZZLE: Falling water drops with a diameter less than .02 inches.

DROUGHT: Period of abnormal dryness for a particular region.

EL NIÑO: Linked ocean and atmospheric events, which have worldwide effects, characterized by warming of water in the tropical Pacific from around the International Date Line to the coast of Peru.

EXTRATROPICAL CYCLONE: A large scale weather system that forms outside the tropics with a low pressure center.

FLASH FLOOD: Flooding with a rapid water rise.

FLOOD WARNING: Heavy rains are expected to cause flooding (minor, moderate or major).

FOG: A cloud with its base on the ground.

FUJITA SCALE: A scale created by Theodore Fujita for classifying tornadoes according to their rotational wind speed and the damage they cause. Categories range from an F0 (low) to an F5 (high) based on the wind speed.

FUNNEL CLOUD: A rotating column of air extending from a cloud, but not reaching the ground.

GOES: Geostationary Operational Environmental Satellite, a U.S. weather satellite in an orbit that keeps it above the same place on the equator.

GULF STREAM: A warm ocean current that flows from the Gulf of Mexico across the Atlantic to the European Coast. It helps warm Western Europe.

GUST FRONT: The boundary between cold air flowing downward out of a thunderstorm and the warmer air at the surface. Its passage is similar to that of a strong cold front.

HAIL: Balls of ice that grow in thunderstorm updrafts.

HEAT LIGHTNING: Glowing flash in clouds. No thunder is heard because lightning is too far away.

HIGH: An area of high atmospheric pressure, also called an anticyclone.

HURRICANE: A tropical cyclone with winds of 74 mph or more.

HYDROSPHERE: The Earth's water.

INTERTROPICAL CONVERGENCE ZONE: The area near the equator, called "The Doldrums" by sailors, where the trade winds converge.

INVERSION: Stable air condition in which air near the ground is cooler than air at a higher altitude.

JET STREAM: A narrow band of wind in the upper atmosphere with speeds greater than 57 mph.

LATENT HEAT: Energy stored when water evaporates into vapor or ice melts into liquid. It's released as heat when water vapor condenses or water freezes.

LATITUDE: Distance on the Earth's surface measured in degrees north and south of the equator.

LIGHTNING: A visible discharge of electricity produced by a thunderstorm.

LONGITUDE: Distance on the Earth's surface measured in degrees east and west from the prime meridian.

LOW: An area of low atmospheric pressure.

MARITIME AIR MASS: An air mass that forms over an ocean, making it humid. It may be warm or cold.

MERIDIONAL FLOW: A north to south to north flow of high altitude winds.

MESOCYCLONE: A rotating, upward moving column of air in a thunderstorm that can spawn tornadoes.

MESOSCALE: In meteorology, weather systems and events up to about 250 miles across.

METEOROLOGICAL BOMB: An extra-tropical cyclone in which the center pressure drops an average of one millibar an hour for 24 hours. Usually refers to storms off the U.S. East Coast.

MICROBURST: A downburst less than 2.5 miles in diameter.

MID LATITUDES: Region of the Earth outside the polar and tropical regions, between latitudes 23.5 degrees and 66.5 degrees.

MILLIBAR: A metric unit of air pressure measurement. The average atmospheric pressure at sea level is 1013 millibars.

MOIST ADIABATIC LAPSE RATE: The variable rate at which rising air cools or sinking air warms when water is changing phases in the air.

MONSOON: Persistent, widespread, seasonal winds that seasonally reverse directions. Usually summer winds from the ocean bring rain, while winter winds from the land are dry.

MULTICELL STORMS: Thunderstorms consisting of clusters of single cell thunderstorms.

NATIONAL CLIMATIC DATA CENTER (NCDC): The National Oceanic and Atmospheric Administration office in Asheville, NC, that keeps climate records.

NATIONAL HURRICANE CENTER (NHC): National Weather Service office in Coral Gables, FL, that tracks and forecasts hurricanes and other weather in the Atlantic, Gulf of Mexico, Caribbean Sea, and parts of the Pacific.

NATIONAL METEOROLOGICAL CENTER (NMC): National Weather Service center in Camp Springs, MD, that prepares worldwide computer forecasts. Hurricane and Severe Storms centers are part of NMC.

NATIONAL SEVERE STORMS FORECAST CENTER: National Weather Service center in Kansas City, MO, that issues watches for severe thunderstorms and tornadoes across the nation.

NATIONAL SEVERE STORMS LABORATORY (NSSL): National Oceanic and Atmospheric Administration Laboratory in Norman, OK, that studies severe thunderstorms.

NATIONAL WEATHER SERVICE: Federal agency that observes and forecasts weather. Formerly the U.S. Weather Bureau, its part of the National Oceanic and Atmospheric Administration, which is part of the Department of Commerce.

NUMERICAL FORECASTING OR PREDICTION: Use of computers to solve mathematical equations and produce weather forecasts.

100 YEAR FLOODS: Water levels that, on average, should occur once a century. This is the same as water level with a 100 to 1 chance of occurring in any single year.

OZONE: Form of oxygen with molecules that consist of three oxygen atoms compared to two atoms for ordinary oxygen molecules.

OZONE HOLE: Zone of decreased ozone content that forms in the stratosphere over Antarctica each spring.

PREFRONTAL SQUALL LINES: Lines of thunderstorms ahead of an advancing cold front.

PRESSURE GRADIENT FORCE: Force acting on air caused by air pressure differences.

RAIN: Falling water drops with a diameter greater than .02 inch.

RAINBOW: Arc or circle of colored light caused by the refraction and reflection of light by water droplets.

RELATIVE HUMIDITY: The ratio of the amount of water vapor actually in the air compared to the maximum amount of water vapor the air can hold at its current temperature and pressure. This is expressed as a percentage.

RIDGE: An elongated area of high atmospheric pressure, running generally north south, at the surface or aloft.

SAFFIR SIMPSON HURRICANE DAMAGE POTENTIAL SCALE: A 1 to 5 scale, developed by Robert Simpson and Herbert Saffir that measures hurricane intensity.

SEA BREEZE: Winds blowing inland from any body of water.

SEVERE THUNDERSTORM: A thunderstorm with winds faster than 57 mph or hailstones three quarters of an inch or larger in diameter.

SHORT WAVE: A bend, or wave of wind, only tens of miles long that moves along in the wind flow of upper atmosphere.

SOLAR ENERGY: The energy produced by the sun.

SQUALL LINE: A line of thunderstorms.

STABLE AIR: Air in which temperature and moisture discourage formation of updrafts and downdrafts. Clouds will be low and flat any precipitation will be steady.

STATIONARY FRONT: A warm cold air boundary with neither cold nor warm air advancing.

STORM SURGE: Quickly rising ocean water levels associated with hurricanes that can cause widespread flooding.

STORM TRACKS: Paths that storms generally follow.

STRATOSPHERE: The layer of the atmosphere from about 7 to 30 miles up.

SUPERCELL: A fierce thunderstorm that usually lasts several hours, often spinning out a series of strong tornadoes.

SYNOPTIC SCALE: Large scale weather events and systems, generally more than 200 miles across.

THUNDER: Sound produced by a lightning discharge.

THUNDERSTORMS: Localized storms that produce lightning, and therefore, thunder.

TORNADO: A strong, rotating column of air extending from the base of a cumulonimbus cloud to the ground.

TRADE WINDS: Global scale winds in the tropics that blow generally toward the west in both hemispheres.

TRANSPIRATION: Release of water vapor into the air by plants.

TROPICAL CYCLONE: A low pressure system in which the central core is warmer than the surrounding atmosphere.

TROPICAL DEPRESSION: A tropical cyclone with maximum sustained winds near the surface of less than 39 mph.

TROPICAL DISTURBANCE: Rotary air circulation 160 to 300 kilometers across associated with a low-pressure area over the tropical ocean.

TROPICAL STORM: A tropical cyclone with 39 to 74 mph winds.

TROPICS: Region of the Earth from latitude 23.5 degrees north the Tropic of Cancer southward across the equator to latitude 23.5 degrees south the Tropic of Capricorn.

TROPOPAUSE: The boundary between the troposphere and the stratosphere.

TROPOSPHERE: The lower layer of the atmosphere, extending from the surface up to 7 or 8 miles above the Earth.

TYPHOON: A tropical cyclone with winds more than 75 miles/hour and located in the north pacific, west of the International Date Line.

WARM FRONT: A warm cold air boundary with warm air advancing.

WARNING: Severe weather conditions are expected in the specified area of the warning, usually within 24 hours.

WATCH: Severe weather conditions pose a threat to coastal areas, generally within 36 hours.

WATER VAPOR: Water in a gaseous state.

TERRORISM-RELATED TERMS

ANTI-TERRORISM: Defensive measures against terrorism.

COMBATING TERRORISM: The full range of Federal programs and activities applied against terrorism, domestically and abroad, regardless of the source or motive.

CONSEQUENCE MANAGEMENT: Consequence management is predominately an emergency management function and includes measures to protect public health and safety, restore essential government services, and provide emergency relief to governments, businesses and individuals affected by the consequences of terrorism. In an actual or potential terrorist incident, a consequence management response will be managed by FEMA using structures and resources of the Federal Response Plan (FPR). These efforts will include support missions as described in other Federal operations plans, such as predictive modeling, predictive action recommendations, and mass decontamination.

COUNTERTERRORISM: Offensive (proactive) measures against terrorism.

CRISIS MANAGEMENT: Crisis management is predominantly a law enforcement function and includes measures to identify, acquire, and plan the use of resources needed to anticipate, prevent and/or resolve a threat or act of terrorism. In a terrorist incident, a crisis management response may include traditional law enforcement missions, such as intelligence, surveillance, tactical operations, negotiation, forensics, and investigations, as well as technical support missions, such as agent identification, search, render safe procedures, transfer and disposal, and limited decontamination. In addition to traditional law enforcement missions, crisis management also includes assurance of public health and safety.

CYBERCRIME: Use of computers to carry out fraud, embezzlement, copyright infringement, scams, and other illegal activities.

CYBER-DETERRENCE: Integration of conventional forces, technological exhibitionism, and strategic simulations as a deterrent to enemy aggression.

CYBERTERRORISM: Computer-based, information-oriented terrorism.

CYBERWAR: Information-oriented warfare waged by formal military forces.

CYBOTAGE: Acts of disruption and destruction against information infrastructures; computer sabotage.

CYBOTEUR: One who commits cybotage; anarchistic or nihilistic computer hacker; computer saboteur.

DIRTY BOMB: A radiological dispersion device that combines conventional explosives, such as dynamite, with radioactive materials in the form of powder or pellets. The idea behind a dirty bomb is to blast radioactive material into the area around the explosion. This could possibly cause buildings and people to be exposed to radioactive material. The main purpose of a dirty bomb is to frighten people and make buildings or land unusable for a long period of time.

HACKING: Breaking into computer networks.

HACTIVISM: Use of hacking by social activists with the intent of disrupting normal operations but not causing serious damage.

INFORMATION WARFARE: When broadly defined, this term refers to the use of technology against technology, to deny some entity the ability to use its own technology and its information. Information warfare may be waged against industries, political spheres of influence, global economic forces, or countries. When narrowly defined, this term refers to military uses of information technology.

INFOSPHERE: The totality of all information media, especially those that are interconnected and internetted.

NETWAR: Information-oriented conflict waged by networks of primarily nonstate actors.

(Some authors restrict the definition of netwar to information related conflict at a grand level between nations or societies. Others broaden it to include attacks on private or corporate systems or a city's infrastructure.)

TERRORISM: Terrorism includes the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.

WEAPON OF MASS DESTRUCTION (WMD): A WMD is any device, material, or substance used in a manner, in a quantity or type, or under circumstances evidencing intent to cause death or serious injury to persons or significant damage to property.

From ATerrorism Evolves Toward Netwar,@ in Rand Review Winter 1998-99 issue; and Denning, Dorothy E., AActivism, Hactivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy,@ in Networks and Netwars: The Future of Terror, Crime, and Militancy . Arquilla, John, and Ronfeldt, David, eds. Rand Corp., 2001. Both accessed at www.rand.org/publications/randreview/issues/rrwinter98.9/ madness.html.

Appendix A:

Hazard Checklists and Procedures

CHECKLISTS AND PROCEDURES [2]

1. Emergency Evacuation Procedures
2. Facility Disaster Supplies Kit
3. Employee Family Disaster Plan
4. Emergency Call-Down Procedures
5. Shelter in Place Procedures

NATURAL HAZARDS CHECKLISTS AND PROCEDURES

6. What to do Before, During and After a Hurricane
7. Flood Safety Checklist
8. Tornado Safety Checklist
9. Lighting Safety Checklist
10. Wildfire Safety Checklist
11. Sinkhole Action Checklist
12. Extreme Heat Safety Checklist
13. Water Conservation Checklist
14. Winter Storm Safety Checklist
15. Steps to Protect Your Farm from Pests and Disease

TECHNOLOGICAL HAZARDS CHECKLISTS AND PROCEDURES

16. What to do During and After a Hazardous Material Incident
17. Fire Safety Checklist
18. Tips for Fire Prevention for Small Business
19. Power Service Disruption Checklist
20. Bomb Threat Procedures
21. Cyber Security Threat Assessment
22. Cyber Security Checklist
23. Checklist to Prepare and Respond to a Chemical/Biological Attack
24. Handling Suspicious Parcels and Letters
25. Radiological Emergency Safety Checklist
26. Radiological Emergency: Immediate Precautions in the Case of a Terrorist Attack
27. Prevention and Response to Workplace Violence
28. The Evacuation "GO BOX"
29. Strategies to Minimize Impact of Workplace Absenteeism (Pandemic Flu)

[2] Use for both Natural and Technological Hazards

CHECKLIST #1

EMERGENCY EVACUATION PROCEDURES

Evacuations are more common than many people realize. Hundreds of times each year, transportation and industrial accidents release harmful substances, forcing thousands of people to leave their homes. Fires and floods cause evacuations even more frequently. And almost every year people along the Gulf and Atlantic coasts evacuate in the face of approaching hurricanes. When community evacuations become necessary, local officials provide information to the public through the media. In some circumstances other warning methods, such as sirens or telephone calls, are also used.

The amount of time you have to evacuate will depend on the disaster. If the event can be monitored, like a hurricane, you might have a day or two to get ready (See what to do before, during and after a Hurricane.) However, many disasters allow no time for people to gather even the most basic necessities.

Planning for evacuation.

Ask your local emergency management agency about community evacuation plans. Learn evacuation levels and routes. In your planning, consider different scales of evacuations. In a hurricane, for example, thousands of coastal residents would evacuate, while a much smaller area would be affected by a chemical release.

- ❑ Talk with your employees about the possibility of evacuation. Plan where you would go if you had to leave the building or the community. Ensure all employees would have transportation in the event of an emergency evacuation.
- ❑ Plan a place to meet your key employees in case you are separated from one another in a disaster. Designate someone to be the "checkpoint" so that employees can call that person to say they are safe.
- ❑ Assemble a disaster supplies kit for each facility. Include a battery-powered radio, flashlight, extra batteries, food, water and first aid kit. See the " Disaster Supplies Kit" for a complete list.
- ❑ Keep fuel in your car(s) if an evacuation seems likely. Gas stations may be closed during emergencies and unable to pump gas during power outages.
- ❑ Know how to shut off your facility's electricity, gas and water supplies at main switches and valves. Have the tools you would need to do this (usually adjustable pipe and crescent wrenches).
- ❑ Listen to a NOAA Weather Alert or battery-powered radio and follow local instructions.

If the danger is a chemical release, bomb threat or fire and you are instructed to evacuate, gather your employees and leave immediately.

- ❑ Implement the Warning Procedure to alert all employees of the danger and immediate evacuation.
- ❑ If there is sufficient time, take the server or backup tapes (in fire-proof container) to a safer location.
- ❑ Congregate at the appropriate meeting place outside of the building to verify all employees have evacuated the building.
- ❑ Confirm the Emergency Communications Plan (call-down procedures, emergency contact).
- ❑ If necessary, initiate the Continuity of Operations Plan (alternate work site(s), telework, etc.).

In other cases, you may have time to follow these steps:

- ❑ Secure your facility. Back up data files and take server(s) to a more secure site. Unplug appliances. Protect equipment.
- ❑ Turn off the main water valve and electricity, if instructed to do so. Close and lock doors and windows.
- ❑ Leave early enough to (1) allow employees to secure their homes and purchase any needed emergency supplies, if appropriate, and (2) avoid being trapped by severe weather, other evacuation traffic, emergency response, etc.
- ❑ Follow recommended evacuation routes. Be alert.

CHECKLIST #2

FACILITY DISASTER SUPPLIES KIT

One of the most important tools for emergency preparedness is the Disaster Supplies Kit. Below are the most important items for your kit at home. At the office, the amount of food and water should reflect what is necessary for a minimum of three days. Stock up today and store in a water-resistant container. Replenish as necessary, especially at the beginning of hurricane season June 1.

- ❑ Two weeks supply of prescription medicines
- ❑ Two weeks supply of non-perishable/special dietary foods
- ❑ Drinking Water/containers - 1 gal/per person/per day (minimum 3 days)
- ❑ Flashlights and batteries for each employee
- ❑ Portable radio and batteries
- ❑ First aid book and kit including bandages, antiseptic, tape, compresses, aspirin and aspirin pain reliever, anti-diarrhea medication, antacid, Syrup of Ipecac (used to promote vomiting if advised by the Poison Control Center)
- ❑ Mosquito repellant
- ❑ Fire extinguisher (small canister, ABC type)
- ❑ Instant tire sealer
- ❑ Whistle and/or distress flag
- ❑ Two coolers (one to keep food; one to go get ice)
- ❑ Plastic tarp, screening, tools and nails, etc.
- ❑ Water purification kit (tablets, chlorine (plain) and iodine)
- ❑ Infant necessities (medicine, sterile water, diapers, ready formula, bottles), if needed
- ❑ Clean-up supplies (mop, buckets, towels, disinfectant)
- ❑ Camera and film
- ❑ Non-electric can opener
- ❑ Extra batteries for camera, flashlights, radio, portable TV & lamps, etc.
- ❑ Garbage Can or bucket with tight-fitting lid (for emergency toilet)
- ❑ Plastic trash bags
- ❑ Toilet paper, paper towels and pre-moistened towelettes

If there is a chance employees would remain at the facility, also consider:

- ❑ Pillows, blankets, sleeping bags or air mattresses
- ❑ Extra clothing, shoes, eyeglasses, etc.
- ❑ Folding chairs, lawn chairs or cots
- ❑ Personal hygiene items (toothbrush, toothpaste, deodorant, etc.)
- ❑ Quiet games, books, playing cards, etc.

Precious commodities before and after a disaster

- ❑ Cash (With no power, banks may be closed, checks and credit cards unaccepted, and ATMs may not be operational.)
- ❑ Charcoal, Wooden Matches and Grill
- ❑ Ice

CHECKLIST #3

EMPLOYEE FAMILY DISASTER PLAN

OUR FAMILY DISASTER PLAN

We don't like to think about a disaster in our community - much less take the time (and expense) to prepare our homes, families and business to weather a storm or other disaster. Yet, if you are armed with knowledge and a little forethought, you can save yourself and your family from potential injury and financial loss. It will also be critical that, as your employer, we know what your needs are before the event and ensure we can contact you after a disaster. To get started, first read the disaster preparedness guide provided to you. Then, prepare your own Family Disaster Plan by completing the checklist below:

1. **KNOW YOUR RISK**

   Will your family have to evacuate in a hurricane? (Y or N) ____ If yes, what Evacuation Level _____

   100-year Flood Zone (Y or N) _____ If yes, is your home elevated above Base Flood Elevation? (Y or N) _____

   Mobile home (Y or N) _____

2. **HAVE AN EVACUATION PLAN**

   If I do not have to evacuate, I will secure my house and stay. My employer can reach me at:

   Phone No. _____

   If told to evacuate, we will go to:

   Friends/Name _____

   Phone No. _____

   Emergency Phone No. _____

   Hotel/Motel _____

   Shelter _____

   Out of the Area (Y or N) ____

   Evacuation Route _____

3. **Members of Your Family**

1. First Name:	**2. First Name:**
Last Name:	**Last Name:**
Age:	**Age:**
Mobile Phone:	**Mobile Phone:**
SS #:	**SS #:**
Employed By:	**Employed By:**
Work Phone:	**Work Phone:**
Blood Type:	**Blood Type:**
Allergies:	**Allergies:**
Special Needs:	**Special Needs:**
3. First Name:	**4. First Name:**
Last Name:	**Last Name:**
Age:	**Age:**
Mobile Phone:	**Mobile Phone:**
SS #:	**SS #:**
Employed By:	**Employed By:**
Work Phone:	**Work Phone:**
Blood Type:	**Blood Type:**
Allergies:	**Allergies:**
Special Needs:	**Special Needs:**

4. **PUT TOGETHER YOUR DISASTER SUPPLIES KIT (see Checklist #2)**

5. **RELATIVES/FRIENDS TO CONTACT W/EMERGENCY INFO**

Name/Phone _____

_____

Name/Phone _____

_____

6. **MEDICAL AND INSURANCE.** Call your agent. Make sure you are adequately covered. Put your Agent's Name/Phone Number and policy in a safe place along with an inventory of your belongings (a video tape is excellent).

Physician	**Dentist**
Name:	Name:
Address:	Address:
Phone:	Phone:
Physician	**Medical Insurance**
Name:	Carrier:
Address:	Policy Number:
Phone:	Address:
Car Insurance	**Home Insurance**
Carrier:	Carrier:
Policy Number:	Policy Number:
Address:	Address:

7. **INSPECT & SECURE YOUR HOME BEFORE THE STORM**
   - Garage Doors - 80% of the severe winds enter through an older, un-reinforced garage door. You can reinforce older metal doors (not wood) with kits sold at a home improvement store or replace with a hurricane-resistant one.
   - Entry Doors - Double-bolt (top and bottom) all doors. (Exterior doors should be solid wood or steel.)
   - Gable Ends/ Roof - During Hurricane Andrew, winds destroyed roofs due to un-reinforced gable ends. If your home was built before 1994, the gables should be retrofitted to strengthen the roof system. When you replace your roof, make sure the new sheathing is attached properly as well as new shingles or tiles.
   - Window Protection- is very important to keep the winds out of your home. Once inside, internal wind pressure can lift your roof right off and expose you and your family to the winds. Windows should also be covered to reduce the risk of flying glass. Code approved shutters, impact resistant windows, plywood sheets (3/4"), shutter or other wind abatement systems should be considered.
   - Maintenance is an important part of reducing the potential risk to damage. Keep your home in good repair.

8. **FAMILY RESPONSIBILITIES**

   Make a list of tasks and who is responsible for each task; Don't forget to include the kids.

9. **PLAN FOR PETS**

Name:	**Name:**
Tag Number:	**Tag Number:**
Type of Animal:	**Type of Animal:**
Pet Shelter	**Veterinarian**
Name:	**Name:**
Address:	**Address:**
Phone:	**Phone:**

10. **DO YOU OR A LOVED ONE REQUIRE EVACUATION ASSISTANCE DUE TO SPECIAL NEEDS? CONTACT YOUR LOCAL EMERGENCY MANAGEMENT DEPARTMENT TO REGISTER TODAY.**

Eldercare

Name _____

Address _____

Phone _____

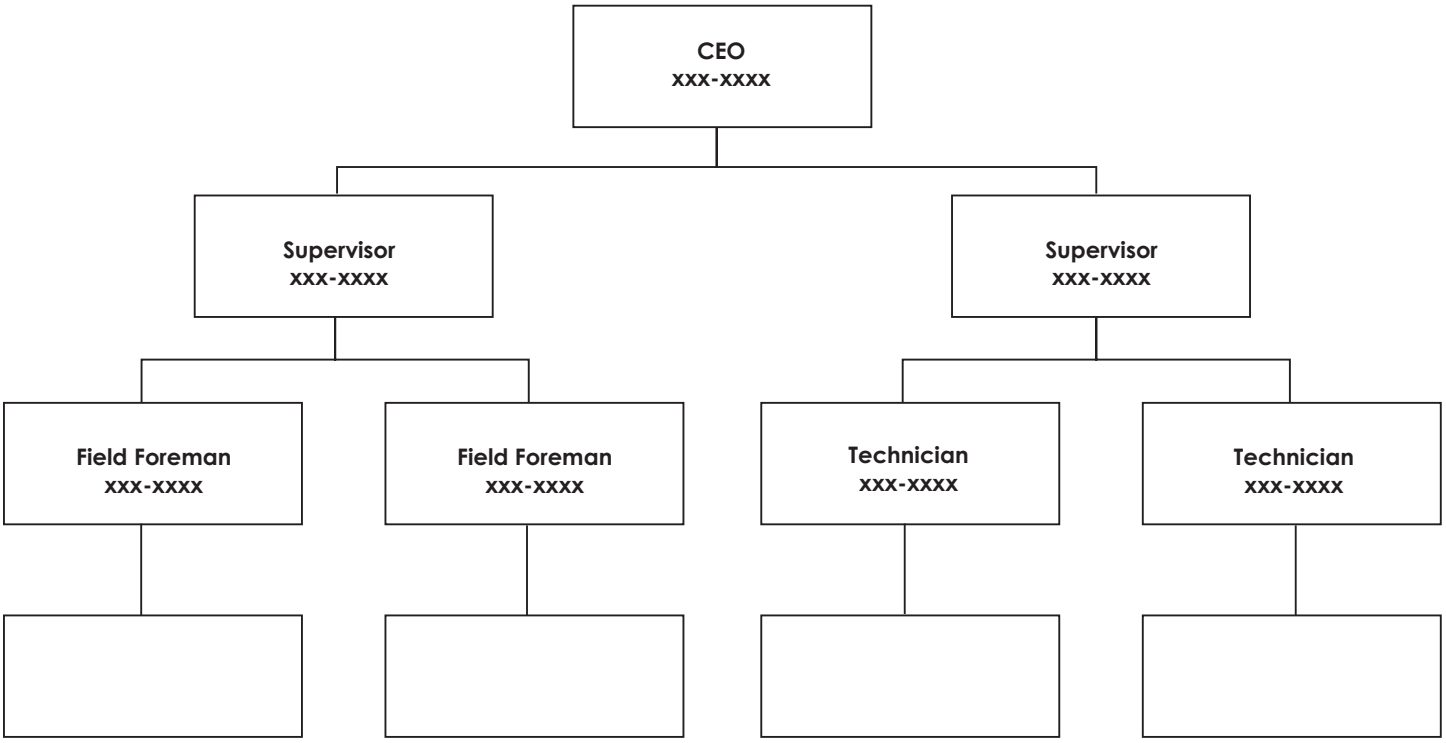
Special Needs Shelter _____

- ❑ Medications (Must be labeled with name and dosage. Including over-the-counter and samples.)
- ❑ Living Will
- ❑ Medical Bracelet-Allergies and Conditions
- ❑ Copy of insurance card (s)
- ❑ Emergency Contact Information
- ❑ Special Diet Needs

CHECKLIST #4

EMERGENCY CALL-DOWN PROCEDURES

(CASCADE SYSTEM)



CHECKLIST #5

SHELTER IN-PLACE PROCEDURES

Stay inside the facility. This action will be recommended if there is a short release, a small amount of hazardous material in the air, or if time does not permit evacuation before the arrival of a cloud of toxic vapor. Take these steps to protect yourself and employees:

- ❑ Stay inside until local officials say you can leave safely. This will most likely be for no more than a few hours.
- ❑ If your business has animals, if possible bring them indoors!
- ❑ Close all doors and windows.
- ❑ Seal all gaps under doorways and windows with dry towels and duct tape.
- ❑ Turn off heating, cooling or ventilation systems.
- ❑ Listen to your local radio or TV stations for further instructions.
- ❑ Resist the impulse to go outdoors and "check things out" before given the "All Clear" by authorities.
- ❑ If you are told to protect your breathing, cover your nose and mouth with a dry handkerchief or other cloth folded over several times.

CHECKLIST #6

WHAT TO DO BEFORE, DURING AND AFTER A HURRICANE

- ❑ **Know Your Risk**. Check your hurricane evacuation level and FEMA flood maps to determine if your business location is vulnerable to storm surge or freshwater flooding. Have your building(s) inspected by a licensed professional to find out if your workplace is vulnerable to hurricane force winds and what is recommended to retrofit.
- ❑ **Take the Necessary Precautions**. If a storm threatens, secure your building. Cover windows. Cover and move equipment/furniture to a secured area.
- ❑ **ALWAYS Protect your data with backup files.** If dependent on data processing, consider an alternate site. Make provisions for alternate communications and power.
- ❑ **Make plans to work with limited cash, and no water, sewer or power for two weeks.** Store emergency supplies at the office.
- ❑ **Protect Your Employees.** Employee safety comes first! Prepare, distribute and exercise your business hurricane plan for recovery. Consider providing shelter to employees and their families and helping employees with supplies after the storm. Establish a rendezvous point and time for employees in case damage is severe and communications are disrupted. Establish a call-down procedure for warning and post-storm communications. Provide Photo IDs and a letter of authorization to enter the building.
- ❑ **Contact Your Customers & Suppliers** and share your communications and recovery plan in advance. Prepare a list of vendors to provide disaster recovery services.
- ❑ **Review Your Insurance Coverage.** Have your business appraised at least every five years. Inventory, document and photograph equipment, supplies and workplace. Have copies of insurance policies and customer service/home numbers. Obtain Business Interruption Insurance. Consider Accounts Receivable and Valuable Papers Coverage and Income Destruction Insurance. If you have Business Owners Protection Package (BOPP), check co-insurance provisions. Remember: Flood damage requires separate coverage and is NOT covered under other insurance programs.
- ❑ **After the Storm.** Use caution before entering your business. Check for power lines, gas leaks and structural damage. If any electrical equipment is wet, contact an electrician. Prepare loss information for insurance claims and get independent estimates of damages. Take pictures before cleanup. Minimize additional damage.

HURRICANE SEASON CHECKLIST
TAKE ACTION NOW

The hurricane season is **June** through **November**. **Be prepared!**

- ❑ Refer to the County Hurricane Evacuation Map. Locate your business facility or facilities and its evacuation level (color). Determine if and when you would have to evacuate your business from storm surge. REMEMBER: All work trailers and most warehouse/ storage facilities are extremely vulnerable to hurricane-force winds, regardless of location.
- ❑ If ordered to evacuate, DECIDE NOW how and when you will communicate with employees and where you can establish an alternative work site if your facility is severely damaged or inaccessible.
- ❑ Check your Disaster Supplies Kit and obtain any items you need for the office. Purchase a battery-powered National Weather Service weather alert radio.
- ❑ Keep your facility in good repair. Make sure loose roofing and siding is tacked down and dead or broken branches from trees are trimmed. Trees should be trimmed up off the ground and away from roofs to reduce the risk of fire as well.
- ❑ Survey your facility to determine if there are any improvements you can make to make the facility safer. You may contact the Small Business Development Center for an Energy/ Mitigation Audit that will identify cost-beneficial improvements for your facility. Or contact a professional engineer or licensed contractor to inspect your home for structural integrity.
- ❑ Make plans and purchase materials to protect your facility before the storm (plywood panels, steel, aluminum or plastic shutters, plastic sheeting, nails, etc.). Make sure all products meet the Dade County large missile impact test.
- ❑ Inventory your property (a video tape is excellent). Store with insurance and title papers and back-up tapes in a fireproof safe and keep a copy in a (fire-proof safe) home located in a non-evacuation zone.

- ❑ Make sure your address (number) is clearly marked on your facility.
- ❑ Whether you rent or own your facility, review your insurance policies with your agent now.

HURRICANE CHECKLIST
AS THE STORM APPROACHES

- ❑ Listen for weather updates on local stations and on NOAA Weather Radio. Don't trust rumors, and stay tuned to the latest information.
- ❑ Check your Disaster Supplies Kit at work. Obtain any needed items. Contact employees and instruct them to do the same.
- ❑ Instruct employees to refill prescriptions and to maintain at least a two-week supply during hurricane season.
- ❑ Clear property or tie down any items that could become flying missiles in high winds, e.g. lawn furniture, potted plants, and trash cans.
- ❑ Protect the windows and glass doors! If you do not have impact resistant windows, install shutters or plywood to cover glass. Brace double entry and garage doors at the top and bottom.
- ❑ Fill fleet cars and equipment gas tanks and check oil, water and tires. Gas pumps don't operate without electricity.
- ❑ Secure your boat early. Drawbridges will be closed to boat traffic after an evacuation order is issued.
- ❑ Obtain sufficient cash for business operations recognizing that banks and ATMs won't be in operation without electricity and few stores will be able to accept credit cards or personal checks.
- ❑ Run through BCP to ensure the communications plan is up-to-date and employees are aware of responsibilities after the storm.
- ❑ Back-up all computer data and ensure that the back-up is stored in a safe place off-site.
- ❑ Close the office in sufficient time to allow employees to secure their homes, obtain needed supplies and evacuate if necessary.

HURRICANE CHECKLIST
NO EVACUATION

- ❑ If your facility is outside the evacuation area and NOT a work trailer, etc. your facility may be able to remain open or serve as shelter for employees.
- ❑ Make sure the windows and doors are protected and the facility is secured.
- ❑ Clean containers for drinking water and sinks for storing cleaning water. Plan on three gallons per person, per day for all uses.
- ❑ Offering your facility as shelter to employees and their families who live in vulnerable areas or mobile homes will have benefits to your operations but may also have some liability. Check first with legal representation.
- ❑ Check the Disaster Supplies Kit. Make sure you have at least a two-week supply of non-perishable foods. Don't forget a non-electric can opener. Instruct any employees to augment the supply with a kit of their own.
- ❑ During the storm, everyone should stay inside and away from windows, skylights and glass doors. Find a safe area in your facility (an interior, reinforced room, closet or bathroom on the lower floor if the storm becomes severe.
- ❑ Wait for official word that the danger is over. Don't be fooled by the storm's calm "eye."
- ❑ If flooding threatens your facility, electricity should be turned off at the main breaker.
- ❑ If your facility loses power, turn off major appliances, such as the air conditioner and water heater to reduce damage.

IF YOU MUST EVACUATE: SECURING YOUR FACILITY

Stay tuned to your local radio and television stations for emergency broadcasts. If ordered to evacuate, you must do so immediately.

- ❑ Ensure important documents, files, back up tapes, emergency contact information, etc. are taken to a safer location. See "Go Box".
- ❑ Let employees, customers and vendors know your continuity plans. Make sure your employees have a safe ride.
- ❑ Turn off electricity, water and gas.
- ❑ Lock windows and doors.

HURRICANE CHECKLIST
AFTER THE STORM

After a disaster your business may be without power, water, food or any of the services we rely on. Immediate response may not be possible, so residents and businesses must be prepared to be self-reliant for several weeks.

RE-ENTRY

- ❑ Be Patient. Access to affected areas will be controlled. You won't be able to return to your facility until search and rescue operations are complete and safety hazards, such as downed trees and power lines, are cleared. It may take up to three days for emergency crews to reach your area. It may take 2-4 weeks before utilities are restored. On barrier islands, it could take much longer.
- ❑ Stay tuned to your local radio station for advice and instructions about emergency medical aid, food and other forms of assistance.
- ❑ Security operations will include checkpoints. It will be critical for you and your employees to have valid identification with your current local address as well as something to prove your employment and need to get back into the area. It is recommended that businesses contact the county emergency management agency and local jurisdiction to determine what specifically would be required.
- ❑ Avoid driving. Roads will have debris that will puncture your tires. Don't add to the congestion of relief workers, supply trucks, law enforcement, etc.

SAFETY CHECKLIST

- ❑ Avoid downed or dangling utility wires. Metal fences may have been "energized" by fallen wires. Be especially careful when cutting or clearing fallen trees. They may have power lines tangled in them.
- ❑ Beware of snakes, insects or animals driven to higher ground by floods.
- ❑ Enter your home with caution. Open windows and doors to ventilate and dry your facility.
- ❑ If there has been flooding, have an electrician inspect your office before turning on the breaker.
- ❑ Be careful with fire. Do not strike a match until you are sure there are no breaks in gas lines. Avoid candles. Use battery-operated flashlights and lanterns instead.
- ❑ Use your telephone only for emergencies to keep lines open for emergency communications.

GENERATORS

- ❑ Fueled by gas, generators can run appliances and fans.
- ❑ Sizes range from 750 watts that will run a fan and a light up to 8,000 watts that will practically run a house (except for the air conditioner).
- ❑ If you have lost power, don't connect a portable generator to building wiring (this could injure or kill neighbors or electrical crews).
- ❑ Plug equipment, computers, etc., directly into the generator.

- ❑ Place generator outdoors or in a well-ventilated area. Don't forget to check the oil every time you add gas. Conserve fuel by alternative appliances. For example, refrigerators can be kept cool by supplying power eight hours a day. Refrigerators require 400-1,000 watts.

REPAIRS

- ❑ Make temporary repairs to correct safety hazards and minimize further damage. This may include covering holes in the roof, walls or windows and debris removal.
- ❑ PROTECT YOURSELF FROM CONTRACTOR FRAUD! Only hire licensed contractors to do repairs. Check with the local Building Department to ensure the contractor is licensed. If you hire a contractor, don't pull the permits for them. If the contractor makes this request, it may be an indication that he is not properly licensed.
- ❑ Take photographs of all damage before repairs and keep receipts for insurance purposes.
- ❑ After assessing damage to your facility, contact your local building department for information on required building permits. Permits are always required for any kind of demolition or permanent repairs, reconstruction, roofing, filling and other types of site development. Report illegal flood plain development to your local building department.
- ❑ Local ordinances do not permit dumping in drainage canals or ditches because it causes backups and overflow in the system. Report illegal dumping.

WATER PRECAUTIONS

Whenever widespread flooding occurs, there is a potential for bacterial contamination. Bacteria, such as shigella and salmonella, can lead to life threatening dehydration for people if untreated by antibiotics. Disinfect any tap water you drink or use for cooking or cleaning. You must purify the tap water until officials notify you of its safety. Bring water to a rolling boil for a full 10 minutes or use chemicals (eight drops of chlorine bleach or iodine per gallon) or water purification tablets, as directed. Let the water sit at least 10 minutes before using. Water you saved in clean containers before the storm will be fine for 2-3 weeks. To be sure, add two drops of chlorine or iodine per gallon before drinking.

CLEAN-UP PRECAUTIONS

- ❑ Call professionals to remove large, uprooted trees, etc.
- ❑ Always use proper safety equipment such as heavy gloves, safety goggles, heavy boots, light- colored long-sleeve shirts and long pants.
- ❑ Tie back long hair, wear a hat and sunscreen.
- ❑ Drink plenty of fluids, rest and ask for help when you need it.
- ❑ Lift with the legs, not with the back.
- ❑ Don't burn trash.
- ❑ If you can't identify it, don't touch it.
- ❑ Be extremely careful with a chain saw and always heed safety warnings.

CHECKLIST #7

FLOOD SAFETY CHECKLIST

If you are at risk from flooding, here are protective measures that need to be taken:

Preparatory Stage

- ❑ KNOW YOUR RISK!

Contact your insurance agent to determine if your business is in the 100-year or 500-year flood plain. If it is, purchase flood insurance! If it isn't, consider purchasing flood insurance. More than 40% of all disaster flood loans are made to victims outside of the designated flood plain. Check your policy (ies) to ensure your business is adequately protected.

- ❑ DISASTER SUPPLIES KIT

Your kit may include a stock of food that requires no cooking/ refrigeration, but it should - at a minimum - have a first aid kit and weather alert radio.

- ❑ If you are vulnerable to flooding, consider acquiring sandbags or other materials to slow seepage into your building. Investigate other methods to reduce your risk of flooding including floodproofing, elevation or relocation.
- ❑ Have a plan to protect your records, equipment and files. Move valuable objects higher. Place them on shelves, tables and counter tops.
- ❑ Fuel your vehicle(s) and check oil and water.

AFTER THE FLOOD: SAFETY TIPS FOR EMPLOYEES

- ❑ Stay on higher ground until coast is clear.
- ❑ DO NOT DRIVE ON A FLOODED ROAD
- ❑ Don't attempt to wade in the water.
- ❑ Stay away from disaster areas.
- ❑ Do not handle live electrical equipment.
- ❑ Report downed power lines.
- ❑ Keep tuned to local stations for emergency information.

CHECKLIST #8

TORNADO SAFETY CHECKLIST

- ❑ Have a Weather Alert Radio in the office.
- ❑ Have a Plan to provide emergency notification (Warning System) to all employees, clients, visitors and customers in an emergency.

If a Tornado Warning is issued or if threatening severe weather approaches, make sure employees:

- ❑ Move to an interior room or hallway on the lowest floor and, if possible, get under a heavy piece of furniture.
- ❑ Stay away from windows.
- ❑ Mobile homes/ work trailers, even if tied down, offer little protection from tornadoes and should be abandoned.
- ❑ Occasionally, tornadoes develop so rapidly that advance warning is not possible. Remain alert for signs of an approaching tornado. Flying debris from tornadoes causes most deaths and injuries.

CHECKLIST #9

LIGHTNING SAFETY CHECKLIST

The chances of being struck by lightning are one in 600,000 but can be reduced by following safety rules. Most lightning deaths and injuries occur when people are caught outdoors. Make sure your employees know your policy regarding thunderstorm and lightning safety. And make sure employees' safety comes first. In recent years, people have been killed by lightning while: boating, swimming, golfing, bike riding, standing under a tree, riding on a lawnmower, talking on the telephone, loading a truck, playing sports, etc.

THE 30-30 RULE

30 seconds:

Count the seconds between seeing lightning and hearing thunder. If this time is less than 30 seconds, lightning is still a potential threat. Seek shelter immediately.

30 Minutes:

After hearing the last thunder, wait 30 minutes before leaving shelter. Half of all lightning deaths occur after the storm passes. Stay in a safe area until you are sure the threat has past.

LIGHTNING CAN STRIKE ANYWHERE!

Lightning Safety Tips

- Check the weather forecast before leaving for extended periods outdoors.
- Watch for signs of approaching storms.
- Postpone outdoor activities if thunderstorms are imminent.
- Check on those who have trouble taking shelter if severe weather threatens.
- If you can hear thunder, seek shelter. Move to a sturdy building or car.
- Do not take shelter in small sheds, under isolated trees, or in a convertible.
- Get out of boats and pools and away from water.
- Do not use electrical appliances or the telephone unless it is cordless.
- If you feel your skin tingle or your hair stand on end, squat low to the ground on the balls of your feet. Place your hands on your knees with your head between them. Make yourself the smallest target possible and minimize your contact with the ground.

CHECKLIST #10

WILDFIRE SAFETY CHECKLIST

PREVENTION: THE FLORIDA FIREWISE PROGRAM

Step 1. Choose a firewise location.

- ❑ Check with local officials to see what fire protection is available.
- ❑ Evaluate the site. A level area is better than a sloped one.
- ❑ Ensure that emergency vehicles will have easy access.
- ❑ Don't forget to clearly mark your location so firefighters can find you.

Step 2. Design and build firewise structures.

- ❑ Work with architects, contractors and fire officials to create a design that is both aesthetically pleasing and firewise.
- ❑ The number one cause of structural losses in wildland fires is from untreated wood shake roofs.
- ❑ Don't let sparks jump from your business or home to the wildland---or from a wildland fire to your home or business.

Step 3. Stay on guard with firewise landscaping and maintenance.

For specific information, go to www.firewise.org

EMERGENCY EVACUATION

- ❑ Implement the Warning Procedure to alert all employees of the danger and immediate evacuation.
- ❑ If there is sufficient time, take the vital records, i.e., server or backup tapes (in fire-proof container) to safer location. See "Go Box".
- ❑ Congregate at the appropriate meeting place outside of the building to verify all employees have evacuated the building.
- ❑ Confirm the Emergency Communications Plan (call-down procedures, emergency contact)
- ❑ If necessary, initiate the Continuity of Operations Plan (alternate work site(s), telework options, etc.).

CHECKLIST #11

SINKHOLE ACTION CHECKLIST

- ❑ If a sinkhole forms on a street, mark and secure the sinkhole, and notify the agency responsible for maintenance, e.g. County Public Works Department; Municipal Public Works Department; Civic Association; or Private road maintained by adjacent property owners.
- ❑ If reported sinkhole is located on private property, mark and secure the area and determine if any structures are in danger. Indications of possible structural damage include: cracks in walls, floors, and pavement, and/or cracks in the ground surface.

If structures are in possible danger:

- ❑ A representative from the County Emergency Management Agency will respond to the scene and conduct a survey to determine if the structure is in danger or other hazards exist, and advise the business owner on contacting the appropriate agencies (i.e., insurance, utilities, phone, fire department).
- ❑ If the business is in danger, occupants will be advised that they should evacuate until assessment and repairs are made.
- ❑ The business owner must contact their insurance agent to send a claims representative out to assess the damage and make arrangements for repairs.

If it is determined that a sinkhole is on private property and no structures are in danger:

- ❑ Ensure that sinkhole is marked and secured. Make sure the sink is fenced, roped, or taped very clearly. Usually, the property owner will be liable if someone is hurt in the sinkhole.
- ❑ If lake or river levels are affected, or you think groundwater quality is endangered by a sinkhole, report it to the Water Management District in your area.
- ❑ If your business is threatened, contact your insurance company.
- ❑ Check carefully for signs of the sinkhole enlarging, especially toward buildings, septic tanks, drain fields, and wells (flowing water into a sinkhole will continue or accelerate its growth). This can be done with a thin hard metal rod that can be pushed into the soil. Areas near the sink will offer less resistance to the rod than the unaffected soil.
- ❑ Do not throw any waste into the sinkhole. Do not use the sinkhole as a drainage system. Pesticides and other wastes seep easily through the sinkhole into the aquifer - your drinking water.
- ❑ Do not construct buildings between sinkholes that form a line in a northwest-southeast or northeast-southwest direction.
- ❑ The county will not repair sinkholes on private property. If the hole is small, fill the hole with clean sand or dirt and monitor it for future growth.
- ❑ If the hole is large, contact your insurance agent and have them send a claims adjuster out to assess the damage and make arrangements for repairs.
- ❑ The business may make contact with a geo-technical engineering firm (private contractor) to evaluate the hole to officially determine if it is a sinkhole.

CHECKLIST #12

EXTREME HEAT SAFETY CHECKLIST

- ❑ Stay indoors as much as possible.
  - If air conditioning is not available, stay on the lowest floor out of the sunshine.
  - Remember that electric fans do not cool; they just blow hot air around.
- ❑ Eat well-balanced, light and regular meals. Avoid using salt tablets unless directed to do so by a physician.
- ❑ Drink plenty of water regularly even if you do not feel thirsty.
  - Persons who have epilepsy or heart, kidney, or liver disease, are on fluid-restrictive diets, or have a problem with fluid retention should consult a doctor before increasing liquid intake.
- ❑ Limit intake of alcoholic beverages.
  - Although beer and alcoholic beverages appear to satisfy thirst, they actually cause further body dehydration.
- ❑ Never leave children or pets alone in closed vehicles.
- ❑ Dress in loose-fitting clothes that cover as much skin as possible.
  - Lightweight, light-colored clothing reflects heat and sunlight and helps maintain normal body temperature.
- ❑ Protect face and head by wearing a wide-brimmed hat.
- ❑ Avoid too much sunshine.
  - Sunburn slows the skin's ability to cool itself. Use a sunscreen lotion with a high SPF (sun protection factor) rating (i.e., 15 or greater).
- ❑ Avoid strenuous work during the warmest part of the day. Use a buddy system when working in extreme heat and take frequent breaks.
- ❑ Spend at least two hours per day in an air-conditioned place. If your home is not air conditioned, consider spending the warmest part of the day in public buildings such as libraries, schools, movie theaters, shopping malls and other community facilities.
- ❑ Check on family, friends, and neighbors who do not have air conditioning and who spend much of their time alone.

First-Aid For Heat-Induced Illnesses

1. Sunburn
   - Symptoms: Skin redness and pain, possible swelling, blisters, fever, headaches.
   - First Aid: Take a shower, using soap, to remove oils that may block pores, preventing the body from cooling naturally. If blisters occur, apply dry, sterile dressings and get medical attention.
2. Heat cramps
   - Symptoms: Painful spasms, usually in leg and abdominal muscles, heavy sweating.
   - First Aid: Get the victim to a cooler location. Lightly stretch and gently massage affected muscles to relieve spasm. Give sips of up to a half glass of cool water every 15 minutes. Do not give liquids with caffeine or alcohol. If nauseous, discontinue liquids.
3. Heat exhaustion
   - Symptoms: Heavy sweating and skin may be cool, pale or flushed. Weak pulse. Normal body temperature is possible but temperature will likely rise. Fainting or dizziness, nausea or vomiting, exhaustion and headaches are possible.
   - First Aid: Get victim to lie down in a cool place. Loosen or remove clothing. Apply cool, wet cloths. Fan or move victim to air-conditioned place. Give sips of water if victim is conscious. Be sure water is consumed slowly. Give half glass of cool water every 15 minutes. If nausea occurs, discontinue. If vomiting occurs, seek immediate medical attention.
4. Heat stroke (sun stroke)
   - Symptoms: High body temperature (105+); hot, red, dry skin; rapid, weak pulse; and rapid, shallow breathing. Possible unconsciousness. Victim will likely not sweat unless victim was sweating from recent strenuous activity.
   - First Aid: Heat stroke is a severe medical emergency. Call 911 or emergency medical services or get the victim to a hospital immediately. Delay can be fatal. Move victim to a cooler environment. Remove clothing. Try a cool bath, sponging or wet sheet to reduce body temperature. Watch for breathing problems. Use extreme caution. Use fans and air conditioners.

CHECKLIST #13

WATER CONSERVATION CHECKLIST

Conserving water is very important during emergency water shortages. Water saved by one user may be enough to protect the critical needs of others. Irrigation practices can be changed to use less water or crops that use less water can be planted. Cities and towns can ration water, factories can change manufacturing methods, and individuals can practice water-saving measures to reduce consumption. If everyone reduces water use during a drought, more water will be available to share.

1. Practice indoor water conservation:

General

- Never pour water down the drain when there may be another use for it; i.e., water your indoor plants
- Repair dripping faucets by replacing washers. One drop per second wastes 2,700 gallons of water per year!

Bathroom

- Check all plumbing for leaks. Have leaks repaired by a plumber.
- Install a toilet displacement device to cut down on the amount of water needed to flush. Place a one-gallon plastic jug of water into the tank to displace toilet flow (a brick may dissolve and loose pieces may cause damage to the internal parts). Be sure installation does not interfere with the operation.
- Consider purchasing a low-volume toilet that uses less than half the water of older models. NOTE: In many areas, low-volume units are required by law.
- Replace your showerhead with an ultra-low-flow version.
- Do not take baths – take short showers. Turn on the water only to get wet and lather and then again to rinse off.
- Place a bucket in the shower to catch excess water for watering plants.
- Don't let the water run while brushing your teeth, washing your face or shaving.
- Don't flush the toilet unnecessarily. Dispose of tissues, insects, and other similar waste in the trash rather than the toilet.

Kitchen

- Operate automatic dishwashers only when they are fully loaded. Use the "light wash" feature if available to use less water.
- Hand wash dishes by filling two containers—one with soapy water and the other with rinse water containing a small amount of chlorine bleach.
- Most dishwashers can clean soiled dishes very well, so dishes do not have to be rinsed before washing. Just remove large particles of food, and put the soiled dishes in the dishwasher.
- Store drinking water in the refrigerator. Don't let the tap run while you are waiting for water to cool.
- Do not waste water waiting for it to get hot. Capture it for other uses such as plant watering or heat it on the stove or in a microwave.
- Do not use running water to thaw meat or other frozen foods. Defrost food overnight in the refrigerator, or use the defrost setting on your microwave.
- Clean vegetables in a pan filled with water rather than running water from the tap.
- Kitchen sink disposals require a lot of water to operate properly. Start a compost pile as an alternate method of disposing of food waste, or simply dispose of food in the garbage.

Laundry

- Operate automatic clothes washers only when they are fully loaded or set the water level for the size of your load.

Long-term indoor water conservation

- Retrofit all household faucets by installing aerators with flow restrictors.

- Consider installing an instant hot water heater on your sink.
- Insulate your water pipes to reduce heat loss and prevent them from breaking if you have a sudden and unexpected spell of freezing weather.
- If you are considering installing a new heat pump or air-conditioning system, the new air-to-air models are just as efficient as the water-to-air type and do not waste water.
- Install a water-softening system only when the minerals in the water would damage your pipes. Turn the softener off while on vacation.
- When purchasing a new appliance, choose one that is more energy and water efficient.

2. Practice outdoor water conservation:

General

- If you have a well at home, check your pump periodically. If the automatic pump turns on and off while water is not being used, you have a leak.

Car washing

- Use a shut-off nozzle on your hose that can be adjusted down to a fine spray, so that water flows only as needed.
- Consider using a commercial car wash that recycles water. If you wash your own car, park on the grass so that you will be watering it at the same time.

Lawn Care

- Don't over water your lawn. A heavy rain eliminates the need for watering for up to two weeks. Most of the year, lawns only need one inch of water per week.
- Position sprinklers so water lands on the lawn and shrubs and not on paved areas.
- Avoid sprinklers that spray a fine mist. Mist can evaporate before it reaches the lawn. Check sprinkler systems and timing devices regularly to be sure they operate properly.
- Raise the lawn mower blade to its highest level. A higher cut encourages grass roots to grow deeper, shades the root system, and holds soil moisture.
- Plant drought-resistant lawn seed.
- Avoid over-fertilizing your lawn.
- Use a broom or blower instead of a hose to clean leaves, et.c. from your driveway or sidewalk.
- Do not leave sprinklers or hoses unattended. A garden hose can pour out 600 gallons or more in only a few hours.

Pool

- Consider installing a new water-saving pool filter. A single back flushing with a traditional filter uses 180 to 250 gallons of water.
- Cover pools and spas to reduce evaporation of water.

Long term outdoor conservation

- Plant native and/or drought-tolerant grasses, ground covers, shrubs and trees. Once established, they do not need water as frequently and usually will survive a dry period without watering. Small plants require less water to become established. Group plants together based on similar water needs.
- Install irrigation devices that are the most water efficient for each use. Micro and drip irrigation and soaker hoses are examples of efficient devices.
- Use mulch to retain moisture in the soil and control weeds that compete for water.
- Avoid purchasing recreational water toys that require a constant stream of water.
- Avoid installing ornamental water features (such as fountains) unless they use recycled water.

Participate in public water conservation programs of your local government, utility or water management district. Follow water conservation and water shortage rules in effect. Remember, you are included in the restrictions even if your water comes from a private well. Be sure to support community efforts that help develop and promote a water conservation ethic.

CHECKLIST #14

WINTER STORM SAFETY CHECKLIST

Preparedness is key to protecting your business, customers and employees. Again, be prepared to evacuate if flooding is imminent and advised by local officials and prepare a disaster supplies kit for your facility and call-down procedures for communicating with employees.

- ❑ If you are vulnerable to flooding, consider acquiring sandbags or other materials to slow seepage into your building. Investigate other methods to reduce your risk of flooding including floodproofing, elevation or relocation.
- ❑ Have a plan to protect your records, equipment and files. Move valuable objects higher. Place them on shelves, tables and counter tops.
- ❑ Fuel your vehicle(s) and check oil and water.
- ❑ If there is sufficient time, take the server or backup tapes (in fire-proof container) to safer location.
- ❑ Confirm the Emergency Communications Plan (call-down procedures, emergency contact).
- ❑ Secure your facility. Back up data files and take server(s) to more secure site. Unplug appliances. Protect equipment.
- ❑ Turn off the main water valve and electricity, if instructed to do so. Close and lock doors and windows.
- ❑ Leave early enough to (1) allow employees to secure their homes and purchase any needed emergency supplies, if appropriate, and (2) avoid being trapped by severe weather, other evacuation traffic, emergency response, etc.
- ❑ Follow recommended evacuation routes. Be alert.

CHECKLIST #15

STEPS TO PROTECT YOUR FARM FROM PEST AND DISEASE

- ❑ Talk seriously with your local police, fire and emergency departments. Get to know them and let them know that you are making security a priority at your facility and will report any suspicious activities.
- ❑ Make sure the appropriate public authorities have copies of maps of your facilities that indicate service shut-off locations, security areas and any other areas of sensitivity or vulnerability.
- ❑ Evaluate every request for information about your operation. Never agree to an unusual request unless you have verified its validity. Whenever possible, require requests for sensitive information or tours to be in writing. Obtain as much information as possible—name, telephone number, address, reason for request, what the person will be doing with the information, who else has been contacted, etc. If anyone hesitates to cooperate with these requests, do not reveal information about or provide access to your operation.
- ❑ Ask for references. Make calls to verify that the person requesting any sensitive information is who he or she claims to be, especially if the person claims to be a reporter.
- ❑ Ensure that access to your facility is controlled. Establish check-in procedures for visitors. Require visitors to sign in and out upon entering and leaving the facility. Use visitor identification badges. This protects your visitor as well as you and your operation.
- ❑ Escort visitors at all times while they are on the premises. Employees should be instructed to report all unescorted visitors to the appropriate management and security personnel immediately.
- ❑ Maintain basic security by locking office doors and file cabinets. Have firewalls installed on your computer systems. Maintain separate business and personal computers. Keep all animal health products under lock and key. Use security lighting and alarms. Maintain fencing and gates. Post signs indicating restricted areas and no trespassing.
- ❑ Thoroughly screen all job applicants. Take the time to check all references. Double check anyone who shows a university or college identification card. Any hesitation by the prospective employee should exclude him or her from further consideration.
- ❑ Watch for unusual behavior by new employees. Pay attention to workers who stay unusually late, arrive unusually early, or access files, information, or other areas of the facility outside their responsibility. Do not allow workers to remove documents from the site. Be suspicious of employees who ask questions on sensitive subjects or bring cameras or video equipment onsite. Watch for workers who are standoffish. Note the mode of dress (e.g., absence of leather or other animal products).
- ❑ Tell all workers at hiring that unannounced locker checks are part of your routine security maintenance operation and that your operation will report and file charges against any employee who breaks the law.
- ❑ Inform employees in vulnerable areas that unauthorized surveillance or infiltration is a possibility. Any suspicious activity should be reported to supervisors or the appropriate security person immediately.
- ❑ Watch for warning signs that your operation may be a target. Such signs can include an increase in requests for animal-specific information or on-farm tours, calls and letters questioning or criticizing your business or particular practices, any harassing calls and letters to you or a nearby operation, increase in media attention to issues relating to the livestock industry, special interest group campaigns locally, and unusual interest in gaining employment.
- ❑ Develop a company statement concerning care, treatment and nutrition for your animals. Designate a single spokesperson to handle all calls about animal care, animal rights or any company policy concerning animals.
- ❑ Conduct routine tests of your security system and, if necessary, mock drills on your response procedures.
- ❑ Develop a crisis communication and action plan. Establish policies and procedures for handling disruptive and illegal situations, as well as for handling adverse publicity that might result. In developing response procedures, remember that steps to protect people should take priority over steps to protect property.

Source: American Farm Bureau. "Steps to Protect Your Farm from Terrorism," *The Voice of Agriculture Newsroom*, October 22, 2001. Accessed at www.fb.org/news/fbn/html/agriculturalterrorism.html.

CHECKLIST #16

WHAT TO DO DURING AND AFTER A HAZARDOUS MATERIAL INCIDENT

IF YOU'RE TOLD TO EVACUATE

- ❑ You should move to the place/shelter designated by public officials. Listen to your radio and TV for specific instructions.
- ❑ Stay as calm as you can. If you already know where to go and what to take, that will help.
- ❑ Quickly gather what you will need, unless you are told to leave immediately.
- ❑ Turn off lights, heating, cooling, and ventilation systems and lock your building.
- ❑ Carpool if possible.
- ❑ Keep car windows/air vents closed. Do not use the air conditioner until you are out of the evacuation area.
- ❑ Drive safely. Law enforcement officers will help with traffic control.
- ❑ Do not worry about your property while you are away. The area will be secured.

IF YOU ARE TOLD TO STAY INDOORS AND SHELTER-IN-PLACE

Stay inside the facility. This action will be recommended if there is a short release, a small amount of hazardous material in the air, or if time does not permit evacuation before the arrival of a cloud of toxic vapor. Take these steps to protect yourself and employees:

- ❑ Stay inside until local officials say you can leave safely. This will most likely be for no more than a few hours.
- ❑ If your business has animals, if possible bring them indoors!
- ❑ Close all doors and windows.
- ❑ Seal all gaps under doorways and windows with damp towels and duct tape.
- ❑ Turn off heating, cooling or ventilation systems.
- ❑ Listen to your local radio or TV stations for further instructions.
- ❑ Resist the impulse to go outdoors and "check things out" before given the "All Clear" by authorities.
- ❑ If you are told to protect your breathing, cover your nose and mouth with a damp handkerchief or other cloth folded over several times.

YOUR CHILDREN

Employees will be concerned for their children. Reassure them that if children are in school at the time the evacuation is ordered, school officials will take care of them. If students have to leave their schools for a safer shelter, they will be the first to move.

Parents should not try to call or go to the children's school to pick them up - that could delay their evacuation to a safer area. Teachers and other adults will take them to a designated place or shelter. In some cases, the school may not be at risk to the chemical release. Either way, you and your employees will be told by local officials through radio and TV where to pick up the children after they have been evacuated.

WHEN YOU RETURN TO YOUR BUSINESS, WHAT PRECAUTIONS SHOULD YOU TAKE?

Officials will notify you what precautions need to be taken. Depending of the type of chemical, you may need to do the following:

- ❑ Wash all dishes and eating utensils.
- ❑ Dispose of any open food, etc.
- ❑ Vacuum furniture, floors, other items.
- ❑ Change air conditioner filters.
- ❑ Air out files, copy paper, etc.
- ❑ Purify water before using.

CHECKLIST #17

FIRE SAFETY CHECKLIST

When OSHA conducts workplace inspections, it checks to see whether employers are complying with OSHA standards for fire safety:

Employee Training

- ❑ OSHA standards require employers to provide proper exits, fire fighting equipment, emergency plans, and employee training to prevent fire deaths and injuries in the workplace.

Building Fire Exits

- ❑ Each workplace building must have at least two means of escape remote from each other to be used in a fire emergency.
- ❑ Fire doors must not be blocked or locked to prevent emergency use when employees are within the buildings.
- ❑ Delayed opening of fire doors is permitted when an approved alarm system is integrated into the fire door design.
- ❑ Exit routes from buildings must be clear and free of obstructions and properly marked with signs designating exits from the building.

Portable Fire Extinguishers

- ❑ Each workplace building must have a full complement of the proper type of fire extinguisher for the fire hazards present.
- ❑ Employees expected or anticipated to use fire extinguishers must be instructed on the hazards of fighting fire, how to properly operate the fire extinguishers available, and what procedures to follow in alerting others to the fire emergency.
- ❑ Only approved fire extinguishers are permitted to be used in workplaces, and they must be kept in good operating condition. Proper maintenance and inspection of this equipment is required of each employer.
- ❑ Where the employer wishes to evacuate employees instead of having them fight small fires there must be written emergency plans and employee training for proper evacuation.

Emergency Evacuation Planning

- ❑ Each employer needs to have a written emergency action plan for evacuation of employees which describes the routes to use and procedures to be followed by employees. Also, procedures for accounting for all evacuated employees must be part of the plan. The written plan must be available for employee review.
- ❑ Where needed, special procedures for helping physically impaired employees must be addressed in the plan. The plan must also include procedures for those employees who must remain behind temporarily to shut down critical plant equipment before they evacuate.
- ❑ The preferred means of alerting employees to a fire emergency must be part of the plan and an employee alarm system must be available throughout the workplace complex and must be used for emergency alerting for evacuation. The alarm system may be voice communication or sound signals such as bells, whistles or horns. Employees must know the evacuation signal.
- ❑ Training of all employees in what is to be done in an emergency is required. Employers must review the plan with newly assigned employees so they know correct actions in an emergency and with all employees when the plan is changed.

Fire Prevention Plan

- ❑ Employers need to implement a written fire prevention plan to complement the fire evacuation plan to minimize the frequency of evacuation. Stopping unwanted fires from occurring is the most efficient way to handle them. The written plan shall be available for employee review.
- ❑ Housekeeping procedures for storage and cleanup of flammable materials and flammable waste must be included in the plan. Recycling of flammable waste such as paper is encouraged; however, handling and packaging procedures must be included in the plan.

- Procedures for controlling workplace ignition sources such as smoking, welding and burning must be addressed in the plan. Heat producing equipment such as burners, heat exchangers, boilers, ovens, stoves, fryers, etc., must be properly maintained and kept clean of accumulations of flammable residues; flammables are not to be stored close to these pieces of equipment.
- All employees are to be apprised of the potential fire hazards of their job and the procedures called for in the employer's fire prevention plan. The plan shall be reviewed with all new employees when they begin their job and with all employees when the plan is changed.

Fire Suppression System

- Properly designed and installed fixed fire suppression systems enhance fire safety in the workplace. Automatic sprinkler systems throughout the workplace are among the most reliable fire fighting means. The fire sprinkler system detects the fire, sounds an alarm and puts the water where the fire and heat are located.
- Automatic fire suppression systems require proper maintenance to keep them in serviceable condition. When it is necessary to take a fire suppression system out of service while business continues, the employer must temporarily substitute a fire watch of trained employees standing by to respond quickly to any fire emergency in the normally protected area. The fire watch must interface with the employers' fire prevention plan and emergency action plan.
- Signs must be posted about areas protected by total flooding fire suppression systems which use agents that are a serious health hazard such as carbon dioxide, Halon 1211, etc. Such automatic systems must be equipped with area pre-discharge alarm systems to warn employees of the impending discharge of the system and allow time to evacuate the area. There must be an emergency action plan to provide for the safe evacuation of employees from within the protected area. Such plans are to be part of the overall evacuation plan for the workplace facility.

This is one of a series of fact sheets highlighting U.S. Department of Labor programs. It is intended as a general description only and does not carry the force of legal opinion. This information will be made available to sensory impaired individuals upon request. Voice phone: (202) 523-8151. TDD message referral phone: 1-800-326-2577.

CHECKLIST #18

TIPS FOR FIRE PREVENTION FOR SMALL BUSINESS

By Captain Bud Gundersen

These few simple precautions can go a long way toward preventing a fire from destroying your business:

FIRE EXTINGUISHERS

- ❑ Every business location is required to have at least one extinguisher. Required extinguishers must be serviced yearly, or immediately after use, by a person having a valid certificate. Extinguishers must be installed on approved brackets or set in a fire department approved cabinet. They must be conspicuously located or have signs which identify the location. Please contact your local fire station if you have any questions regarding the size, type, or placement of extinguishers.

A FEW MORE TIPS…

Water Heaters: The burner flame can easily start a fire if flammable items are placed too close. Maintain at least three feet of clearance around your hot water heater.

Electrical Panels: In the event of a fire, three feet of clearance around the electrical panel is necessary to access circuit breakers.

Exit Aisles: Must be clear of storage at all times.

Fire Control Valves: Often located in obscure areas of buildings, fire control valves can get blocked by storage. Maintain a three-foot access aisle and make sure that the valves are well marked.

ELECTRICAL HAZARDS

- ❑ Extension cords are often misused and can be very hazardous. They should be used only for temporary wiring, not permanent use. They should not be run through ceilings, walls, doors or windows. Also, beware of the extension cord "octopus." Using multiple outlet adapters to run numerous items off a single outlet can be dangerous. It is much safer to install additional outlets rather than to use adapters and extension cords.

EXIT DOORS

- ❑ For security purposes many business owners lock rear exit doors. Even in a small shop, someone can be trapped by a fire and need to rely on the rear door to escape. All required exit doors must be unlocked during business hours or have escape hardware which allows them to be opened from the inside without a key. This is a crucial issue to life safety. Both security and fire safety can be accommodated by installing escape hardware or a door alarm.

ADDRESS NUMBERS

- ❑ Make sure your address is clearly visible from the street. If you have a fire or medical emergency, the fire department wants to find you fast. It is also very helpful if someone can wait for them out on the street and flag them in.

DATA BACK-UP

- ❑ While protecting your employees will always be your first priority, mitigation of business loss will include more than fire extinguishers, sprinkler systems and quick fire response. Your business needs to protect its records and data files. Our reliance on electronic data makes data protection a major concern for your business survival. Even in small businesses, it is crucial to back-up your data files at least once a week.

FIRE-PROOF SAFES

- ❑ Keep a copy of your electronic files and critical data/ information in a fire-resistant safe. If you are in a hurricane evacuation zone, flood zone or vulnerable to other areas, then an alternate site (outside of the vulnerability zone) should be selected and a fire-resistant safe kept there for keeping records during a potential evacuation.

CHECKLIST #19

POWER SERVICE DISRUPTION CHECKLIST

Power Service Disruption could be the result of a weather event, an accident or a terrorist attack. There are some physical measures a business can take to be prepared for Power Service Disruptions. (i.e., surge protectors or backup generation for critical equipment). As in the case of any other emergency, the business needs to address liabilities, risks and response activities in advance. An emergency plan can include some of the following measures.

Facility

- ❑ If your lights fail, first try checking your breakers or fuses. Re-setting the breakers or putting in new fuses may bring your lights back on. To reset a breaker, turn it to the OFF position, press firmly off, then push to the ON position. If re-setting the breaker or replacing the fuses doesn't help, call your local electric utility.
- ❑ Post phone number for local electric utility at appropriate locations.
- ❑ If using back-up generation, what are your procedures to avoid a backfeed?

Medical Emergency

In the case of a medical emergency during a power outage, employees should seek immediate care at the nearest appropriate health care facility. Note that some telephones require electricity and may not be in service during an outage. Businesses are encouraged to have a back-up communication plan in case of such an event. When requesting emergency assistance, location finding devices such as GPS can be very useful during an event that changes the landscape.

Facility Protection and Security

- ❑ Even if people do not know whether radioactive materials were present, following these simple steps can help reduce their injury from other chemicals that might have been present in the blast.
- ❑ Determine your threat level and communicate to employees.
- ❑ Employers are encouraged to develop a business security plan. Included in this plan should be security processes dealing with power outages/disruptions. Need for security guards because your alarm system is not functioning?
- ❑ Be on the alert for fires and call authorities if smoke or fire is spotted.
- ❑ What to do if you have another emergency during the outage (e.g., material spill).
- ❑ What to do if water enters your facility. What equipment could you use when the lights come back on?
- ❑ Procedure for re-entering the building.
- ❑ Employee Field Work.
- ❑ Inform personnel that any fallen wire is potentially hazardous. (See Stay Safe this Storm Season pamphlet.)
- ❑ Inform personnel how to deal with a fallen power line on their car.

Communications

- ❑ Inform the employees how they will be communicating with their immediate supervisor or employer if they are in the field during a large scale power outage.
- ❑ Publish a telephone number to be used by employees to call their supervisor and be prepared to provide reporting instructions.
- ❑ Make appropriate communication to your customers.

CHECKLIST #20

BOMB THREAT PROCEDURES

- ❑ If you receive a bomb threat by phone, instruct employee(s) to get as much information from the caller as possible. Keep the caller on the line and record everything that is said.
- ❑ If you are notified of a bomb threat referring to a delivered package, do not touch any suspicious packages. Clear the area around the suspicious packages and notify the police immediately.
- ❑ At the same time, the emergency warning procedure should be implemented, so others can notify law enforcement, building management and staff.
- ❑ Initiate shutdown and emergency evacuation procedures.
- ❑ At meeting place, verify the evacuation of all employees and visitors.

BOMB THREAT

KEEP THE CALLER ON THE LINE AS LONG AS POSSIBLE!

EXACT TIME AND DATE OF CALL: _____

EXACT WORDS OF CALLER: _____

Voice

- ❑ Loud
- ❑ High Pitched
- ❑ Raspy
- ❑ Intoxicated
- ❑ Soft
- ❑ Deep
- ❑ Pleasant
- ❑ Other

Language

- ❑ Excellent
- ❑ Fair
- ❑ Foul
- ❑ Good
- ❑ Poor
- ❑ Other

Accent

- ❑ Local
- ❑ Foreign
- ❑ Race
- ❑ Not Local
- ❑ Region

Speech

- ❑ Fast
- ❑ Distinct
- ❑ Stutter
- ❑ Slurred
- ❑ Slow
- ❑ Distorted
- ❑ Nasal
- ❑ Lisp
- ❑ Other

Manner

- ❑ Calm
- ❑ Rational
- ❑ Coherent
- ❑ Deliberate
- ❑ Righteous
- ❑ Angry
- ❑ Irrational
- ❑ Incoherent
- ❑ Emotional
- ❑ Laughing

Familiarity With Facility?

- ❑ Much
- ❑ Some
- ❑ None

Background Noise

- ❑ Factory Machines
- ❑ Bedlam
- ❑ Music
- ❑ Office Machines
- ❑ Mixed
- ❑ Street Traffic
- ❑ Trains
- ❑ Animals
- ❑ Quiet
- ❑ Voices
- ❑ Airplanes
- ❑ Party Atmosphere

Questions to Ask the Caller

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 did you place the bomb? _____
8. Where are you calling from? _____
9. What is your address? _____
10. What is your name? _____

DIAL 911 IMMEDIATELY AND REPORT THREAT

CHECKLIST #21

CYBER SECURITY THREAT ASSESSMENT

SECURITY CHECKLIST	Yes	No
PHYSICAL SECURITY		
1. Is your computing area and equipment physically secured?		
2. Are there procedures in place to prevent terminals from being left in a logged-on state, however briefly?		
3. Are screens automatically locked after 10 minutes idle?		
4. Are modems set to Auto-Answer OFF (not to accept incoming calls)?		
5. Are your PCs inaccessible to unauthorized users (e.g., located away from public areas)?		
6. Does your staff wear ID badges?		
7. Do you check the credentials of external contractors?		
8. Do you have procedures for protecting data during equipment repairs?		
9. Is waste paper binned or shredded?		
10. Do you have procedures for disposing of waste material?		
11. Do your policies for disposing of old computer equipment protect against loss of data (e.g., by reading old disks and hard drives)?		
12. Do you have policies covering laptop security (e.g., cable lock or secure storage)?		
ACCOUNT AND PASSWORD MANAGEMENT		
13. Do you ensure that only authorized personnel have access to your computers?		
14. Do you require and enforce appropriate passwords?		
15. Are your passwords secure (not easy to guess, regularly changed, no use of temporary or default passwords)?		
16. Are your computers set up so that staff entering passwords cannot be viewed by others?		
CONFIDENTIALITY OF SENSITIVE DATA		
17. Are you exercising responsibility to protect sensitive data under your control?		
18. Is your most valuable or sensitive data encrypted?		
DISASTER RECOVERY		
19. Do you have a current business continuity plan?		
SECURITY AWARENESS AND EDUCATION		
20. Are you providing information about computer security to your staff?		
21. Are employees taught to be alert to possible security breaches?		

CHECKLIST #22

CYBER SECURITY CHECKLIST

IMPACT SCALE	LIKELIHOOD SCALE
0 Impact is negligible	**0 Unlikely to occur**
1 Effect is minor; major agency operations are not affected.	**1 Likely to occur less than once per year**
2 Agency operations are unavailable for a certain amount of time, costs are incurred, public/customer confidence is minimally affected.	**2 Likely to occur once per year**
3 Significant loss of operations; significant impact on public/customer confidence.	**3 Likely to occur once per month**
4 Effect is disastrous; systems are down for an extended period of time; systems need to be rebuilt and data replaced.	**4 Likely to occur once per week**
5 Effect is catastrophic; critical systems are offline for an extended period; data are lost, irreparably corrupted; public health and safety are affected.	**5 Likely to occur daily**

THREATS	IMPACT (0-5)	LIKELIHOOD (0-5)	TOTAL (IMPACT X LIKELIHOOD)
GENERAL THREATS			
Human error: 1. Accidental destruction, modification, disclosure, or incorrect classification of information.			
2. Ignorance: Inadequate security awareness, lack of security guidelines, lack of proper documentation, lack of knowledge.			
3. Workload: Too many or too few system administrators; highly pressured users.			
4. Users may inadvertently give information on security weaknesses to attackers.			
5. Incorrect system configuration.			
6. Security policy not adequate or not enforced.			
SABOTAGE			
1. Dishonesty: Fraud, theft, embezzlement, selling of confidential agency information.			
2. Attacks by "social engineering": • Attackers may use telephone to impersonate employees to persuade users/administrators to give username/passwords/ modem numbers, etc. • Attackers may persuade users to execute Trojan horse programs.			
3. Abuse of privileges/trust.			
4. Unauthorized use of "open" terminals/PCs.			
5. Mixing of test and production data or environments.			
6. Introduction of unauthorized software or hardware.			
7. Time bombs: Software programmed to damage a system on a certain date.			

THREATS	IMPACT (0-5)	LIKELIHOOD (0-5)	TOTAL (IMPACT X LIKELIHOOD)
8. Operating system design errors: Certain systems were not designed to be highly secure.			
9. Protocol design errors: Certain protocols were not designed to be highly secure. Protocol weaknesses in TCP/IP can result in: • Source routing, DNS spoofing, TCP sequence guessing, unauthorized access. • Hijacked sessions and authentication session/transaction replay; data is changed or copied during transmission. • Denial of service, due to ICMP bombing, TCP_SYN flooding, large PING packets, etc.			
10. Logic bomb: Software programmed to damage a system under certain conditions.			
11. Viruses in programs, documents, e-mail attachments.			
IDENTIFICATION/AUTHORIZATION THREATS			
1. Attack programs masquerading as normal programs (Trojan horses).			
2. Attack hardware masquerading as normal commercial hardware.			
3. External attackers masquerading as valid users or customers.			
4. Internal attackers masquerading as valid users or customers.			
5. Attackers masquerading as helpdesk/support personnel.			
RELIABILITY OF SERVICE THREATS			
1. Major natural disasters: fire, smoke, water, earthquake, storms/ hurricanes/tornadoes, power cuts, etc.			
2. Minor natural disasters, of short duration, or causing little damage.			
3. Major human-caused disasters: war, terrorist incidents, bombs, civil disturbance, dangerous chemicals, radiological accidents, etc.			
4. Equipment failure from defective hardware, cabling, or communications system.			
5. Equipment failure from airborne dust, electromagnetic interference, or static electricity.			
6. Denial of service: • Network abuse: Misuse of routing protocols to confuse and mislead systems. • Server overloading (processes, swap space, memory, "tmp" directories, overloading services). • E-mail bombing. • Downloading or receipt of malicious Applets, ActiveX controls, macros, Postcript files, etc.			

THREATS	IMPACT (0-5)	LIKELIHOOD (0-5)	TOTAL (IMPACT X LIKELIHOOD)
7. Sabotage: Malicious, deliberate damage of information or information processing functions. • Physical destruction of network interface devices, cables. • Physical destruction of computing devices or media. • Destruction of electronic devices and media by electromagnetic radiation weapons (HERF Gun, EMP/T Gun). • Theft. • Deliberate electrical overloads or shutting off electrical power. • Viruses and/or worms. • Deletion of critical system files.			
PRIVACY THREATS			
1. Eavesdropping: • Electromagnetic eavesdropping/Van Eck radiation. • Telephone/fax eavesdropping (via "clip-on," telephone bugs, inductive sensors, or hacking the public telephone exchanges. • Network eavesdropping: Unauthorized monitoring of sensitive data crossing the internal network, unknown to the data owner. • Network eavesdropping: Unauthorized monitoring of sensitive data crossing the Internet, unknown to the data owner. • Subversion of DNS to redirect e-mail or other traffic. • Subversion of routing protocols to redirect e-mail or other traffic. • Radio signal eavesdropping. • Rubbish eavesdropping (analyzing waste for confidential documents, etc.).			
INTEGRITY/ACCURACY THREATS			
1. Malicious, deliberate damage of information or information processing functions from external sources.			
2. Malicious, deliberate damage of information or information processing functions from internal sources.			
3. Deliberate modification of information.			
ACCESS CONTROL THREATS			
1. Password cracking (access to password files, use of bad (blank, default, rarely changed) passwords).			
2. External access to password files, and sniffing of the network.			
3. Attack programs allowing external access to systems (back doors visible to external networks).			
4. Attack programs allowing internal access to systems (back doors visible to internal networks).			
5. Unsecured maintenance modes, developer backdoors.			
6. Modems easily connected, allowing uncontrollable extension of the internal network.			
7. Bugs in network software which can open unknown/ unexpected security holes. (Holes can be exploited from external networks to gain access. This threat grows as software becomes increasingly complex.)			
8. Unauthorized physical access to system.			

THREATS	IMPACT (0-5)	LIKELIHOOD (0-5)	TOTAL (IMPACT X LIKELIHOOD)
REPUDIATION THREATS			
1. Receivers of confidential information may refuse to acknowledge receipt.			
2. Senders of confidential information may refuse to acknowledge source.			
LEGAL THREATS			
1. Failure to comply with regulatory or legal requirements (e.g., to protect confidentiality of employee data).			
2. Liability for acts of internal users or attackers who abuse the system to perpetrate unlawful acts (e.g., incitement to racism, gambling, money laundering, distribution of pornographic or violent material).			
3. Liability for damages if an internal user attacks other sites.			

CHECKLIST #23

CHECKLIST TO PREPARE AND RESPOND TO A CHEMICAL/BIOLOGICAL ATTACK

Assemble a disaster supply kit (see the "Emergency Planning and Disaster Supplies" chapter for more information) and be sure to include:

- ❑ Battery-powered commercial radio with extra batteries.
- ❑ Non-perishable food and drinking water.
- ❑ Roll of duct tape and scissors.
- ❑ Plastic for doors, windows and vents for the room in which you will shelter in place—this should be an internal room where you can block out air that may contain hazardous chemical or biological agents. To save critical time during an emergency, sheeting should be pre-measured and cut for each opening.
- ❑ First aid kit.
- ❑ Sanitation supplies including soap, water and bleach.

What to do During a Chemical or Biological Attack:

- ❑ Listen to your radio for instructions from authorities such as whether to remain inside or to evacuate.

If you are instructed to remain in your home, the building where you are, or other shelter during a chemical or biological attack:

- ❑ Turn off all ventilation, including furnaces, air conditioners, vents and fans.
- ❑ Seek shelter in an internal room, preferably one without windows. Seal the room with duct tape and plastic sheeting. Ten square feet of floor space per person will provide sufficient air to prevent carbon dioxide build-up for up to five hours. (See "Shelter-in-Place" Checklist)
- ❑ Remain in protected areas where toxic vapors are reduced or eliminated and be sure to take your battery-operated radio with you.

If you are caught in an unprotected area, you should:

- ❑ Attempt to get up-wind of the contaminated area.
- ❑ Attempt to find shelter as quickly as possible.
- ❑ Listen to your radio for official instructions.

What to do after a chemical attack:

Immediate symptoms of exposure to chemical agents may include blurred vision, eye irritation, difficulty breathing and nausea. A person affected by a chemical or biological agent requires immediate attention by professional medical personnel. If medical help is not immediately available, decontaminate yourself and assist in decontaminating others. Decontamination is needed within minutes of exposure to minimize health consequences. (However, you should not leave the safety of a shelter to go outdoors to help others until authorities announce it is safe to do so.)

Use extreme caution when helping others who have been exposed to chemical agents:

- ❑ Remove all clothing and other items in contact with the body. Contaminated clothing normally removed over the head should be cut off to avoid contact with the eyes, nose, and mouth. Put into a plastic bag if possible. Decontaminate hands using soap and water. Remove eyeglasses or contact lenses. Put glasses in a pan of household bleach to decontaminate.
- ❑ Remove all items in contact with the body.
- ❑ Flush eyes with lots of water.
- ❑ Gently wash face and hair with soap and water; then thoroughly rinse with water.

- ❑ Decontaminate other body areas likely to have been contaminated. Blot (do not swab or scrape) with a cloth soaked in soapy water and rinse with clear water.
- ❑ Change into uncontaminated clothes. Clothing stored in drawers or closets is likely to be uncontaminated.
- ❑ If possible, proceed to a medical facility for screening.

What to do after a biological attack

In many biological attacks people will not know they have been exposed to an agent. In such situations the first evidence of an attack may be when you notice symptoms of the disease caused by an agent exposure and you should seek immediate medical attention for treatment.

In some situations, like the anthrax letters sent in 2001, people may be alerted to a potential exposure. If this is the case, pay close attention to all official warnings and instructions on how to proceed. The delivery of medical services for a biological event may be handled differently to respond to increased demand. Again, it will be important for you to pay attention to official instructions via radio, television, and emergency alert systems.

If your skin or clothing comes in contact with a visible, potentially infectious substance, you should remove and bag your clothes and personal items and wash yourself with warm soapy water immediately. Put on clean clothes and seek medical assistance.

For more information, visit the website for the Centers for Disease Control and Prevention, www.bt.cdc.gov.

CHECKLIST #24

HANDLING SUSPICIOUS PARCELS OR LETTERS

Be wary of suspicious packages and letters. They can contain explosives, chemical or biological agents. Be particularly cautious at your place of employment. Some typical characteristics postal inspectors have detected over the years, which ought to trigger suspicion, include parcels that:

- ❑ Are unexpected or from someone unfamiliar to you.
- ❑ Have no return address, or have one that can't be verified as legitimate.
- ❑ Are marked with restrictive endorsements, such as "Personal," "Confidential" or "Do not x-ray."
- ❑ Have protruding wires or aluminum foil, strange odors or stains.
- ❑ Show a city or state in the postmark that doesn't match the return address.
- ❑ Are of unusual weight, given their size, or are lopsided or oddly shaped.
- ❑ Are marked with threatening language or have inappropriate or unusual labeling.
- ❑ Have excessive postage or excessive packaging material such as masking tape and string.
- ❑ Have misspellings of common words.
- ❑ Are addressed to someone no longer with your organization or are otherwise outdated.
- ❑ Have incorrect titles or a title without a name.
- ❑ Are not addressed to a specific person.
- ❑ Have handwritten or poorly typed addresses.

With suspicious envelopes and packages other than those that might contain explosives, take these additional steps against possible biological and chemical agents:

- ❑ Refrain from eating or drinking in a designated mail handling area.
- ❑ Place suspicious envelopes or packages in a plastic bag or some other type of container to prevent leakage of contents. Never sniff or smell suspect mail.
- ❑ If you do not have a container, then cover the envelope or package with anything available (e.g., clothing, paper, trash can, etc.) and do not remove the cover.
- ❑ Leave the room and close the door, or section off the area
- ❑ Wash your hands with soapy water to prevent spreading any powder to your face.
- ❑ If you are at work, report the incident to your building security official or an available supervisor, who should notify police and other authorities without delay.
- ❑ List all people who were in the room or area when this suspicious letter or package was recognized. Give a copy of this list to both the local public health authorities and law enforcement officials for follow-up investigations and advice.
- ❑ If you are at home, report the incident to local police.

CHECKLIST #25

RADIOLOGICAL EMERGENCY SAFETY CHECKLIST

Immediate Precautions

- ❑ Notify your Facility Radiation Safety Officer (if applicable), 911, the local authorities and Radiation Control Authority on Accident Conditions. Follow applicable permit and regulatory requirements.
- ❑ Notify 911 of the possible presence of radioactive materials.
- ❑ Isolate hazard area in accordance with your As Low As Reasonably Achievable (ALARA) plan and restrict access.
- ❑ Do Not Touch containers.
- ❑ Upon arrival of Law Enforcement or Fire Department, inform the First Responder that radioactivity may be present.
- ❑ In the case of fire, Do Not attempt to move containers out of fire zone.
- ❑ Retreat to a safe area and wait for Local Authorities. Please note, radioactivity does not change flammability or properties of other materials.
- ❑ In the case of a medical emergency, use First Aid treatment according to the nature of the injury.
- ❑ Advise medical personnel that victim may be contaminated with radioactive material.
- ❑ Detain persons exposed to Radioactive Material until arrival or instruction of Radiation Control Authority. Potential route of exposure can include Inhalation, Ingestion, or Breaks in Skin.
- ❑ Include business specific information in your emergency plans. Inform the employees regarding radiation safety. Follow your ALARA plan. Publish a telephone number to be used by employees to call their supervisor and be prepared to provide reporting instructions.

CHECKLIST #26

RADIOLOGICAL EMERGENCY

Immediate Precautions in the Case of a Terrorist Attack

Radiation cannot be seen, smelled, felt, or tasted by humans. Therefore, if people are present at the scene of an explosion, they will not know whether radioactive materials were involved at the time of the explosion. However, following these simple steps can help reduce their injury from other chemicals that might have been present in the blast.

If people are not too severely injured by the initial blast, they should:

- ❑ Leave the immediate area on foot. Do not panic. Do not take public or private transportation such as buses, subways, or cars because if radioactive materials were involved, they may contaminate cars or the public transportation system.
- ❑ Go inside the nearest building. Staying inside will reduce people's exposure to any radioactive material that may be on dust at the scene.
- ❑ Remove their clothes as soon as possible, place them in a plastic bag, and seal it. Removing clothing will remove most of the contamination caused by external exposure to radioactive materials. Saving the contaminated clothing would allow testing for exposure without invasive sampling.
- ❑ Take a shower or wash themselves as best they can. Washing will reduce the amount of radioactive contamination on the body and will effectively reduce total exposure.
- ❑ Be on the lookout for information. Once emergency personnel can assess the scene and the damage, they will be able to tell people whether radiation was involved.

Note:
There are many questions regarding the likelihood of whether terrorists would use radioactive materials in attacks since radioactive materials are hard to handle and the impact to the public would not be as tangible or visible after an attack. Different methods can be used in a radiological terrorist attack. A weapon could include explosion as a mechanism to disperse radiation as in the case of a dirty bomb or it could be more Apassive@ and include exposing the public to radioactive sources from gauges used in industry or to radioactive waste.

CHECKLIST #27

PREVENTION AND RESPONSE TO WORKPLACE VIOLENCE

- ❑ Establish an atmosphere of awareness and encourage employees to report suspicious activity or behavior, strangers, unexplained events, unscheduled deliveries or suspicious mail.
- ❑ Maintain strict hiring policies that include background checks.
- ❑ Establish written workplace anti-violence policies and security procedures with zero tolerance for any instance of violence.
- ❑ List prohibited conduct.
- ❑ Monitor current employees' behavior.
- ❑ Train managers and supervisors how to recognize and resolve problems.
- ❑ Maintain a working environment that is open to communication and respectful to all employees.
- ❑ Balance a violence-free workplace with employee rights.
- ❑ If you find yourself struggling to wade through these complicated laws, you may want to consult an employment law attorney.
- ❑ Institute appropriate security procedures to prevent attacks on the facility or your employees, by restricting access to your facility and incorporating crime prevention techniques.
- ❑ Establish a procedure to alert management and staff and law enforcement of a potential threat ("panic button," intercom, code word).
- ❑ Ensure all employees understand the Emergency Evacuation Procedures.

CHECKLIST #28

THE EVACUATION "GO BOX"

The "Go Box" contains copies of important documents, equipment and supplies essential for the business to continue to operate. It should be stored in a fire-proof secure container in an alternate location. Below are recommended items; however, each business unit should discuss and specifically designate the contents of their "Go Box."

Recommended "Go Box" contents:

- ❑ Copy of emergency contact list of employees and key customers/clients
- ❑ Copy of insurance policies, agent contact information
- ❑ Copy of listing of emergency vendors (contractors, plumbers, electricians, restoration contractors, mold remediation, etc.)
- ❑ Copy of listing of vendors & suppliers (and alternates) essential for mission critical activities
- ❑ Back up files/ tapes or server(s) of electronic data
- ❑ Copy of essential policies, emergency procedures, Business Continuity Plans
- ❑ General Office supplies plus any special forms, etc. used in your business
- ❑ Other _____
- ❑ Other _____
- ❑ Other _____
- ❑ Other _____
- ❑ Other _____
- ❑ Other _____

Documentation Requirements for a SBA disaster Loan:

- ❑ Corporations/ Partnerships: Copy of 3 years tax returns / 1 year personal tax returns on principles (affiliates with greater than 20% interest) / One year tax returns on affiliated business entity
- ❑ Sole Proprietorships: Copy of 3 years tax returns with Schedule C
- ❑ Copy of Current Profit & Loss Statement (within 90 days)
- ❑ Copy of listing of aged accounts receivables/ payables
- ❑ Copy of listing of inventory
- ❑ Copy of Schedule of Liability
- ❑ Copy of balance sheet (as recent as possible)

CHECKLIST #29

STRATEGIES TO MINIMIZE IMPACT OF WORKPLACE ABSENTEEISM

- ❑ Plan for ill individuals to remain at home. Encourage ill persons to stay home and establish return-to-work policies after illness.
- ❑ Identify critical job functions and plan for their continuity, such as temporarily suspend non-critical activities, cross-train employees to cover critical functions, and cover the most critical functions with fewer staff.
- ❑ Identify employees who might need extra assistance to stay home when they are ill because, for example, they live alone or have a disability.
- ❑ Review Federal and State employment laws that identify your employer obligations and options for employees.
- ❑ Establish and clearly communicate policies on sick (and other) leave and employee compensation.
- ❑ Develop a workplace culture that recognizes and encourages behaviors such as voluntarily staying home when ill in order to recover and to avoid spreading infection to others.
- ❑ Develop policies on what to do when a person becomes ill at the workplace.
- ❑ Provide employees with information on taking care of ill people at home. Such information will be posted on www.pandemicflu.gov.
- ❑ Establish policies for an alternate or flexible worksite (e.g., work via the internet, e-mailed or mailed work assignments) and flexible work hours, where feasible.
- ❑ Develop guidelines to address business continuity requirements created by jobs that will not allow teleworking (e.g., production or assembly line workers).
- ❑ Establish and clearly communicate policies on family leave and employee compensation, especially Federal laws and laws in your State regarding leave of workers who need to care for an ill family member or voluntarily remain home.
- ❑ Plan for dismissal of students and childcare closure.
- ❑ Identify employees who may need to stay home if schools dismiss students and childcare programs close during a severe pandemic.
- ❑ Plan for alternative staffing or staffing schedules on the basis of your identification of employees who may need to stay home.
- ❑ Identify critical job functions and plan now for cross-training employees to cover those functions in case of prolonged absenteeism during a pandemic.
- ❑ Establish policies for employees with children to work from home, if possible, and consider flexible work hours and schedules (e.g., staggered shifts).
- ❑ Encourage employees who have children in their household to make plans to care for their children if officials recommend dismissal of students from schools, colleges, universities, and childcare programs. Advise employees to plan for an extended period (up to 12 weeks) in case the pandemic is severe.
- ❑ In a severe pandemic, parents would be advised to protect their children by reducing out-of-school social contacts and mixing with other children. Although limiting all outside contact may not be feasible, parents may be able to develop support systems with co-workers, friends, families, or neighbors if they continue to need childcare. For example, they could prepare a plan in which two to three families work together to supervise and provide care for a small group of infants and young children while their parents are at work (studies suggest that childcare group size of less than six children may be associated with fewer respiratory infections). Talk with your employees about any benefits, programs, or other assistance they may be eligible for if they have to stay home to mind children for a prolonged period during a pandemic.
- ❑ Coordinate with State and local government and faith-based and community-based organizations to assist workers who cannot report to work for a prolonged period.
- ❑ Plan for workplace and community social distancing measures.
- ❑ Become familiar with social distancing methods that may be used during a pandemic to modify the frequency and type of person-to-person contact (**e.g., reducing hand-shaking, limiting face-to-face meetings and shared workstations, promoting teleworking, offering liberal/unscheduled leave policies, staggered shifts**).
- ❑ Plan to operate businesses and other workplaces using social distancing and other measures to minimize close contact

between and among employees and customers. Determine how the work environment may be reconfigured to allow for more distance between employees and between employees and customers during a pandemic. If social distancing is not feasible in some work settings, employ other protective measures (guidance available at www.pandemicflu.gov).

- ❑ Review and implement guidance from the Occupational Safety and Health Administration (OSHA) to adopt appropriate work practices and precautions to protect employees from occupational exposure to influenza virus during a pandemic. Risk of occupational exposure to influenza virus depends in part on whether or not jobs require close proximity to people potentially infected with the pandemic influenza virus or whether employees are required to have either repeated or extended contact with the public. OSHA will post and periodically update such guidance on www.pandemicflu.gov.
- ❑ Encourage good hygiene at the workplace. Provide employees and staff with information about the importance of hand hygiene (information can be found at www.cdc.gov/cleanhands/) as well as convenient access to soap and water and/or alcohol-based hand gel in your facility. Educate employees about covering their cough to prevent the spread of germs (www.cdc.gov/flu/protect/covercough.htm).
- ❑ Communicate with your employees and staff. Disseminate your company's pandemic plan to all employees and stakeholders in advance of a pandemic; include roles/actions expected of employees and other stakeholders during implementation of the plan.
- ❑ Provide information to encourage employees (and their families) to prepare for a pandemic by providing preparedness information. Resources are available at www.pandemicflu.gov/plan/individual/checklist.html.
- ❑ Help your community. Coordinate your business' pandemic plans and actions with local health and community planning.
- ❑ Find volunteers in your business who want to help people in need, such as elderly neighbors, single parents of small children, or people without the resources to get the medical or other help they will need.
- ❑ Think of ways your business can reach out to other businesses and others in your community to help them plan for a pandemic. Participate in community-wide exercises to enhance pandemic preparedness.
- ❑ Assess criteria that need to be met to resume normal operations and provide notification to employees of activation of the business resumption plan.
- ❑ Assess the availability of medical, mental health, and social services for employees after the pandemic.