



**“The Two P’s of Disaster Planning: When We Cannot Always Prevent,
Then We Always Prepare”**

In the hectic, busy lives that people now lead, it is not likely that disasters can always be “*prevented*”, but the lesson to be learned from recent events during the past several years is that people can be “*prepared*” for unsightly occurrences. Corporations are continually reassessing their incident response preparedness for the purpose of mitigating risks and improving protection of their employees, visitors, customers, assets and facilities. Thus, it is imperative that every company, no matter what size, have in place a plan to respond to a corporate disaster. A corporate disaster is any event which interrupts or threatens the continued viability of a company. It can result in death or significant injuries to employees, customers or the public; shut down your business; disrupt operations; cause physical or environmental damage; or threaten the facility's financial standings or public image. Earthquakes, fires, severe winter storms, floods, hurricanes, volcanic eruptions, hazardous spills, product recalls, financial misconduct and now terrorism, are the most prevalent crises with potential for disaster.

In addition to today's threats of global terrorism targeted towards U.S. enterprises, business leaders must be concerned about the following critical risks:

- ✦ Natural disasters such as earthquakes, hurricanes, floods, and tornadoes, along with other fire disasters, threaten businesses everywhere. It is an amazing statistic that 44% of businesses that lose records in a disaster never resume business; yet the majority of businesses spend less than 3% of their total budget on disaster recovery planning and many do not have an emergency recovery plan.
- ✦ Workplace violence has become an American epidemic since the early 1990's with OSHA now reporting homicide as the second leading cause of fatalities with nearly 1,000 workers murdered and 1.5 million workplace assaults annually.
- ✦ Employee theft and fraud cost U.S. businesses an estimated \$120 billion annually and is a contributing factor in 30% of all business failures.
- ✦ Intellectual property loss and related cyber crimes cost U.S. businesses well over \$100 billion annually according to the White House Office of Science and Technology; and 93% of companies that experience a significant data loss are out of business within five years.

Consequently, business leaders should ask three “*critical interrelated questions*” within their organizations:

- ✦ Do the systems and programs that may have served us well in the past, continue to serve the heightened and complex needs of today?
- ✦ Does our organization have written emergency procedures and protocols in place to appropriately respond to a critical incident or the threat of one?

- ✚ If so, when was the last time that these programs were audited, tested or drilled and then updated based upon the results?

It must be understood that while recent tragedies have shaken Americans' sense of security, the basic principles utilized to secure premises, protect personnel and ensure business continuity remain intact. It simply makes good sense for companies to critically look at existing emergency and disaster management policies and procedures and to measure and adopt best practices proven to have successfully worked in the past.

Emergency and disaster management is the process of identifying, preparing for, mitigating, responding to and recovering from a disaster. It is a dynamic process. Planning, though critical, is not the only component. Training, conducting drills, testing equipment, and coordinating activities within the organization are other important functions.

A successful crisis response and disaster plan insures that responsibilities have been fulfilled for:

- ✚ Protection of employees, environment and assets.
- ✚ Compliance with federal, state and local regulatory requirements.
- ✚ Enhancement of recovery from financial losses, regulatory fines, loss of market share, damages to property or equipment, and business interruption.
- ✚ Reduction of criminal or civil liabilities in the event of an incident.
- ✚ Maintenance of image and credibility amongst employees, customers, suppliers and the general community.

Many in the business community, whether in response to the events of September 11th or to the effects of a natural disaster such as Hurricane Katrina, were struck by the number of businesses that did not have plans in place to respond to a disaster or other crisis. Further, recent catastrophic events like the Virginia Tech shootings have rendered many plans obsolete.

The first step in developing a crisis response plan is to assemble a disaster planning team. The most effective teams draw on all segments of the organization including Financial Officers, Risk Management, Human Resources, Purchasing, Marketing, Legal and Security. This will insure that no crucial areas or issues are overlooked.

Once the team is in place, an analysis of the organization's capabilities to handle crisis and related disasters must be completed. This would include reviews of insurance policies including exclusions and endorsements; evaluations of employee skills already present; customer and supplier relations; back-up systems for computers and alternate computer resources; communications systems available for emergencies; on-site storage of food and supplies; evacuation routes, drills and plans; and staff skills regarding first aid and CPR.

In addition, external resources must be identified including police and fire, emergency storage facilities, medical support and hospitals, and neighboring businesses that would allow the use of its property for gathering areas and assembly following evacuations.

The Plan

A Crisis Response Plan is formulated following a thorough analysis of the potential disaster issues, previously set forth, which may confront a company.

As with any process, this takes time and numerous steps for completion. The plan should include crisis response procedures for every department, designation of crisis response team members, procedures for notifying employees in case of facility closures, priority list of vendors to use in the event of a disaster, and a disaster retrieval system that consists of back-ups for all critical information or reports. This system should be kept off-site, with the off-site location noted in the crisis plan.

The plan should include the following:

- ✚ A written outline for management detailing each person's responsibilities during a crisis
- ✚ A written policy statement detailing procedures to be followed in emergency situations
- ✚ Crisis management training for management and employees
- ✚ Distribution of support documents, such as maps of evacuation routes and "What To Do In Case Of..." manuals and posters to all employees

Cooperation With The Government

Disasters present many problems that most companies cannot respond to without assistance. Accordingly, cooperation with the government is essential. Many areas of the country now have mutual aid pacts, which are agreements between businesses and local government to assist each other by providing materials, equipment and personnel needed to ensure effective disaster control.

In establishing a partnership with government, some critical responsibilities of companies are:

- ✚ All local businesses must be involved in the planning process to gain maximum planning efficiencies.
- ✚ Major companies should demonstrate leadership in plan development and encourage/support suppliers, contractors, and other community businesses.
- ✚ Learn what skills and resources are available in the private sector and determine who the on-site experts are.
- ✚ Progressive private sector leaders will develop detailed plans on who is in charge of a critical incident and who is responsible for coordination with the public sector.
- ✚ In small businesses, the emergency planning process may be the responsibility of the owner or manager who may have limited experience in emergency planning and may need assistance from the public sector or an experienced private sector partner, both during the planning or an actual critical incident.
- ✚ In large businesses, specialized personnel are dedicated to security, fire, or safety and emergency planning, and they will have primary responsibility for response. Other company staff (personnel, medical, public affairs, and

operations managers) may support them. Plans should include resources needed to support public sector responders. Identify the person who will interface with the public sector incident commander, have knowledge of the facility and resources, and have decision-making authority.

- ✦ Top management must support mutual aid pacts, and financial responsibility for resource sharing must be specified during the planning process.
- ✦ Each business must identify needed contractor resources and how they may be shared within the community. Joint planning will identify mutual expectations of the use of the same outside resources and create understanding of the limited resources in the public sector.
- ✦ Planning must consider the Maximum Allowable or Acceptable Down Time before the continued existence of a business is threatened, and must identify resources required to maintain or resume business activities at an acceptable level.
- ✦ Businesses must overcome the attitude that they can handle catastrophic events by themselves. During the planning process, confidence and trust must be exhibited by both sectors.
- ✦ The planning process is more than touring facilities. Take time to understand layouts, fire, and security systems. Bring public responders into facilities to obtain first-hand knowledge of risk locations, safety processes, and technologies.
- ✦ Consider using current private/public sector liaisons (such as community policing officers, school liaison officers, fire prevention officials, facility managers, and security managers) as catalysts for the joint planning process.
- ✦ Develop joint public/private resources and expertise inventory for each identified risk.
- ✦ In mutual aid planning, determine if certifications, licenses, and other requirements for private sector emergency response personnel are acceptable in the affected jurisdictions.
- ✦ Consider and develop mutual aid pacts that deal with resources or expertise that can be used or shared by other private or public entities during a critical incident.
- ✦ Mutual aid pacts between the public to private sector or private to private sector can be letters of understanding or informal agreements that do not mandate resource use in a critical incident. They are voluntary agreements between companies and the public sector to support each other in an emergency.
- ✦ Include the media in the planning process.
- ✦ Disseminate plans throughout the organization and update them continually. Don't let them become a dusty book sitting on the shelf.
- ✦ Cross train public/private resources to create understanding of credentials and capabilities. All legal requirements and situations that determine how public and private sector resources may be utilized must be understood.

- ✚ All personnel, both public and private, who are involved in a critical incident, must understand the incident command system. Egos must go out the window.

The horrible events of recent past have prompted many companies to reassess their emergency and disaster plans. While there is no "one size fits all" plan, companies will benefit from paying attention to the potential issues confronting their business and preparing and implementing a plan consisting of the key components identified in this article.

Once the crisis response plan has been designed, it can be implemented by integrating it into the company operations, training employees and constantly evaluating and upgrading it. A critical element of the plan implementation is employee communication. New hire orientation handbooks, job description assignments, and, of course, disaster drills and training, are common methods for communication of the plan.

Finally, the plan should not remain dormant. There must be an understanding that even the best crisis management plan is a work-in-progress. Effective crisis preparedness ensures that the plan grows and changes with the organization. Regular review and adjustment is essential to reflect changes in personnel and circumstances. In addition to routine testing of crisis response plans, an annual audit should be completed to consider how well the plan has been integrated with all other business operations.