Risk*topics*

Effective Disaster Recovery

Strike before disaster does!

A warning well worth heeding. But what exactly is a disaster? A disaster is an event that threatens the very viability and survival of your business. Every day challenges faced by business are often mistaken as disasters. The reality is that a disaster is a once in a life time event for most businesses. In fact, 43% of businesses that experience a disaster never reopen and another 29% close for good within two years. Disasters tend to follow "Murphy's Law". They tend to occur when you least expect it or are least prepared for it. There is no such thing as a "right time" for a disaster.

What is a disaster?

A disaster is a calamitous event that occurs with out any prior warning and causes substantial interruption requiring prompt management attention. Disasters come in many types and forms. You can classify them simply as natural or man-made. Natural disasters include floods, hurricanes, tornadoes, earthquake and others. The extent of the threat is a function of geographic location of your business. For example, the earthquake threat is much higher in California than in Florida. By the same token, the hurricane threat is higher in Florida than in California.

There are many man-made threats faced by business. They vary by the type of operations. For simplicity, they can be classified as fire/explosion and toxic releases, products and service brand protection, internal and external. A chemical toxic release or a fire/explosion manifests itself in a very obvious way. Compared to a fire/explosion, many other disasters, such as a product disaster are "slowly developing" wrecking havoc with your business reputation and brand recognition. Product disaster may range from a highly publicized liability case to a massive regulatory action or a recall. Many events that are internal to a business may result in an adverse impact. These events range from computer system failures, loss of utilities, failures of critical processes and equipment to work place violence. Disasters of external origins include many threats, such as supplier chain disruptions, terrorism and others.

Risk Engineering

Where standard solutions are the exception

ZURICH

Disaster management, catastrophe management, contingency planning, crisis management, emergency response and recovery, business recovery and continuity are various versions of the same concept of planning of pre-loss preventive measures, emergency response and post-disaster actions to assure survival and continuity of a business. An effective plan must consider various aspects of pre, during and post disaster exposures. The overall goal is to maximize business continuity and minimize business interruption by being prepared the event.

Need for Planning:

When a disaster strikes, what is the management's responsibility? Management has the responsibility to plan for appropriate emergency response and recovery. In addition, the business is also accountable to its shareholders, employees as well as the community. Crisis response results in a reevaluation of a company's management by all stakeholders. A well-planned response provides an opportunity to turn a negative into a positive impact for the future of the business. When a disaster strikes, the survival of the business is on the line. The lack of an effective emergency response and recovery plan may spell the difference between success and failure. A business recovery plan with out any focus on prevention and emergency response programs is doomed to fail. Failing to plan is certainly planning to fail.

Challenge

Most businesses have developed parts of the emergency response plan in response to various regulatory requirements. For example, the Environmental Protection Agency requires businesses in the chemical segment to have appropriate Risk Management Plans (RMP) and Spill Prevention Control and Countermeasure Plan (SPCC) in place. Occupational Safety and Health Administration (OSHA) has evacuation requirements for employee safety. The challenge is to develop a proactive plan that is integrated and addresses a wide range of credible scenarios that may one day impact your business.

Perhaps you have considered developing a Disaster Management Plan, but are reluctant to commit resources to an effort that appears to have marginal payback. Contingency Planning is not a cost, but an investment in your company's future and survival. Development of the plan requires a review of the business processes for their criticality. This leads to a better understanding of your own business processes, a reduction in redundant efforts and better utilization of resources. A 360-degree holistic approach will lead to a more integrated, yet simple and effective plan. An effective plan will help also you reduce the potential civil and criminal liabilities by better documentation and transparency of your intentions and efforts.

Some argue that you can not plan for all foreseeable and unforeseeable threats facing your business. Planning is a "state of mind". When you plan your response for the foreseeable events, it gives you a strong framework to respond to many of the unforeseeable events. Many consider this to be such a daunting task that they are afraid to take even the first step. The task of developing the entire plan can be managed by a systematic approach that allows you manage it in phases so it does not overwhelm you.

Developing the Plan

You can hire a consultant to "write a plan" for you or you can involve your

own staff in the development of the plan. Unless your staff has the ownership of the plan, it will never be a living document and it will likely gather dust on someone's shelf. Various software programs are available for writing emergency response and business continuity plans. Some are simple word processing type programs, and a few products in the market have all the bells and whistles, such as automatic telephony and advance web-based communication feature, area map overlays and access to material safety data sheets and other references. Some of these programs can be expensive and have significant system requirements. The key to success is to keep it simple to implement and access the plan in case of an emergency. Integrating the plan into daily activities reduces the "learning curve" and keeps it a current and living document.

Phase I:

Zurich's program is divided into three phases. Phase I starts with obtaining commitment from the senior management, including allocation of resources and budget for the development of the plan. This is followed by a <u>Vulnerability and Business Impact Analysis</u>. Some potential disasters are very obvious, while others are not. The <u>Vulnerability and Business Impact Analysis</u> is a systematic attempt to identify all credible threats and to assess the likelihood and potential severity of business impact of various emergency scenarios. A compilation of all the credible threats will help you identify the critical vulnerabilities based on the likelihood and the severity of business impact on your balance sheet.

Phase II:

The phase II focuses on auditing the current level of emergency preparedness in response to the critical vulnerabilities identified in Phase I. Most publicly traded businesses have some form of contingency plans. Some are more formal than others. A good starting point for most companies is to dust off the Y2K plans that were required by the Securities and Exchange Commission. An honest and realistic review is a <u>Gap Analysis</u> to assess the gap in each existing level of preparedness. This effort will lead to several action plans to fortify the prevention and response-recovery programs for

<u>Gap Analysis</u> is the critical assessment of the internal preparedness and external support. Consider factors, such as the protection of people, property, environment and vital records; alarms, procedures and emergency response organization; adequacy of resources (both people and equipment); capabilities, training and support. In-depth audits of critical functions, such as security, computer network and data back ups is a must. A review of your response to past incidents and the effectiveness of emergency drills provide a reality check. Most disasters are like domino or chain events. Internal preparedness should focus on the earliest detection of any abnormal event and plan for mitigation measures to control and prevent damaging escalation into a catastrophe. Assessment of external support focuses on interaction and joint drills with various emergency response organizations, standby contracts and mutual aid pacts for emergency resources and services, and public relations. Communication is the critical factor for both internal preparedness and external support. This includes identifying key members and alternates for the emergency response team, current verified telephone/cell phones and pager numbers, testing of alarms and mock drills.

Phase III:

Phase III focuses on developing appropriate strategies for your balance sheet protection by closing the gaps identified in Phase II. In addition to enhancing prevention plans and the hazard-specific response elements in the emergency response plan, Phase III focuses on recovery and restoration through business continuity planning. This consists of planning to minimize the anticipated business interruption in the aftermath of a disaster. Assuring the safety and security of people and stabilization of the immediate crisis is the primary task. Recovery planning starts with site safety and security, followed by a damage assessment and salvage and recovery planning. The success of any recovery and restoration will depend on the advance consideration and prioritization of your goals for recovery. Depending on your priority to get back in operation as quickly as possible or to salvage the vital documents, electronic data and contents, your recovery strategy is going to be very different. This prioritization will help you develop your recovery strategy that is consistent with your recovery goals and needs. Whether the anticipated loss is small or extensive, recovery planning should consider designated response and recovery teams based on their function and specific activities. Examples include management, human resources, and facilities–operations and public affairs. Teams for restoring specific activities include telecommunication, data center, utilities and others. Recovery for a small loss and minor damage can be handled with internal resources. Extensive damage will most certainly require services of a qualified salvage and restoration company. This is especially true in case of extensive fire and water damage to vital records, computer media/records and electronic equipment. Standby arrangements with restoration contractors should be considered in the planning process.

The responsibility and procedures for the activation and deployment of these recovery teams and contractors should be part of the plan. In the aftermath of a major disaster, key persons may not be readily available. Consider establishing chains of command and lines of succession for key personnel. Based on the initial damage assessment and your recovery strategy, the decisions about temporary relocation of the facility, repair/replacement of critical equipment or contracting production are some of the key decisions that must be made. An accurate inventory and assessment of critical processes, assets and resources required for the resumption of business will make it easy to restore operations quickly.

Many catastrophic events have a significant physical and psychological impact on employees and associates. This should also be considered explicitly in the recovery strategy. Counseling and other employee assistance programs will help your employees cope with the adverse impact of the event and adjust during the recovery phase.

Testing the Plan

An effective plan is a living document. In addition to the emergency response and recovery teams, all employees and contractors should be familiar with emergency response activities and their own specific roles such as alarm signals and evacuation, gathering points and powering down the critical equipment. Mock drills and table-top exercises will help you identify and critique the strengths and weaknesses of the plan. The drills may focus on planned or unplanned scenarios to verify the understanding of procedures by employees.

The results of the drills will help you focus on additional training as needed.

Establish formal procedures for periodic reviews of the plan. These reviews should occur at least annually. Establish change management procedures to address the impact of material changes to processes, business priorities, personnel assignments and other information. Since prompt communication is the key, periodic of check calling-trees to verify the accuracy of phone numbers, cell phones and pagers should be conducted.

It is not is not a matter of "if a disaster will strike". It is only a matter of "when a disaster will strike". Lack of planning is a threat to your business survival. Be prepared and plan ahead.

Help from Zurich

You are the expert in your business and you have the intimate knowledge of your business processes. You are the best judge of your business environment and your goals and priorities for recovery. Only you can "write your plan." If comprehensive disaster management planning is still a daunting task for you, Zurich Risk Engineering can guide you through the process. We will work with you through our three phase planning process to facilitate the development and implementation of an effective plan.

We can

- Facilitate a discussion with key members of your management staff to complete a Vulnerability and Business Impact Analysis for your operation.
- Complete a Gap Analysis to identify the strengths and weaknesses in your procedures and management systems for emergency response and recovery.
- Provide an assessment of your prevention and mitigation efforts for overall operations a specific vulnerability, such as life safety, premise security or hazardous material transportation.

Assisting our customers in the development of an effective emergency response and business continuity plan is just the another aspect of our partnership with our valued customers. Zurich Risk Engineering is uniquely qualified to work with you to provide the full range of risk control services that focus on addressing large catastrophes that threaten your balance sheet to every day events, which at times can seem disastrous themselves. This is truly a "win-win" situation. While we can provide no guarantee that all the disasters will be averted, our mutual efeforts will ultimately pay dividends.

ZURICH

Zurich Services Corporation
Risk Engineering
1400 American Lane
Schaumburg, IL 60196

Telephone +1-800-982-5964
Fax +1-847-605-7736

ISO 9001
Quality-Assured Solution Provider

Risk Engineering Driven Services   Team-Based Solutions   *Knowledge Transfer*