Communications of the IIMA

Volume 6 | Issue 2 Article 4

2006

# Disaster Planning and Management

Holmes E. Miller
*Muhlenberg College*

Kurt J. Engemann
*Iona College*

Ronald R. Yage
*Iona College*

# Disaster Planning and Management

Holmes E. Miller
Muhlenberg College, Allentown, PA 18104

Kurt J. Engemann
Iona College, New Rochelle, NY 10801

Ronald R. Yager
Iona College, New Rochelle, NY 10801

## ABSTRACT

*Recent events such as hurricanes, tsunamis, earthquakes, power outages, and the threat of pandemics have highlighted our vulnerability to natural disasters. This vulnerability is exacerbated by many organizations' increasing dependence on computer, telecommunications, and other technologies, and trends toward integrating suppliers and business partners into everyday business operations. In response many organizations are implementing disaster recovery planning processes. In this paper we discuss how to identify threats and scenarios; how to articulate the disaster recovery strategies; and four elements of the generic disaster recovery plan: Mitigation, preparedness, response, and recovery. We then provide examples of software that can help disaster recovery professionals in the planning and implementation process. Finally we present some trends that will reinforce the criticality of the issue.*

Keywords: Disaster Recovery Planning; Business Continuity Planning; Risk Assessment

## INTRODUCTION

Several major natural disasters that have occurred in the past few years have placed disaster management on the front pages: The Tsunami of late 2004, Hurricanes Katrina and Rita, and the earthquake in Pakistan in 2005 affected both life and property and emphasized our vulnerability to natural threats. EM-DAT (2006) figures complied by the Belgian Université Catholique de Louvain's Center for Research on the Epidemiology of Disasters (CRED) and the United Nations International Strategy for Disaster Reduction (UN/ISDR) indicate that:

- In 2005 the number of natural disasters was 360, up from 305 the year before. The number of floods increased by 57 per cent in 2005 (107 in 2004 and 168 in 2005) and droughts by about 47 per cent (15 in 2004 and 22 in 2005).
- In total 157 million people--seven million more than in 2004--required immediate assistance, were evacuated, injured or lost their livelihoods. Despite this, loss of life (91,900) was significantly lower than in 2004, during which 244,500 people died as a result of natural hazards (a large portion due to the Indian Ocean Tsunami).
- Disasters in 2005 cost a total of $159 billion in damage, although out of this figure, $125 billion were losses caused by Hurricane Katrina. Notwithstanding, costs incurred from disaster damage rose by 71 per cent from the total $92.9 billion in 2004.

"These figures re-affirm trends we have been observing for the past decade," says Salvano Briceno, UN/ISDR Director, "less people are dying from disasters, but there are many more long-term, negative implications for sustainable human development. Countries and communities need to understand their risks, invest in resources and prioritize their policies to reduce their vulnerability to natural hazards. It is the only way to spare lives, reduce economic and environmental destruction when the next disaster hits."

Data from the EM-DAT database reinforces the trend of increasing worldwide economic impact. In eight out of the past eleven years, worldwide losses exceeded $50 billion and in four of those years, losses were approximately $100 billion or more. Beyond changes in the frequency of natural disasters (not even including man-made disasters and terroristic activities which also are of increasing concern), the increase in population growth and industrialization has caused increases in the number of people affected, and has exacerbated economic losses. We are more vulnerable due to factors ranging from larger populations in disaster-prone areas to often aging infrastructures. Moreover, due to the inter-connectedness of modern business enterprises, even relatively "minor" events such as a hurricane or fire, if occurring in a vulnerable commercial link, can devastate business operations.

Given these changes and our increasing vulnerability, some key questions facing disaster managers are:

- Can we prevent/mitigate the occurrence disasters and if so, what are the cost/benefit implications?
- In an ever-increasingly connected world economy, how can we prepare for disasters?
- When a disaster does occur, how can we respond in a manner that minimizes damages to property, equipment, and most importantly, human life?
- How can organizations recover from disaster and resume operation in what may be a degraded operating environment?

Disaster management has a long history, starting with Noah's mitigation strategy of building an ark to deal with the effects of the great flood. More recently, many organizations have implemented structured management processes. Examples of such methodologies are given in Hiles (2004), Wallace and Webber (2004), and Zsidisn et. al. (2003). The specific methodologies cover many of the steps mentioned in this paper, specifically the section of "Disaster Planning." A first step is risk assessment which involves estimating the likelihood of occurrence of events (Lewis et. al 2003). Estimating event probabilities is particularly challenging because of the relatively small probabilities of event occurrences. Given the probabilities of events occurring, the disaster recovery process also calls for estimating potential losses, again a challenging task given the hypothetical nature of the endeavor. Decision analysis is a method often used to facilitate calculating expected losses once the event probabilities and looses are quantified (see Engemann and Miller 1992). Kunreuther (1996) discusses both issues related to estimating probabilities, losses and one mitigation approach – insurance – which will be discussed below in more detail.

To be effective, the disaster recovery planning process must be business driven, i.e., business managers must frame priorities and provide overall guidance and support. An example of such a business-driven process is given in Miller and Engemann (1996). Once the business priorities have been revealed and risks evaluated, structured methodologies can be used to develop the overall disaster recovery plan. After the plan is developed, to ensure the plan is current the final and ongoing steps involve maintenance and testing (Maslen 1996, Iyer and Sarkis 1998).

In the following sections we will discuss the disaster recovery planning process in more detail. Although the points to be discussed are valid for all environments we will frame the discussion in terms of a business organization. In addition, we will discuss the Disaster Recovery Plan, the living document that guides an organization through the various steps from before a disaster strikes to recovery and resumption of normal activities. We divide our discussion in four parts: Mitigation, Preparedness, Emergency Response, and Recovery. These address the four questions posed above and reflect phases of disaster management planning standard both in practice and the literature. In our discussion the terms "disaster recovery" and the more recently popular term "business continuity" (signifying continuing business operations "without skipping a beat") will be used interchangeably.

## PHASES OF DISASTER MANAGEMENT

### *Mitigation*

The Mitigation Phase seeks to prevent hazardous events when possible, reduce their severity when they actually do occur, and minimize the ensuing losses and damages. Although preventing or reducing the occurrence rate of natural disasters such as hurricanes, earthquakes, and floods is impossible, events *resulting from* the instigating event often can be mitigated and even prevented. For example, while little could be done to prevent Hurricane Katrina from striking the Gulf Coast, the flooding of New Orleans was the result of a preventable act: The levees failing, which caused far more damage than the hurricane itself.

Preventing or mitigating subsequent events is the result of steps taken and controls implemented prior to the initiating event's occurrence. Stronger levees in New Orleans are one example; a tsunami early warning system is another; hurricane resistant shatter-proof windows are a third. All of these actions reduce or eliminate losses.

When a disaster strikes, losses may be viewed as direct and indirect. Generally, direct losses are immediate and are caused by the disaster's occurrence (e.g., loss of property, loss of life). Indirect losses often are economic and include losses incurred subsequent to the disaster, for example, lost future business. Losses directly caused by a disaster can be mitigated by steps taken long before the disaster occurs. The logic behind these mitigating actions is that given a specific event -- for example, fire, flooding, wind damage from hurricanes, pandemics -- one identifies *how* damage is caused. For example, hurricane winds can shatter glass, rip roofs of buildings, and even lift and displace buildings. Given these results from an event, one asks what can be done to lessen the losses. Possible actions range from avoiding losses altogether to reducing the losses by "hardening" the targets. Avoiding losses may mean not locating any facilities in areas where an event is likely to occur. While rational, often complete avoidance is not practical. For example ideally people could avoid hurricane threats by not locating in coastal areas; to avoid earthquakes people would avoid locating near fault lines. Such changes, however, are unlikely to happen in the near term.

Even if one cannot avoid an event, one may reduce its impact by addressing the questions, "How can the event cause damage and what can we do about it?" The answers provide guidance regarding which targets should be hardened, and how they should be hardened. Often cost/benefit decisions determine whether or not to take action. Some examples of effective mitigating actions include:

- Building codes and other construction standards that specify that structures can withstand earthquake level shocks or hurricane winds (Mileti 1999). For example Ryland (2005) points out that building codes implemented as a result of Hurricane Andrew saved over $20 million in one Florida county alone, after Hurricane Charley in 2005.
- Fire retardant construction materials, fire breaks, fire doors and fire suppressant systems that reduce the direct and indirect losses due to fires (Voelkert 2006). In addition to physical responses to fire, ensuring sufficient numbers of fire houses and other emergency services are available and locating those emergency services can reduce response times and also mitigate the effects of fires and other disasters.
- Locating facilities to avoid threats. While cities are where they are, the situation is different for factories, data centers, and service processing centers. Judicious planning and some foresight in considering underlying risks can cause companies to avoid disasters entirely.
- Protecting telecommunication systems, databases, and computer hardware from being destroyed or rendered inaccessible by hardening the systems and designing the systems to ensure there is no single point of failure (Whitman 2003, Baskerville 1993). Ellison et. al. (1999) discusses the concept of survivability to ensure a robust response to a system shock – i.e., ensure the system fulfills its mission rather than focusing on protecting specific physical assets.

Several technological and analytical tools exist to facilitate disaster mitigation efforts. Underlying all of them is a well-educated and properly trained staff that judiciously uses information. For example, Geographical Information Systems (GIS) can augment the mitigation effort. GIS applications manipulate geographically referenced information, and allow users to collect and integrate, store, analyze, and display information (see Heywood et. al. 2002). GIS applications also have been applied to predicting and modeling disasters – for example, GIS applications have predicted landslides (Carrara et. al. 1999); tsunamis (Wong et. al 2004); and flooding (Tsihrintzis et. al. 1996).

Beyond GIS, other information processing applications can also help mitigate the effects of disasters. Catastrophe modeling can be used to simulate natural disaster events and estimate their impact (Smith 2000). These models be used to test various mitigation strategies by developing a loss profile under one scenario, and then testing alternatives, such as using different sites, or reallocating resources and then seeing how the loss profile changes. The result would be lower losses when a real disaster actually occurred.

Insurance can also be used to mitigate losses. Generally, insuring catastrophic risks requires specialized insurance such as earthquake insurance or flood insurance. In light of recent events, obtaining reasonable prices for these policies is a challenge. Kovacs and Kunreuther (2001) and Kunreuther (1996) point out that insurers offer coverage for uncertain events under two conditions: They can estimate the chances of events occurring and the losses if they do occur, and they can set premiums for each class of customers. The more ambiguity regarding probabilities and losses, the higher will be the premiums. This is coupled with two other problems: "Adverse selection" (where insurance priced on average probabilities creates incentives for customers with better than average probabilities of avoiding losses to not purchase, and for the poorest risks to purchase); and "Moral hazard" (where a customer with insurance acts more recklessly). Natural disasters introduce a third risk: Correlated risk. For example, for hurricanes, floods, earthquakes, many policy holders in a given area may simultaneously file claims since all will be affected. This results in insurance companies seeking to leave markets, or pricing products with high premiums.

Given these facts although insuring for physical losses and business interruption often makes good sense -- no company should rely on insurance to the exclusion of disaster recovery plans. Indeed, having well maintained and tested plans may be a prerequisite for being able to secure insurance in the first place! Moreover, the biggest risks cannot be covered by insurance policies alone – for example, customer loyalty, a business' reputation and the public's trust. Insurance's mitigating role is minor relative to having an effective disaster recovery plan (or the more recently coined term, business continuity plan).

### *Preparedness*

Preparedness prior to a disaster involves putting in place the various steps called for by the disaster recovery plan. Five general steps include: Identifying threats and given these threats, targeting various scenarios that might manifest themselves; determining how a company will function if a disaster strikes, including which areas are critical and which are non-critical; identifying suppliers and customers needed to continue operating and given these relationships, ensuring that contact lists and communications links are in place; preparing for the possibility that business locations and supplies are inaccessible. (i.e., pre-positioning supplies and using alternate facilities); ensuring the members of the crisis management team have been identified and all individuals – from management team members to employees – know their roles and understand their responsibility if a disaster occurs.

To prepare, step 1 is to identify relevant disaster scenarios, which starts with identifying natural hazards in the region, and assessing risks and vulnerabilities. These then can be used to estimate the specific disaster's effects and with guidance from business managers, to highlight the required level of response. Not all scenarios apply everywhere and not all business functions need be immediately accessible. For example, Chicago might not need to plan for hurricanes, and a 401K online query system might be inoperable for several days. While the same general plan might work in the face of several different scenarios, events can occur that can render a disaster recovery plan ineffective. For example, the northeast power outage of 2003 (CNN 2003) highlighted weaknesses of disaster recovery plans that called for backing up data centers in geographically dispersed sites, that still ended up on the same large power grid. A well-crafted plan that might have worked for a major hurricane striking New York City, would be less effective for of an outage such as this.

Since every scenario cannot be identified, plans must be robust and must provide the capability of working when faced with an unplanned event. For example, no organization planned specifically for September 11th yet contingency plans tailored for other events were executed (Beacham and McManus 2004) and though the results were mixed, larger companies such as Cantor Fitzgerald even in the face of horrendous losses of life, functioned better than many smaller firms. Since when faced with an event, no organization can function at the same level for all products and services as in its normal environment, triage operations can help separate the critical from the non-critical activities.

As noted above, business needs determine the critical operations and services. Atkinson (2003) discusses Wal-Mart's approach to identify threats and critical business functions, which begins with a five hour risk identification workshop attended by senior managers to get them thinking about what risks might prevent them from meeting their business objectives. After a series of queries, the executives identified 20 to 30 key risks and then voted to select the highest ones. This is one of several structured methodologies to elicit senior management preferences necessary in developing the overall preparedness strategy.

For a critical operation to function in a disaster requires that all inputs to that operation function effectively. Rather than merely backing-up a computer system, all the elements in the value chain must perform and all the information and telecommunications links necessary for proper functioning must be available. Any link that breaks renders the chain ineffective. In practice this means that beyond ensuring computers are available, also ensuring that: Telecommunications networks are functioning; databases are backed up; software is available and compatible with equipment at the backup site; supplies are available; customer and supplier information is accessible including information about their backup sites in light of regional events; and most importantly, people are available and are trained. As outsourcing and supplier-partner relationships are becoming increasingly common, the preparedness plan also must take these linkages into account. Moreover, organizations should ensure that disasters at the outsourcing unit do not impact the home unit – for example, a fire at a supporting unit overseas affecting a U. S. based organization. Achieving the proper degree of support involves integrating event scenarios and business requirements. Given these, the backup architecture must be identified and implemented, and all auxiliary tasks such and pre-positioning supplies and employee training must take place. As with any plan, the preparedness plan must be well maintained and also tested, not only to identify weaknesses, but also to ensure the plan is congruent with changing business and technical environments.

To be effective, plans require trained employees. Employees involved in processing must be available at the auxiliary site and know how to function in that environment. A crisis management team consisting of business leaders, supplemented by technical managers and disaster management specialists, must also be in place. All team members must be trained, responsibilities must be communicated, and all supporting information and communications resources must be put in place at the emergency management center. Based on the vulnerabilities identified in other phases of preparedness, the crisis management team in advance would have drafted a strategy to respond to specific events and also have trained in "war room" settings for actual disasters.

Finally, the preparedness plan must be prepared and implemented. The University of Wisconsin Disaster Management Center (2006) suggests a five step process which includes many of the points discussed above:

> Step 1 is to determine, as discussed above via meetings with senior business managers, the objectives to be met in each affected sector;
> Step 2 is putting in place the strategies and approaches necessary to accomplish these objectives and to fill in any identified gaps;
> Step 3 is to document and implement the disaster preparedness plan – i.e., the formal document that specifies activities and the responsibilities of each participant;
> Step 4 is to ensure that strategic resources used in response to a disaster are pre-positioned and that relationships with auxiliary parties are specified (e.g., suppliers, customers, business partners, internal employees); and
> Step 5 is to train personnel in executing the plan and testing the plan via drills because a preparedness plan is of little value unless people have the tools, supplies, and training to execute it effectively.

### *Emergency Response*

Emergency Response includes those immediate actions taken to deal with a disaster or an emergency. We include in "Response" detecting the disaster -- obvious in some cases such as hurricanes and earthquakes, but for biological disasters, a significant activity (Helferich and Cook 2002). The emergency response phase should address the disaster or emergency itself, as well as the problems that are caused by the disaster or emergency. For example, in the case of a flood this phase would call for rescuing people from flooded buildings, and then housing and feeding them before more permanent plans are made in the recovery phase.

At the core of the emergency response effort is implementing procedures that tie together resources to achieve the immediate organizational objectives when confronted with a disaster. Most important is saving lives and ensuring the safety of all affected personnel. This includes that the proper safety equipment, evacuation plans, and linkages with safety authorities are in place, have been tested, and are operable. The well-publicized events in the aftermath of Hurricane Katrina in New Orleans illustrate much of what *not to do* in emergency response. Two internal FEMA reports in response to Hurricane Katrina and hurricanes in 2004, say (Jordan 2006):

> Both reports describe FEMA's blunders in trying to communicate and coordinate with onsite disaster responders, and get much-needed supplies such as food, water and ice to victims. Mitre, in early 2005, found FEMA was incapable of getting a clear picture of the disaster as it unfolded because it did not have a system capable of sharing information from the ground up. It also concluded that FEMA could not track supplies as they were being distributed. One unnamed employee interviewed for the Mitre report worried about holes in the tracking system, noting: "White House is asking, 'Where are the water trucks?' I didn't know. ... We don't have confidence that the trucks have checked in, arrived at the destination. We have to rely on third parties to tell us they have arrived." The February report noted that responders in New Orleans were unable to communicate easily and quickly with the emergency operations center in Baton Rouge because of inadequate phone and data systems. It also said FEMA's tracking system "was of little use."

This quote and the other well-documented problems illustrate the importance of successfully integrating four key elements involved in emergency response: Physical entities such as supplies, equipment, and facilities; people; information; and interfaces with external parties such as government agencies and also in the case of businesses, vendors and customers. Each of these elements presents challenges that must be met for emergency response efforts to succeed.

As a first step, an organization must decide where to locate emergency response facilities. For governmental organizations, this includes firehouses, EMS centers, and other first responder staging areas. One option that has been used successfully is to employ quantitative location models. Examples include: Modeling deployment of fire houses (Walker et. al. 1979, Police and EMS operations (Green and Kolesar 2004; Larson 1972, 1974, 2002) and strategies to handle biological attacks (Kaplan et. al 2002).

For businesses, facilities for emergency response include where to locate backup processing centers, for information and for business transactions. Three options are: To use dual, spatially separate in-house facilities – for example, as with Cantor Fitzgerald's London processing Center mentioned above which was used to process transaction in the wake of the September 11th attacks. The risk of backup center in one organization is that both might be affected by the same event, witness the northeast power outage of 2003 or potential events such as a biological or nuclear terrorist attack, a hurricane, earthquake, or pandemic which affects a broad area. The second option is similar to the first but involves two firms sharing a mutual backup agreement. This strategy often is more cost effective than the first yet the downside is that it places one organization at the mercy of another and raises issues regarding security of information and scalability for recovery in the aftermath of an event. The third option is to use a facility owner by a third party, such as a hot site for computer processing managed by a company such as SunGuard.

Given the selection of an offsite processing strategy, adequate supplies must be pre-positioned in quantities large enough to enable processing through the emergency response phase and into the recovery phase. Not only must the right supplies be in place in the proper amounts, but as a result of maintaining and testing the disaster recovery plan, the supplies must not be obsolete and must be functional. If pre-positioning supplies is unreasonable, agreements should be in place to obtain them in case of an emergency. Although agreements may work when only one location is destroyed, for regional incidents (e.g., earthquakes, hurricanes, and radiological incidents) the firms with whom the agreement is held may themselves be incapacitated.

Having the right number of people with the proper skills and training is critical to the success of any emergency response effort. Although invariably they rise to meet the challenges, people must be trained and have the proper tools to succeed. Moreover, they must be relatively unaffected by the disaster. A pandemic, radiological incident or other regional incident could degrade response, by the responders themselves being incapacitated.

A successful plan helps guarantee that adequate information exists and that this information is communicated effectively. Since the 911 emergency response communication system began over 30 years ago (Larson 2004) richer information has become available via wireless and now may be incorporated in many new and even existing systems (Curry et. al. 2004). GIS technology (Cutter 2003) provides a means of identifying the location of people and supplies and increasingly is being incorporated in many disaster recovery plans. Information underlying any emergency response plan includes a list of the individuals involved, contact numbers, and a enumeration of their responsibilities. Information systems can be used to increase the likelihood that emergency response plans work successfully communicating with the responders (Turoff 2002). Equally important are systems allowing ongoing communization between responders during an emergency, as well as communicating with other parties who may not be responders, yet that may need access to information about how the emergency is evolving (Odegard and Van Wyngarden 2006). Communicating with outside parties also is critical, especially given the interconnectedness of businesses on a local and global scale. This might start with a list of emergency response equipment suppliers and to facilitate recovery operations, expand to include supply chain links which must be intact, workable, and well-maintained.

### *Recovery*

The objective of the Recovery phase is to eventually resume normal processing. What is "normal" depends upon the processing objectives as spelled-out in the disaster recovery plan. For example, the overall strategy might call for a select group of critical services to be up and running immediately. Another group might take a week and for significant disasters, another group might take a month or more. In some cases the service might never resume. Regardless, the process should evolve according to the overall plan. Naturally the timing of when operations can resume and in what degree depends upon the severity of the event. For example, during Hurricane Andrew, BellSouth and Cellular planned ahead and secured over 100 cell sites, and lined-up outside vendors prior to the event, thus reducing the severity of the impact and shortening the recovery period (Blake 1992). On the other hand, Hurricane Andrew had a different impact offshore - some estimates indicated 45-60 days were needed to work off the backlog of recovery work on offshore rigs (Koen 1992).

Each event requires separate actions, and even the same event affects different types of businesses in its own way. Some events, like hurricanes, can be foretold and personnel can be evacuated. Others, like earthquakes, tornadoes, power outages, happen suddenly. Some events place humans at risk and others affect business but not human safety. Regardless of the specific event, during recovery each of the four issues discussed above in the "Response" section must be addressed: Equipment and supplies; people; information and communication; and links with suppliers, customers, and external parties.

Whereas in the emergency response phase one needs the proper equipment and supplies to begin processing on a limited basis, the recovery phase requires that they function for the full recovery period at the recovery site. The problems encountered often concern scalability. Initially triage might require that only the most critical transactions be processed and only the most important customers be served. Recovery means widening the scale to include all of the volume normally encountered, not only with respect to computer processing systems, but on a broader scale that includes the entire service delivery process (which requires integrating computer processing with telecommunications, people, and information).

Even given the safe evacuation of personnel, people issues are ongoing. For example, individuals rescued and working at a backup facility may still fell the trauma of the event itself; people may be affected by the safety and experience of other family members, acquaintances, or coworkers; employees who for the first few days expended "superhuman" effort during the response phase, may suffer burnout during the long term recovery period. The disaster recovery plan must not only include steps for physical recovery, but must also address the emotional stability of the workforce.

Two other key issues encountered during recovery concern long-term operations at the backup site being less effective than operations at the primary site, and ensuring that supplies, equipment, information, and personnel can support ongoing (and possibly scaled-up) operations. This means replenishing supplies, establishing communications on a the upgraded scale, housing processing employees and managers, interfacing with suppliers and business partners, and ensuring all information flow and storage requirements are being met. Finally the plan must also consider the move *back* from the backup site to the primary site!

## THE DISASTER RECOVERY PLAN

### *The Plan Structure*

The disaster recovery plan documents the steps for mitigation, preparedness, emergency response, and recovery. It is the result of a process that begins with senior management's awareness that a plan is indeed necessary, and ends with ongoing maintenance, testing, and if need be, implementation should a disaster occur. Cisco Systems (2006) provides steps in a "template" which reflects the general state-of-the-art: Pre-study, Management Awareness, Planning, Assessments and Audits, Priority, Strategy, Plan, Verification, Management Approval, Implementation, and Periodic Reports and Audits.

As noted, obtaining the ongoing commitment of senior business management is particularly important. Senior managers not only need to initiate and support the plan (which often consumes significant organizational resources), but are critical for obtaining priorities regarding which applications needs to be backed up in what degree and prioritizing regarding which applications need to be up and running and how soon. A second key element of the planning process is identifying likely disaster scenarios, planning for them, and identifying their likelihood of occurrence and subsequent losses if they do occur. Organizations need to address a broad range of scenarios because a plan appropriate for one disaster scenario may be inappropriate for another. This is especially true if people are not available, if records or equipment are destroyed, or for regional outages such as hurricanes and earthquakes, if suppliers and partners also are disabled.

### *Disaster Recovery Planning Software*

Specialized software can help structure thinking, highlight questions, and simplify a complex and often lengthy process. Helferich and Cook (2002) present a summary of disaster recovery software to assist in developing a disaster recovery plan:

| COMPANY | FUNCTION | SOURCE |
|---|---|---|
| BR Procative Inc. | Comprehensive planning process; a company adds its own critical information | www.brproactive.com |
| FEMA | Global Management System -- an online searchable database with links to web sites | www.app1.fema.gov.gems |
| Blule292, Inc. | Create and maintain web contingency plans | www.binomial.com |
| Disaster recovery Journal | Full range of disaster recovery providers | www.drj.com |
| TAMP Computer Systems | Provide a methodology, database management system and formatted recovery plan | www.drsbytamp.com |

In addition to this software, a brief sample of the multitude of disaster recovery-related software offered includes the following products for developing plans, GIS systems, and risk assessment:

| COMPANY | FUNCTION | SOURCE |
|---|---|---|
| Strohl Systems | Software to assist in building a plan | http://www.strohlsystems.com/ |
| XOSoft | Software for continuous processing | http://www.xosoft.com/ |
| SunGuard | Various software products in a suite to address various phases of disaster recovery process | www.sunguard.com |
| Dialogic Communications Corp. | Communicator! NXT is a GIS-driven software that provides remote access to digital, street-level maps for notification purposes. | http://www.dccusa.com/communicator-nxt.asp |
| Risk Wizard | Software suite to help businesses assess risks of all varieties | www.riskwizard.com |

## CONCLUSIONS

In their exhaustive study, Helferich and Cook (2002) state that "The typical large U. S. Corporation has given disaster preparedness a low priority because of competing business issues, the lack or recognition of the true level of disaster vulnerability and an assumption that the service and government sectors are responsible for disaster response." Indeed, a recent survey indicates that 19% of companies surveyed have no business continuity plan whatsoever, the primary barrier being perceptions that they cost too much (SteelEye 2006). These figures are disheartening because structured disaster management planning methodologies have been used for over twenty years. One reason "why" is that disaster management planning requires spending time and money to plan for events with very low probabilities of occurrence. Perhaps many managers are willing to take the risk because they underestimate the likelihood of occurrence of events and the magnitude of the resulting losses.

In some industries such as banking, boards of directors are responsible for ensuring disaster recovery plans are in place and as a result disaster recovery is a well-established process. In other industries where no mandate exists boards of directors and senior managers must take responsibility and implement contingency plans because doing so is good business practice. If any silver lining can be gleaned from recent disasters, it is that most people are now aware of why disaster plans are necessary and are aware of the damage that can be caused when they do not exist.

We believe that in the aftermath of recent disasters more businesses will develop, maintain, and test disaster recovery plans. Four trends will play a part:

1. *Increased business exposure due to the frequency, severity, and diversity of disasters; coupled with our dependency on technology*

Recent natural and man-made threats indicate that no business is immune from disaster. Because more potential events can now affect a business, disaster recovery plans for one event such as a fire, may be inappropriate for another, such as pandemic. Plans must be wide-ranging in scope and must be robust. Moreover, as we become more dependent on technology, the cessation of those technologies poses increased risks. This heightened complexity creates additional points of failure. The nexus between our greater reliance on technology and the increased likelihood that many businesses will experience a disaster event create potential losses far exceeding exposures of earlier years characterized by manual processing and a slower pace of business.

*2. Increased business exposure due to outsourcing and partnering*

More than ever before, organizations depend on other business entities, such as suppliers and business partners. Specialization and telecommunications and the ability to transmit large amounts of information accurately and quickly have led to many businesses becoming more "virtual." This poses two major risks: First, many suppliers and business partners must be incorporated in the planning process and into the plan itself. A second risk occurs when the supplier or partner itself suffers a disaster. For example, a 1997 fire at a Toyota supplier caused Toyota to close two plants, fall behind in production by 50,000 vehicles, and lose an estimated $149 million in operating profits (New York Times 1997). Organizations' dependence on suppliers and business partners is exacerbated by the trend toward globalization and outsourcing because the higher frequency of events and a less robust infrastructure in many less developed countries, and a lower level of disaster recovery planning in those areas.

*3. Increased business exposure due to customer expectations*

The flip-side of more businesses having sound disaster recovery plans is that customers expect higher levels of service when a disaster strikes. When the disaster strikes, if all businesses in an area are not operating, no one is disadvantaged relative to the competition. However, if all other competitors are operating any organization without a plan will incur direct losses due to the disruption and longer term losses due to the perception that the organization is poorly managed and undependable. No organization is an island -- in calculating its exposure one must consider competitive losses and in developing a strategy, one must be aware of the strategies of competitors, suppliers, and business partners.

*4. Technology as an enabler rather than disabler*

Though in many ways technology has exacerbated a business' exposure to disaster events, technology also is part of the solution. Thanks to technology, disaster recovery planning is quicker and more well-informed. A businesses strategy itself also can leverage technology. GIS is one example. Another is using cell phones in case of downed phone lines, enabling employees may work from home or from processing centers across the country or even in other areas of the world.

Many organizations now take planning for disaster as a given – a trend that only will increase. The challenge to managers is to blend the ongoing developments in processing and business operations with the capability to deal with disasters when they occur. To succeed, the basic elements of disaster recovery planning will remain the same: Committed business mangers; identifying and planning for specific scenarios; mitigating threats; preparing for disasters; responding to them; and recovering from them.

## REFERENCES

Atkinson, W (2003), "Enterprise Risk Management at Wal-Mart," *Risk Management*, (December), 20(12), 36-39.

Baskerville, R, (1993), "Information Systems Security Design Methods: Implications For Information Systems Development," *ACM Computing Surveys*, 25(4), 375-414.

Beacham, AE and McManus, DJ., (2004), "Recovery of Financial Services Firms in the World Trade Center, Post 9/11/01," *Information Systems Security*, (May/June) 46-55.

Blake, P (1992), "Recovering from Andrew's Wrath .. The Cellular Industry Fights Back," *Cellular Business*, Vol. 9 (December), 16-24.

Carrara, A., Guzzetti, F.Cardinali, M., Reichenbach P. (1999), "Use of GIS Technology in the Prediction and Monitoring of Landslide Hazard", *Natural Hazards* 20: 117–135.

Cisco Systems, (2006), *Disaster Recovery: Best Practices White Paper*, Document ID: 15118, http://www.cisco.com/warp/public/63/disrec.html.

CNN, (2003), "Major power outage hits New York, other large cities," http://www.cnn.com/2003/US/08/14/power.outage/, (August 14).

Curry, M; Phillips, D; and Regan, P, (2004); "Emergency Response Systems and the Creeping Legibility of People and Places," *Information Society*, (Nov/Dec), 20(5), 357-369

Cutter SL (2003), "GI Science, Disasters, and Emergency Management," *Transactions in* GIS, 7(4), 439-446

Ellison, RJ., Fisher, DA., Linger, RC., Lipson, HF. Longstaff, TA., Mead, NR. (1999), "Survivability: Protecting Your Critical Systems," *IEEE Internet Computing*, (November/December), 3(6).

EM-DAT (2006), http://www.em-dat.net/index.htm

Engemann, KJ and HE Miller, (1992); "Operations Risk Management At A Major Bank", Interfaces, 22(6), 140–149.

Green, LV. and PJ Kolesar, (2004), "Applying Management Science to Emergency Response Systems: Lessons from the Past," Management Science, August 2004, 50(8), 1001-1014.

Helferich, OK and Cook, RL. (2002), *Securing the Supply Chain*, Council of Logistics Management, Oak Brook, Illinois

Heywood, I., Cornelius, S., and Carver, S. (2002). *An Introduction to Geographical Information Systems.* Addison Wesley Longman. 2nd edition.

Hiles, A. (2004); Business Continuity: Best Practices--World-Class Business Continuity Management, Second Edition (Paperback), Rothstein Associates Inc.

Iyer, R.K., Sarkis, J. (1998); Disaster recovery planning in an automated manufacturing environment, IEEE Transactions on Engineering Management, 45(2), 163-175.

Jordan, LJ (2006), "Latest review of FEMA echoes pre-Katrina advice," http://seattlepi.nwsource.com/national/265347_katrina05.html, (April 4).

Kaplan, Edward H., David L. Craft and Lawrence M. Wein, (2002), "Emergency Response to a Smallpox Attack: the Case for Mass Vaccination," PNAS, 99(16), 10935-10940.

Koen, AD. (1992), "Time Required for Gulf Restoration Uncertain," *Oil and Gas Journal*, 90 (40), 26-28.

Kovacs, P and Kunreuther, HW (2001); "Managing Catastrophic Risk: Lessons from Canada," Institute for Catastrophic Loss Reduction (ICLR) Research Paper No. 13; (April); Institute for Catastrophic Loss Reduction: Toronto, Canada.

Kunreuther, HW (1996); "Mitigating Disaster Losses through Insurance," *Journal of Risk and Uncertainty*, Vol. 12; 171-187.

Larson, RC. (2004), "OR Models for Homeland Security," OR/MS Today, 31 (6), Larson, RC., (1972), "Urban Police Patrol Analysis," Cambridge, Mass.: MIT Press.

Larson, RC., (1974), "A Hypercube Queueing Modeling for Facility Location and Redistricting in Urban Emergency Services," *Journal of Computers and Operations Research*, 9(1), 67-95.

Larson, RC., (2002), "Public Sector Operations Research: A Personal Perspective," Operations Research, 50(1), 135-145.

Lewis Jr.,W, RT Watson, and A Pickren. (2003). "An Empirical Assessment Of IT Disaster Probabilities," *Communications of the ACM*, 46(9): 201-206.

Maslen, C (1996); "Testing The Plan Is More Important Than The Plan Itself," *Information Management & Computer Security*, 4(3); 26–29

Mileti, D (1999), *Disasters by Design*, Joseph Henry Press: Washington D.C., 161-65.

Miller, HE and Engemann, KJ. (1996); A Methodology For Managing Information-Based Risk; *Information Resources Management Journal*; 9(2); 17-24

New York Times - Anonymous (1997), "Toyota Output Hurt By Fire at Supplier," *New York Times*, (February 7).

Odegard, L. and van Wyngaarden, R, (2006); "The Best Of Both Worlds In Reilly, Jim (2005); "At MISO, Emergency Drills Mean Communications," *Transmission & Distribution World*, (May), 57 (5), 35-41

Smith, JM., (2000); "Reducing Uncertainties with Catastrophe Models," *Risk Management*, 47(2), 23-26.

SteelEye Technologies (2006), "SteelEye Business Continuity Index," www.steeleye.com.

Tsihrintzis, VA Hamid, R , Fuentes, HR, (1996), "Use of Geographic Information Systems (GIS) in water resources: A review," *Water Resources Management*, Issue: Volume 10, Number 4, (August), 251 – 277

Turoff, M. (2002); "Past and Future Emergency Response Information Systems," *Communications of the ACM*, 45 (4), 29-32,

University of Wisconsin (2006), "Lesson 2: Prerequisites for Preparedness Planning, University of Wisconsin Disaster Management Center," http://dmc.engr.wisc.edu/courses/preparedness/BB04-02.html.

Voelkert, C, (2006), "Achieving A Balanced Fire Protection Plan," *Occupational Health & Safety*, February, 75(2), 32-94.

Walker, W, J. Chaiken, E. Ignall (eds.), (1979), "Fire Department Deployment Analysis," North Holland Press, N.Y.

Wallace, M., and Webber, L. (2004); The Disaster Recovery Handbook: A Step-by-Step Plan to Ensure Business Continuity and Protect Vital Operations, Facilities, and Assets (AMACON)

Whitman, ME., (2003), "Enemy At The Gate: Threats To Information Security," Communications-ACM, Volume 46, Number 8, 91-95.

Wong, FL.; Geist, EL.; Venturato, AJ. , (2004), "GIS Development of Probabilistic Tsunami Hazard Maps," *American Geophysical Union, Fall Meeting 2004*, (December) abstract OS23D-1343

Zsidisin, GA., Ragatz, GL., and Melnyk, SA. (2003); Effective Practices in Business Continuity Planning for Purchasing and Supply Management., The Eli Broad Graduate School of Management, Michigan State University.