A review of Disaster Management with special focus on its Threats and Strategies.

Dr. Vijay Prakash Srivastava
Associate Professor
Department of Commerce
Pt. LMS Govt P G College, Rishikesh,

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 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. 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 2012, Soloman Islands, Northern Chili, and the earthquake in Indonesia and Philippines affected both life and property and emphasized our vulnerability to natural threats. During the natural disasters, figures compiled by the various national and international Agencies working in the sector of Disaster Management are :

- The number of natural disasters were 1570, up from 1290 the year before. The number of floods increased by 91 per cent in 2008 (258 in 2008 and 492 in 2011) and droughts by about 82 per cent (23 in 2008 and 42 in 2011).
- In total 339 million people, more than eight million in 2011 required immediate assistance, were evacuated, injured or lost their livelihoods. Despite this, loss of life (98,200) was significantly lower than in 2008, during which 359,200 people died as a result of natural hazards (a large portion due to the Indian Ocean Tsunami).
- Disasters in 2008 cost a total of $ 489 billion in damage, although out of this figure, $ 268 billion were losses caused by Chili and
Philippines. Notwithstanding, costs incurred from disaster damage rose by 82 per cent from the total $169 billion in 2011.

"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."

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.

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.

Preparedness

Preparedness prior to a disaster involves putting in place the various steps called for by the disaster recovery plan. Five general steps include:
(1) Identifying threats and given these threats, targeting various scenarios that might manifest themselves; (2) determining how a company will function if a disaster strikes, including which areas are critical and which are non-critical; (3) identifying suppliers and customers needed to continue operating and given these relationships, ensuring that contact lists and communications links are in place; (4) preparing for the possibility that business locations and supplies are inaccessible. (*i.e.*, pre-positioning supplies and using alternate facilities);
(5) 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. 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 ofpreparedness, 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 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):

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.

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.

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, 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.

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."

In some industries such as banking, boards of directors are responsible for ensuring that 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*

2. *Increased business exposure due to outsourcing and partnering*
3. *Increased business exposure due to customer expectations*
4. *Technology as an enabler rather than disabler*

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 managers; identifying and planning for specific scenarios; mitigating threats; preparing for disasters; responding to them; and recovering from them.

References

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.

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.

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).

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

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