Session No. 703

@ Your Service:
Business Continuity Planning, Surviving Katrina

William H. Barbarow, CSP
Fireman's Fund Insurance Company
Irvine, CA

Lester E. Washington, Jr.,CLSD
Marriott International
Converse, TX

Introduction

The long-term success of your business relies on your ability to sustain operations through business cycles and unforeseen events such as natural and man-made disasters. Businesses that do not plan for disasters risk their very existence. These businesses do not reopen or fail after opening due to the loss of customers, key staff, needed resources, and lack of investor support. This document will assist you in developing a Business Continuity Plan so your business can survive disasters such as: Fire, Natural Events {Flood, Hurricane, Tornado, Earthquakes, Winter Storms, Wildfires, Volcano, and Tsunami}, Hazardous Material Release, Technology Emergencies including communication failures & cyber attacks, Civil Disturbance, Workplace Violence, Power Outages, Terrorism, Sabotage, Virus Outbreak, and system/equipment failures during a crisis. Loss Prevention is easier, less costly, and more profitable than recovering from a loss. A comprehensive Business Continuity Plan provides the foundation for successfully meeting your corporate mission and allows you to evaluate your readiness to respond to unforeseen events.

The disaster planning process described below is an approach you can use to organize and construct your Business Continuity Plan. Once developed the plan must be trained, exercised, evaluated, and revised (at least annually). The plan must be comprehensive, inclusive of all potential stakeholders, and it must contemplate the worse possible conditions such as was learned in Katrina, where the infrastructure was destroyed, community emergency response was inconsistent/delayed, and there was limited available lodging for residents and emergency responders. When you plan for disasters, plan for the most severe conditions. Katrina had winds of more than 170 miles per hour, it created storm surges, wide spread floods and loss of life. It was hard to difficult to comprehend the damage done to the infrastructure. Some things are out of your control, but they are still within your area of responsibility.

Most companies address their property/business interruption loss exposures with a combination of insurance and deductibles. When evaluating your potential financial impact of a loss do not overlook the increased cost of materials, specialized construction skills, costs associated with re-use of building components and/or systems and costs due to limited site access.

Following an insurable loss, filing an insurance claim requires proof of ownership, documented damage, equipment inventory including serial numbers, copies of financial records & contracts, and your insurance policy. From the time the loss is incurred until it is settled and recovery is complete, document all your communications, transactions, and expenses.

Why Are We Here? "Marriott Int'l Lessons Learned from Katrina"

Katrina awakened us to the reality "What can go Wrong will go Wrong". Prior to Hurricane Katrina, Business Continuity was more a paper exercise vs. tool that could assist Marriott International with preparing for a disaster, be it man-made or natural. The majority of Marriott International's preparedness efforts focused on the ominous ever looming "terrorist threat".

Shortly before Katrina making landfall on that fateful day in September 2005 many of the Marriott Hotels in the City of New Orleans were busy preparing for conferences being held at the hotels and the events associated with them. When Mayor Nagin issued the mandatory evacuation of the City of New Orleans the hotels went into what is called "Mardi Gras" mode; which basically is reinforcing the physical security presence at each hotel by hiring NOPD officers to supplement the "in house" security staffing.

Preparations in anticipation of the potential flooding associated with the Hurricane were already underway in the guise of placing sandbags along the building perimeters, entry ways into the parking areas and lobbies. Windows were either boarded up or taped to minimize the potential for both damage and injury to guests or associates in the event the window shattered under the force of the winds.

Guests had been alerted and provided with written instructions regarding safe guarding themselves while in their guest rooms and the location of the designated "shelter in place" if it became necessary to require evacuation of guests to that location once Hurricane Katrina made land.

By then it was too late for the many guests in most if not all of the hotels in the City of New Orleans to get transportation to the Airport or attempt to drive out of the city due to the mass confusion and congestion on the roadways.

All the Marriott International hotels had "shelter in place" procedures and supplies and as such felt confident that no matter how severe the impact of Hurricane Katrina, that everything would be "just fine." How wrong they were!! The initial impact of Hurricane Katrina was very minimal, in fact the City of New Orleans faired very well, as did all the Marriott hotels in the city. It was not until the levies were breached that this situation quickly plummeted into *chaos*.

The next couple of days saw the City of New Orleans go from confusion, anger, apprehension into total anarchy. During this time those guests that were housed in the Marriott hotels in the city

began to sense the seriousness of the situation and became very demanding to say the least. The "shelter in place" supplies quickly disappeared as there were not adequate enough supplies to meet the needs of a prolonged confinement.

Eventually the guests of several of the outer lying Marriott hotels in the downtown area were relocated the large Marriott hotel on Canal Street for their safety. A couple of days after consolidating the guests in this hotel Marriott International put together a rescue effort and sent in personnel to extract the beleaguered guests and associates.

Upon completion of the successful rescue/extraction effort Marriott International began the process of securing the hotels which by now had been vandalized and looted. Paramilitary personnel were contracted to first secure the hotels and then provide security for Marriott International personnel performing recovery efforts. Initial recovery efforts were hampered first by the inexperience of the personnel and the lack of resources (electricity, water) or an infrastructure in the city.

The recovery effort was staged from Baton Rouge and required a daily 2.5-3 hr drive into and out of the City of New Orleans the first 3 weeks of the recovery effort. During the recovery effort there were numerous challenges that had to be considered with the initial decision to deploy personnel to the area:

- Contamination tools/equipment/clothing from putrid standing water in the buildings.
- Weather related health issues (i.e. heat stroke, dehydration). Humidity created by water and heat index meant that personnel needed abundance of fresh drinking water available and clean fresh clothing each day.
- Potential of bacterial infection from cuts/scrapes
- Allergic reaction to insect/reptilian/animal bites.
- Personal safety/security of recovery personnel.
- Reliable communication equipment, we found that satellite phones, blackberry units and Nextel direct connect were best option until cellular and land line service was restored.
- Transportation of recovery personnel.
- No potable water, resources to replenish food supply.
- No civilian authority (city government, police, fire departments) to partner with.

In preparation for deployment of personnel to New Orleans the Occupational Health Division outlined guidelines (recommended immunizations, protective gear, food/water requirements, sanitation standards etc) to assist each individual with preparing for exposure to the harsh environment that they would be confronted with while in New Orleans. What we did not consider are the following:

- Water borne illnesses due to spillage of sewage into flood waters.
- Inhalation of mold spores which could potentially cause upper respiratory infection. Eventually needed to bring in an Environmental Health specialist to conduct air quality testing (daily) prior to recovery personnel entering contaminated sites.
- Decontamination of tools/equipment/clothing.
- Recontamination of sites, this due to inconsistent/insufficient decontamination procedures at the entry point to each site.
- Capability to replenish fuel supply daily for vehicles.
- Refusal by military/police personnel to allow recovery personnel into restricted areas.

- Badges/ID's/Vehicle decals for easy identification by police/military personnel.
- Specialized and non specialized tools to assist recovery personnel. Many brought their own tools.

The following are Marriott International's Lessons Learned:

- Test and retest your plan, conduct table top exercises with senior leadership at corporate, regional and at the business units.
- Partner with local authorities to insure that they are fully aware of your corporate response and your expectations of them.
- Establish a "recovery" protocol that is sent in advance to the affected area leadership to assist in preparing for the influx of recovery personnel, supplies.
- Create "emergency tool/supply locker" and stage in strategic or potential "hot spot" locations for easy delivery/accessibility by recovery personnel.
- Establish advance procedures/protocol (retainer) to procure needed supplies (generators, fuel, food, communication equipment, rental cars) from key vendors.
- Know the extent of insurance policy and coverage level in advance. This will alleviate the apprehension in spending money on the recovery effort since much of the residual costs incurred can be recovered.
- Have PR personnel on site as quickly as possible. This will insure that your recovery efforts and corporate message is heard along with the negative images and stories offered by the media.
- Designate "Team Leader" on site who leads the recovery effort. By doing so you will help to minimize any problematic power struggles.
- Identify medical personnel to insure that they are integrated into the advance response team.
- Identify personnel needed for advance response and recovery teams. These individuals should possess the requisite skill, training, needed to meet the needs of the recovery operation.
- Establish and entry and exit strategy of recovery personnel since in many cases there will be a rotation of personnel until the recovery efforts are complete.

Marriott International and others faced additional challenges post Katrina such as data recovery and recycling of refrigerant. Data recovery was difficult, flooded areas were deep in contaminated water damaging equipment, data, and limiting access for prolonged periods of time. Data recovery is more than having a tape backup on site incase of a system failure. The ability to backup the data frequently, store it remotely and test the process are important to insure future success. All the refrigeration equipment had to be collected and recycled properly with recovery of the refrigerant.

Disaster Planning Process

Your planning process starts by establishing your team. This is not an activity for one person working alone. The primary purpose of disaster planning is businesses need to maintain tenants/residents, customers, and their income stream by identifying and evaluating their loss exposures, then developing plans to eliminate, mitigate or accept these exposures. The plans developed will include a response, and recovery components to resume operations.

The members of your team should include representatives from management, risk management, security, public relations, safety, legal, human relations, engineering, maintenance, etc. The team

activities will include first establishing a mission statement, assigning responsibility /authority, and setting timelines for completing the project. Once you have defined what you want to accomplish and when you intend to have it completed, then communicate the mission to interested 3rd parties such as tenants and customers to identify and incorporate their needs and values into the plan. Communicating your planning process allows all stakeholders in your business to have input as your ability to positively respond to an emergency affects them.

Analyzing your Risks, Capabilities, and Hazards

The analysis phase starts with your business activity including your resources and business requirements. First identify the critical operations that must be retained include tenant/customer retention, services, and products. Next ascertain your key internal plans and documents that support your critical operations these can include:

- Evacuation Plan
- Building Plans including fire protection plans
- Safety and Health Program
- Environmental Policies
- Security Procedures
- Insurance Programs/Policies
- Finance and purchasing procedures
- Facility closing plan
- Employee Manuals
- Hazardous materials plan
- Process safety assessment {HVAC, sprinkler systems, alarm systems, utilities, technologies, equipment requirements}
- Risk Management Plan
- Vital records including intellectual property, capital improvement plan, leases and contracts (specific terms and conditions)

Many of the documents listed above relate to codes and standards that must be complied with and/or referenced. Therefore you will need to maintain working copies of documents such as: Occupational Safety and Health regulations, Fire Codes, Environmental regulations, Seismic safety codes, Transportation regulations, Zoning regulations, and corporate policies. Emergency responders will need access to plans on building design, construction, fire protection, hazardous materials, etc. Make these plans available by electronic copy or store them off site in a location where they can be easily accessed.

In any emergency it is important to know the resources/capabilities you have available to respond to the conditions. Your internal resources/capabilities include your employees, key contacts/critical phone numbers, supplies (plastic bags, plywood, water, food, sanitation supplies, tools, lighting), search and rescue equipment, shelter capabilities, personal protection equipment, onsite power generators & fuel, portable air movement devices, pumps, computer equipment & software, telecommunication (hardwired and wireless). Some of these resources have measured life times (food and water have a 5 year life) and must be replaced on an ongoing basis. Your external resources can include local emergency management office, Fire Department, hazardous materials response unit, emergency medical services, hospitals, local and state police, community

service organizations, utility companies, contractors, suppliers/ vendors, and insurance broker & carrier industry experts. When you experience a regional disaster such as Katrina, your challenges are magnified. You face coordination issues between public and private sectors for the assessment of damage, response, and approval to established codes. There is a need for rapid wide spread assessment of damage, temporary fixes to the infrastructure to restore needed utilities while planning for the long term fix.

Perform a Business Impact Analysis to identify the assets most critical to continuing your operation and the mission of your organization. These strategic assets could be exposed to direct failure or they could fail due to an interdependency on other assets. Evaluate which of these assets is most likely to experience a loss. Include your executive leadership in the asset selection and evaluation process to gain their support for the process and prioritizing future financial resources to move forward not only on the business continuity plan but also for ongoing service/maintenance and security. Performing and prioritizing preventive maintenance is critical to insure the ongoing reliability of an asset. Once you identify your essential assets and operations you will identify the resources available and develop a plan on how to acquire them through formal and informal written agreements such as Memoranda of Understanding between public agencies and private companies. Some public agencies and cities are forming Formal Public Private Partnerships with the private sector. We need each other to recover from a catastrophe. Examples of these formal partnership programs are; (1) Credentialing [allows authorized essential employees access to restricted areas to rescue assets, stabilize IT systems & conduct damage assessments], (2) Information Sharing [FBI's InfraGard & terrorism early warning group, (3) Communications [link communication systems of emergency management officials and businesses], and (4) Resources [registry of private sector resources available to public sector]. You may utilize a network of liaisons with these agencies to maintain an ongoing presence.

When working with private companies you need to pre-arrange purchase orders and methods of finance. This can include establishing pre-negotiated rates at a hotel to house key staff during the disaster. The hotel choice will be influenced by the presence of on-site food, communication resources, meeting rooms, services etc. Some of your vendor's will be looked on to provide critical resources essential to your recovery. Request a copy of their continuity plan and evaluate their plan for completeness. If they have gaps in their plan work with them to address these areas or look at alternative vendors that you can rely on.

Now, analyze how susceptible you are to a loss. You can identify potential building and occupant hazards and determine the probability of risk. Use an evaluation matrix to evaluate the probability of a loss occurring vs. the severity of it's impact. This will allow you to focus initially on the most likely events with the highest potential severity (in a later section we will look at key potential events you face). The assessment process or the likelihood of a loss occurring is influenced by historical data, geographical data, technology, human error, physical, regulatory, terror exposure i.e. (symbols of America; physical location and/or building tenants). Once you have completed your assessment to determine the most likely events then evaluate their impact of each loss exposure in terms of it's effect on your business, your property, and on human life, (after most storms: food, water, ice, gas, and money are in short supply).

Your successful recovery from any loss exposure depends on your access and utilization of your external and internal resources including any backup systems. There are national associations that have web sites to assist organizations in planning and disaster recovery:

A. OSHA- Hurricane eMatrix:
Hazard Exposure and Risk Assessment Matrix for Hurricane Response and Recovery, developed after Katrina, Wilma, and Rita; www.osha.gov/SLTC/etools/hurricane/index.html. People responding to the aftermath of a natural disaster face changes in working conditions. There are new safety and health hazards that must be identified, evaluated, and controlled to reduce or eliminate occupational safety and health risks. The web-site is setup with general recommendations and task specific best practices.

The process starts by analyzing each task a responder will perform to identify hazards and controls, a Job Hazard Analysis can be used to accomplish this. The Risk Assessment Matrix, on the site, guides employers in making decisions assessing risk and best practices in areas such as: (1) worksite evaluation, (2) chemical and/or physical exposure monitoring and sampling, (3) hazard control, (4) work practices, (5) recommended personal gear, (6) personal protective equipment, (7) suggested training, and (8) medical considerations.

There are general recommendations on addressing: structural instability, contact with utilities, release of stored energy in machinery, noise, falls from height or through openings, exposure to asbestos, exposure to lead, material handling, exposure to unknown chemicals, lacerations, falls on working surfaces, personal hygiene and decontamination, fatigue, stress (including temperature extremes), animal exposures, impact to eyes/face from flying objects, sunburn, fires, motor vehicle/ machinery accidents, and contact with poisonous plants.

Finally Activity Sheets are provided for specific tasks: (A) Building Assessment, Restoration and Demolition, (B) Waste/Debris Removal and Reduction, (C) Infrastructure Repair and Restoration, (D) Community Support and Public Health Services, (E) Restoration of Maritime Infrastructure and Water Related Activities, and (F) Operation Specific Sheets [confined space, aerial lifts, HAZWOPER activities, trenches/ excavation, cranes, work zone safety, and heavy equipment. Each of these sheets gives a list of expected safety & health hazards, recommended engineering controls, work practices, administrative controls, personal protective equipment, applicable training needs, and reference materials.

B. The American Society for Healthcare Engineering (ASHE):
www.ashe.org/ashe/codes/hurricane/index.html. ASHE's site offers a page dedicated to support for healthcare facilities, as well as a members-only forum for discussions related to the hurricane, guidance on reopening shuttered hospitals, and a link to information on remediating water problems in buildings.

C. The National Institute for Occupational Safety and Health: www.cdc.gov/niosh/topics/flood. Among the resources accessible through this site are guidelines from the Centers for Disease Control and Prevention on personal protective equipment, disaster site management, air quality, electrical hazards, confined spaces, carbon monoxide, hazardous materials, and motor vehicle and machine safety.

D. The National Clearinghouse for Educational Facilities: www.edfacilities.org. The site pulls together resources for schools, including a safe school facilities checklist, guidelines for mold remediation, state-specific cost estimates for construction, and guidelines for disaster and crisis management for school districts and community colleges.

E. Federal Emergency Management Agency: http://www.fema.gov . The site has information on how to protect your business from disasters, emergency management guide for business & industry, a checklist for business recovery, flood maps etc.

F. U.S. Department of Agriculture Disaster Information: http://www.fsa.usda.gov/FSA/webapp?area=home&subject=diap&topic=landing. The site includes disaster assistance information.

G. U.S. Fire Administration: http://www.usfa.dhs.gov/safety/tips/disaster.shtm. The site has disaster fire safety tips.

H. OSHA Publication"Fire Service Features", http://www.osha.gov/pls/publications/pubindex.list The manual is intended to educate architects and engineers on the workplace needs for firefighters so designs can accommodate these needs and reduce the time it takes to mitigate an incident.

I. Planning for a Pandemic Flu, checklists developed by CDC and Health and Human Services: http://www.pandemicflu.gov/plan/business/businesschecklist.html This website includes checklists for planning business impact, impact on your customers and employees, establishing policies during a pandemic, allocating resources to protect your employees and customers during a pandemic, and how to educate your employees.

J. U.S. Chemical Safety and Hazard Identification Board, http://www.csb.gov/index.cfm?folder=Mission_History&page=index The Chemical Safety Board is an independent federal agency charged with investigating industrial chemical accidents. The website provides access to their investigations, lessons learned, and recommendations to prevent re-occurrence. In the case of Katrina, they post a safety bulletin on "Precautions Needed During Oil and Chemical Facility Startup".

K. Department of Homeland Security, "National Planning Scenarios", Version 20.1 Draft, http://media.washingtonpost.com/wp-srv/nation/nationalsecurity/earlywarning/NationalPlanningScenariosApril2005.pdf#search=%22National%20Planning%20Scenarios%22. This document provides the design basis for national preparedness goals and responder capability standards to the following hazards; nuclear, biological, chemical, natural disaster, radiological, and cyber.

Planning Process to Eliminate, Mitigate/Control, or Accept the Loss Exposures

Start with your potential loss exposures: Fire, Natural Events {Flood, Hurricane, Tornado, Earthquakes, Winter Storms, Wildfires, and Tsunami}, Hazardous Material Release, Technology

Emergencies including communication failures, Civil Disturbance, Workplace Violence, Power Outages, Terrorism, Sabotage, Virus Outbreak, and system failures during a crisis. Then evaluate their potential impact on your operation, develop a frequency/severity grid to determine the most events most likely to occur and have the greatest impact. An essential component of the evaluation process is maintaining ongoing monitoring of these exposures. Weather conditions often develop over time you need to continuously monitor conditions to prepare for a possible storm or tornado. The same monitoring is crucial for civil disturbances, changes in terrorism alerts, etc.

You can use a Project Management approach for your planning process on dealing with your Loss Exposures. Start with how you will be organized and how you will manage the process. Establish authority levels and responsibilities. Involve your executive corporate members to provide guidance/direction, resource availability, and they can mandate enforcement through new corporate policies. Decide who you will involve with: (A) planning, (B) analysis, (C) policies & procedures, (D) coordination, (E) testing, and (F) plan refinement that ensures control and execution. The process needs to be ongoing with a continuous lifecycle that tracks new business needs, technology changes, and maintains a clear business focus. The project requires defined goals and objectives, mission, purpose, expected outcomes, leadership, decision making and coordination process, timelines/milestones, deliverables, progress reports, and ongoing communication. This will allow your planning process to be integrated across all key areas and foster knowledge sharing.

The planning process goes through stages of refinement. Develop your plan through the following steps: tabletop exercise (all the players are together in a single location for this exercise) ⇒final draft ⇒distribute full document to all parties (including an implementation checklist). Once your plan is complete, establish a training and communication schedule for internal staff & tenants or other parties affected. Provide a method to store and retrieve the plan when it is needed (include off site storage in case you cannot enter the building after the event). Initially assign internal response procedures such as utility shutoffs, internal emergency medical response capabilities, recovery locations, reporting/notification to outside agencies, and external resources such as contractors and vendors available to you in time of a crisis.

Implementing a training plan allows your plan to become functional. Training exercises will reveal conflicts, overlaps, and gaps. Develop a training plan that is relevant to your facility and is problem oriented. You should utilize the facility, equipment designed for command, communication, control, and documentation to uncover potential problems such as their ability to function in a flood, or on emergency power. Also test the backup equipment such as generators, uninterrupted power supplies, communication devices (such as satellite phones, radios, computers) etc. Train in a dynamic situation where the exercise dynamics change based on the decisions made. Documentation of the entire exercise will serve as a useful learning tool. During the training process determine which outside agencies you will need to work with. With these outside agencies you will need to maintain ongoing communication and coordination of your ongoing activities. The outside agencies can include community emergency management office, Mayor or community administrator's office, Local Emergency Planning Committee, Fire Department, Police Department, Emergency medical services organizations, American Red Cross, Public Works Department, Planning Commission, Telephone companies, utilities, neighboring businesses, and banks (access to money is key review your bank's disaster recovery plan).

Communication Plans

Effective communications is essential throughout the entire process of evaluating the impact of loss exposures and responding to them. Communications include internal, external, as well as to impacted 3rd parties. You will need to communicate with members of your response team, company staff that work at the affected facilities, those working outside the affected area, and external stakeholders. Make a list of all possible audiences so you do not over look anyone. Storms such as Katrina destroyed trunk lines and flooded switching facilities. Computers, radios, and satellite phones can play a key role in the communication plan. Computers can be used to route radio communication to search out functioning radio repeaters. It is important to make certain that the radios are set at the correct frequency to communicate with others.

Establish a communication plan that provides redundancies so one person's inability to carry out their assignment will not curtail your plan. Consider an Internet-based emergency response system, conference calling, or, an automated call tree that can deliver a consistent message and keep your team informed. The most reliable satellite communications system is a self contained independently powered system that will allow you a gateway to the world via phone, fax and Ethernet. Your selections will focus on service provider experience working in disasters with harsh conditions and their ability to integrate the remote solution into your corporate network. Your communications plan may have to address international communications and multilanguage issues.

Communications especially external communications to the public and media need to be planned out and practiced so the information is correct, the right amount of information is communicated, and the message communicates what people need to know and is clear. Many companies utilize an external Crisis Management consulting firm to assist them in this area and develop a crisis management plan and an external message before the incident occurs. The consulting company can also provide assistance in media training, a media analyst on media relations along with speaking opportunities to prepare for a possible event. The plan must be written and practiced and distributed to individuals in charge of safety and security plus the management team. It is

advisable for members of the management team to carry wallet size cards with all their emergency contact information.

External communication needs go beyond communicating information on the disaster and it's effect on your organization. Your customers expect 24/7/365 access to your company services. You need an infrastructure that is designed to meet those needs and is flexible and integrated so it can automatically switch between data centers, balance workloads, share data, and support. Remember; before you send your message consider the legal, public relations, financial, and business implications.

Life Safety Considerations

Life Safety is a critical component of any disaster plan. You must be able to warn all the people in your building of a danger and provide them with the ability to evacuate to a safe location. This process starts with detecting a fire and communicating a warning via alarm systems (siren, strobe lighting, or directional fire alarm notification devices) and/ or verbal instructions prompting immediate action. The evacuation process includes providing exit signs/markings in hallways and stairways, emergency power to illuminate the path of travel, designating a place of assembly once outside the structure to account for everyone and then being able to instruct them further such as their ability to leave the site on their own or location of an emergency shelter on site or possible evacuation from site to a safe location. Conduct fire evacuation drills on a regular basis to familiarize people with the alarm sounds and document your evacuation times to track your results.

If your building has people identified with mobility impairments, implement a "buddy" system" to assist them in evacuation. Further, if you have individuals in your building that are using wheelchairs or walkers and are required to use stairs for emergency egress you may want to use an Emergency Evacuation Chair. This chair makes evacuation safer for all individuals including those who are providing assistance, including reducing the time to evacuate.

Two electrical hazards that can lead to failure and possibly fire are power surges and arcing. There have been changes to the codes and standards since 2000 to address surges; National Electrical Code Article 285 (Transient Voltage Surge Suppressors added in 2002) and UL 1449 (Standard for Transient Voltage Surge Suppressors). Install an arc fault interrupter to detect and stop electrical arcs that cause fires.

Emergency power must be sustainable over a long period of time when a regional disaster takes place. The system you select must be of the proper capacity, be reliable, and you will need ample fuel. The most common fuels are natural gas, propane, and diesel. Propane and diesel can be stored on site in above ground or buried tanks (properly anchored), if flood is a concern then storage should be above flood levels. The other considerations are cost of the generating units, fuel consumption rates, and circuitry. Gas and propane generators cost more and consume more fuel per hour. Once selected the generator must be installed, preventative maintenance implemented, and the unit must be load tested at least monthly to ensure it's proper operation. An emergency lighting system requires ongoing testing. NFPA Life Safety Code 101 requires testing for 30 seconds every 30 days and for 90 minutes annually. The circuitry required for emergency lighting is also important. You can have a night lighting component circuitry or you can use devices that do not require the night lighting circuitry. The latter save money and allow you to

deliver emergency lighting on standard circuitry. Photoluminescent markings and signs that glow in the dark can be used to improve life safety for your occupants. These devices can serve as a stand alone solution to marking exits or as a back-up to an emergency lighting system. New York City's Local Law 26 has established a set of standards for photoluminescent markings.

The materials used in building construction, furnishings, and decoration have a significant affect on occupant safety. Materials burn rates and smoke generation are key concerns. Select materials that have been tested and approved for your occupancy. Limiting smoke travel is also important. Seal, with approved materials, all holes in walls and floors. Provide smoke detectors in HVAC ducts to shut them down in a fire or exhaust the smoke. Furnish self closing fire rated doors in interior hallways and stairwells.

The property protection plan you implement will determine how effective you are in saving lives and protecting your property from loss exposures (fire, earthquake, carbon monoxide, & wind). The components of a property protection system can include fire/heat/smoke detection including computer based addressable fire alarm system (allows you to pinpoint and continuously monitor each alarm/device location); internal fire fighting capabilities, sprinkler systems and pumps, fire suppression systems for special hazards such as cooking, and smoke detectors that will initiate actions such as closing dampers in HVAC ducts. Installing and monitoring detection systems provides occupants with early warning, allows them to evacuate the building safely, and facilitates early response by internal staff and fire fighters. Your staff should be trained, at a minimum, on how to investigate fire alarms, operate hand held fire extinguishers, and assist in evacuating the building including aiding people with disabilities (warning them of the emergency and supporting their evacuation). The fire/heat/smoke alarm systems must meet the needs of the occupants, such as specialized alarms for the deaf or hard of hearing. Sprinkler systems, fire pumps, and fire suppression systems must be designed/installed, maintained, and tested (valve test, flow tests, control panel tests, periodic servicing) to National Fire Protection Association codes, International Building Codes, and those of the local authority having jurisdiction. The 2007 edition of NFPA 13 code is compliant with ASCE 7 on sprinkler installations in seismic zones (bracing, flexible connections etc.).

Occupants in buildings with carbon based (oil, gas, wood) fueled heating or generating systems have a possible exposure to carbon monoxide from incomplete combustion and improperly designed or functioning venting. Companies such as Marriott International are placing carbon monoxide detectors near all fuel fired devices to provide early warning of carbon monoxide exposure and thus provide time for a safe evacuation.

Wind is a loss exposure to your property and its occupants. Wind exposure can be evaluated by using historical information and adjusting it for your property's characteristics such as building height, construction components, etc. Wind damage controls include metal shutters, laminated glass, or window film used independently or in conjunction with other control measures to prevent breakage and the expulsion of glass shards.

Business Information and Asset Protection and Recovery

Preserving records of customer information, leases, and other high value items is important. Much of our information is stored on computers. Computers and laptops are vulnerable to theft, and therefore pose the risk of theft of the personal data of your customers, employees and

vendors. In order to protect this data, employees must take care not to store non-public personal information on the local drive of their desktop or laptop, on removable flash drives, or a writeable CD.

Storing non-public personal information on a file server that is part of the protected network provides greater security and ensures that the data will be backed up and can be recovered if need be. Disaster recovery starts with consolidating your data and servers. Then evaluate your data retention needs i.e. data to be backed up, archived, and the frequency for these actions. For regulatory reasons you may need to have more than one copy of the archived data stored at a separate location. The location of the data storage is important for availability during and after an event.

Your internal wireless area network can be security risk. You need to protect your signal from leaving your building and from allowing others to eavesdrop. Wireless area network signal leakage can be controlled by providing a Radio Frequency barrier on the skin of your building using such materials as foil backed drywall, certain window films, low-e-glass and pane poured flooring. Have a professional evaluate the adequacy of your control measures by theoretical calculations and/or an electromagnetic pulse device.

Information stored on paper is susceptible to fire damage, theft, and water damage (from fighting a fire, broken pipes, weather, etc.). Wet documents can be recovered and restored. One method of restoration is freeze drying the documents. This method has certain requirements for how documents are handled and packed. One of the important issues is to pack books, files, and records in clean boxes with a minimum space between items to allow for expansion during freezing but still secure for shipping. Freezing can stabilize the damaged paper, arrest inks from bleeding, and limit mold and bacteria development. In affect the freezing of these documents provides you time to select how you will dry the items and which information is a priority.

Security

Security protects your people, property, assets, and products including your intellectual products. Security starts with your hiring process, goes on through site access controls including during controls for special events. Tools available to security staff include perimeter protection (fences, gates, building materials), surveillance & detection equipment (CCTV systems with intelligent tracking video, digital video recording, alarm systems, tamper resistant smart cards), and internal response (security dogs, armed staff including electronic weapons, guns, nightsticks, mace, etc). Security systems can be integrated. Security hardware, software, and information can be connected locally and to a wider area network. This configuration allows monitoring, information storage, and management.

Your security needs are affected by your neighborhood, the work done by your employees, and the value of your assets. Overall security can be enhanced by permitting occupant parking near your building and visitor parking farther away. Provide access control systems by building entrances and require visitors to register when they enter the building. Employee access can be managed by using a biometric hand punch system, optical turnstiles (optical units scan cards) or mechanical turnstiles (none of these take the place of security personnel or prevent unauthorized entry). Also provide a dedicated delivery entrance. Utilize the principles of Crime Prevention Through Environmental Design to control access to your building, increase visibility, and overall

occupant safety. Protecting your air quality from attack is important, for assistance refer to the NIOSH publication No.2002-139, “Protecting Building Environments from Airborne Chemical, Biological, or Radiological Attacks”.

If your facility can face armed intruders or an attack, use building materials to deter them. Some Human Resource departments within companies, insurance claim offices & banks, use bullet resistant windows with poly carbonates. Military and chemical companies may purchase blast resistant exterior doors that are test certified to ASTM E90, FM, UFC, UBC, ICBO standards. These doors can withstand pressure up to 3.0 Pounds per Square Inch. The doors can also be fire and smoke resistive (3 hour fire - UL label, smoke 20 minutes).

Shopping Malls have been a terrorist target in Europe, Middle East, and Asia. Now security guards in American malls are being trained in anti terrorism. The training will be conducted using a 14 hour standardized course developed by the International Council of Shopping Centers and the Homeland Security Policy Institute at George Washington University.

Coordinate security with fire, life safety, and ADA concerns such as tying in exit door locks into the fire alarm system so all exit routes provide free egress and ingress during an emergency. System coordination can be achieved by using an open system that integrates security, fire protection, energy usage, paging/communications, etc. An integrated system can track energy usage, spot system/ equipment faults (prior to failure mode provides early warning, allows rapid response). Security badges in an integrated system can have electronic tags, if the person enters a prohibited space not only will an alarm register, but CCTV will also start tracking the person.

Security system standards are being developed. The National Fire Protection Association, in 2006, published the first editions of NFPA 730 & 731. NFPA 730 – “Guide for Premises Security” is occupancy based standard to protect people, premises, and information. NFPA 731- “Standard for Installation of Electronic Security Systems” sets minimum system performance and installation standards.

Available Plant Security Resources;
The National Cyber Alert System, https:/forms.us-cert.gov/maillists.
The AICHE’s Center for Chemical Process Safety, www.aiche.org/ccps.
Process Control Systems Forum, www.pcsforum.org.
The American Chemistry Council’s Responsible Care Security Code of Management Practices, www.americanchemistry.com/s_acc/sec_employment.asp?CID=373&DID=1254.

Water Damage & Recovery

Water and moisture intrusion require an immediate response by trained professionals. Delayed response increases your potential exposure to bacteria, fungus, virus, and mold. There are guidelines for restoration work; “Institute of Inspection Cleaning and Restoration Certification’s 500 Standard and Reference Guide for Professional Water Damage Restoration”. Water can be classified as Category 1, 2, or 3. Category 1 is clean water. Category 2 contains a significant degree of chemical, biological, and/or physical contamination and has the potential to cause sickness or harm to humans who are exposed to or consume it, after 48 hours this water in a flooded area may change to a Category 3. Category 3 water is grossly unsanitary water with

pathogens (sewage, river/stream/ground water from floods). The overall remediation process includes excess water removal, evaporation, dehumidification, evaluation of building materials and furnishings for retention or removal. The water classification and amount will determine the equipment, personal protective equipment, monitoring, and disposal requirements.

Slow water intrusion can be detected through Thermal Imaging, using an infrared camera. The camera detects heat. Water is a heat sink and retains its heat longer than the surrounding dry materials, which will cool faster allowing the operator to see the presence of water. The same camera can also be used to detect heat signatures of electrical equipment. Electrical equipment with loose connections, missing insulation, or if overloaded will generate excess heat from the load or possible arching. The infrared camera can evaluate these potential loss exposures and allow you to take preventative measures to limit your losses.

Best Practices Allow you to Recover

Once you analyze your loss exposures, you need to develop and implement control procedures/ best practices to control and recover from these exposures. The execution of the process requires it's own documentation audit process to ensure that it is effective. Post disaster when you no longer occupy the building you will need to have a plan for facility shutdown procedures to minimize the potential of further losses.

Manufacturing and chemical processes can be dangerous or explosive if they operate outside of their design specification. Many of these companies alarm equipment and processors to track processes and warn when they are out of specification. With the advent Distribution Control Devices, which have nominal cost, companies have alarmed everything. This action has produced information overload. Two organizations (Engineering Equipment and Materials Users Association and Instrumentation Systems, and Automation Society) have produced best practices guides for alarm management. The key to effective alarm management is to limit number of alarms especially high priority alarms. High priority alarms indicate immediate action is required to correct a problem. The alarm must also communicate what action is needed to correct the condition.

Risk Management concerns include: responder safety, environmental controls, and 3rd party safety. The emergency responders will be required to work in physically challenging environments. They will need appropriate personal protective equipment (PPE) for biological and/or chemical exposures. Trained staff first must perform sampling to qualify and quantify these exposures. After the samples are evaluated then the appropriate PPE can be provided. If NIOSH approved respirators are required then medically qualified staff will need to fit test the responders. Other concerns include; sanitation (personal & for their equipment), safe tools (guards/grounding), confined space entry procedures, safe working areas (free of sewage, mold, hazardous chemicals & gases), medical supplies/treatment/monitoring, communication tools, stress relief from working in an area of devastation (recovering dead bodies), and transportation. Debris removal and containment are a consideration. When hiring a 3rd party proper Risk Transfer/ Contractual Liability controls must be in-place prior to any work commencing. These controls include; current certificates of insurance with your company named as an additional named insured, contracts and/or purchase orders detailing the work to be performed, hold harmless agreements, etc. The companies you select should have an existing Health and Safety

plan designed for anticipated conditions and they should be able to articulate their plan to your satisfaction prior to signing any contracts. Their Health and Safety plan should meet or exceed your own plan requirements.

Your employees are essential to implementing your recovery plan. No company plan is complete without including your employee's own personal disaster plan. The Risk Management department and Continuity Team can assist your employees in developing their personal plans. The six components of an employee's home preparedness plan are; (1) water, (2) food, (3) first aid supplies & possible training in 1st Aid and/or CPR, (4) bedding, (5) tools & emergency supplies, and (6) clothing. You will also want your plan to address employee travel, transportation and communication needs. Occasionally, you may need to relocate key staff members and their families outside the disaster area so they can function more effectively, plan for it. Restoring your e-mail will assist in communicating a consistent message to your staff and others.

Business recovery and restoration process includes involving professionals in continuity planning, damage assessment, cleanup, restoration, reconstruction, documentation of actions, maintaining chain of custody on materials that may have contributed to the loss, post incident development of a Lessons Learned document to assist in improving the plan, and insurance company communication. Resumption of operations with customers and tenants can only take place after the area is safe and tests have verified the atmosphere, infrastructure, and structures meet all existing codes and standards.

Finally there needs to be a plan to safely dispose of unusable assets and recover potentially harmful substances. The disposal plan should include HVAC & refrigeration equipment (including Freon gas recovery), propane gas tanks/cylinders, electronic goods, hazardous substances (paints, degreasers, cleaning supplies, lubricants), etc.

Business Continuity Plans Are Living Documents

The Business Continuity Plan is a living document. The implementation process includes; conducting training with internal staff and tenants ⇒drills ⇒exercises ⇒modifying the plan based on drills and exercises. Provide for a continuous improvement process with at least annual plan reviews. This must be part of your culture and value system having assigned roles, defined responsibilities, and the expectation that successful implementation is a business necessity. As your business undergoes continuous change you need to be prepared to meet that need.

Losses negatively impact your organization. There is a value in learning from your prior losses and from the prior losses of others within your industry. This information will allow you to implement controls to prevent the loss from occurring.

Here is a sample of a Lessons Learned from a prior loss;

Blocked Drains Cause Roof Collapse, during a heavy rainstorm water collected on the roof, the added weight exceeded the load capacity of the roof and it collapsed. Post loss analysis revealed that the roof drains were clogged. Roofs and drains are recognized loss exposures. In this case, they had not been inspected for some time. A preventative maintenance program that was in-place and followed would have prevented this type of loss.

Conclusion

After experiencing Katrina, Rita, earthquakes in California, Tsunami, floods, anthrax, and winter storms are we prepared? In 2005, the Insurance Information Network of California and Fireman's Fund Insurance Company co-sponsored a statewide poll of California residents, 22% consider themselves prepared for a disaster. At the recent American Military University symposium speakers noted that local communities have major gaps in their disaster plans and don't address mass casualties. Don't wait for a disaster to strike take pre-emptive actions to protect yourself, your family, and your place of business from a disaster. Put in-place a plan to recover and resume your life, your business. Form partnerships with other businesses and public agencies. Take action now!

Bibliography

"A System Ready for Disaster." *Occupational Health and Safety*. Feb. 2007: 78-80.
"All Circuits Are Busy Now." *Disaster Recovery Journal*. Winter 2006
"Asset prioritization strategy: A quantitative approach." *Journal of Business Continuity & Emergency Planning*. May 2006: 37-46.
"Best Practices." Professional Safety. October 2005: 48-50.
"Beyond disaster recovery: becoming a resilient business." *IBM Solutions Point of View*. Oct. 2005
"Biometrics Solves Buddy Punching for Hilton Resort." *Access Control & Security Systems*. January 2007:25
"Business Owners Are Reminded of the Perils of Power Loss." *Disaster Recovery Journal*. Fall 2006
"Californians and Disaster Preparedness -- On Shaking Ground?" *Disaster Safety Review*. Spring 2006: 9-11.
"Catching Up." *Building Operating Management.* Feb.2007: 61-66.
"Controlling the Business Interruption Exposure." *Engineering and Safety.* Sept.2004
"Establishing A Corporate Business Continuity Program And Continuity Program Office." *Disaster Recovery Journal*. Summer 2006
"Everyone Needs a Place to Sleep." *Disaster Recovery Journal*. Spring 2006
"Fire Safety Plan." *Engineering and Safety.* Oct. 2002
"Forces of Nature." Security Products. Nov. 2006: 54-56.
"Forming Public Private Partnerships." *Disaster Recovery Journal*. Winter 2007: 67
"Ice, Gas & Money." *Disaster Recovery Journal*. Fall 2006
"It's Not Your father's Security Anymore." *Fire Protection Engineering.* Winter 2007: 16-24
"Lessons Learned from Katrina." *Disaster Recovery Journal*. Summer 2006
"Lessons Learned from Katrina." *ASSE, EnviroMentor* 2006 Newsletter
"Managing Alarms." *Control Engineering*. February 2007: 50-54
"NIST's WTC Investigation." *Facility Safety Management*. July 2005
"Over-current Issues For Voltage Surge Suppressors." *IMPO*. Jan. 2007: 22-25.

"Panic slowly." *IBM Solutions Point of View*. Sept. 2006
"Protecting Your Plant From Attack". IMPO. Feb: 24-27
"Resources for Developing Emergency Plans." *Engineering and Safety*. Nov.2006
"Response to Fire Alarms." *Fire Protection Engineering*. Winter 2007:9-14
"Safety Tips." *Health + Safety*. Feb. 2007: 52.
"Targeting Terror in the Mall". *AC & SS*.Feb.2007:8
"Testing Murphy's Law." *Disaster Management*
"Water Damage Restoration." *Building Services Management*. Feb. 2007: 12-17.
"Wireless Security: Keeping The Network Under Wraps." *Building Operating Management*. Jan. 2006: 34-35.