Strategic Planning to Protect Information Resources in the Event of Disasters and Suggestions for Recovery (with Importance for Oman)

S. Arockiasamy[*], John D Haynes and Mohammed Al Rashdi

University of Nizwa, Sultanate of Oman

Abstract: A disaster can be defined as an often unexpected event, which has the great capacity for disruption for a business, corporation or government. Furthermore there is the likely longer term impact upon such organizations and governments. The disasters can take place in life at any time in any organization, but the recovery management and response time is very important. Developing countries like Oman should have a clear plan to handle these issues so that in future the survival and recovery becomes easier after unexpected events take place. The recovery plan as mentioned in many articles and papers will teach theoretical methodologies or ideas, but in general clear crisis plans and strategies will be more important and useful for many organizations to sustain their business/government without serious - or at least long-term - consequences. The reasons for defining a disaster or crisis is to establish a detailed plan or sets of strategies in relation to what constitutes that specific or general crisis. Furthermore certain technologies must be set in place to predict, monitor and aid in the recovery process. The essential point is to create circumstances where there is a minimization of the risks along with improvements in decision-making in preparation and in recovery for and of such disaster events. This paper is aimed at discussing and analyzing the issues related to disasters and recovery plans and consequent strategies and certain utilized appropriate technologies where such planning is important for Oman (who suffered a major natural disaster in 2007).

Keywords: Disaster Management, Strategic Planning, Recovery Plans, Risk Minimization.

1. Introduction

This paper is not about Oman, nor is it about an analysis of the Omani cyclone disaster in 2007, but this paper is of importance for Oman (to take note of for future disaster preparedness). A disaster can be defined as an often unexpected event, which has the great capacity for disruption for a business, corporation or government. Furthermore there is the likely longer term impact upon such organizations and governments [2]. A Disaster Recovery Management Plan needs to be prepared with continuity of critical business processes specifically within and beyond the disaster event. This management plan should facilitate an effective process of deriving a solution that can be used to recover all important business and government processes within the minimum time duration utilizing crucial records that are stored in different places (especially out of country on-line storage if possible). The derived plan should help people in a situation where they need to deal with emergency situations with these procedures. These plans might be generated and utilized individually but this will be useful to support people who are in need. The first plan should be the Disaster Management plan. This plan will allow organizations to handle difficult situations with many coordination activities during any crisis situation. This will also discuss the development, management and testing of the Disaster Recovery plan. It is very important that we must discuss the culture (and this is particularly important in Oman) and employee knowledge of the Disaster Recovery process. Basically, the issue "disaster" is not the same all the time since the disasters can occur in varying degrees. So, this plan has to be considered very seriously and must incorporate recovery procedures that entail management as well as technical details to save information and records without any problems. For example, consider the following plan by Patoli [7] who refers specifically to Medical Disaster Recovery [8], but for the purposes of this paper it has been paraphrased into more general terms.

Phase 1: Pre-disaster Preparedness. The first consideration is planning and development, and technological needs. In this planning stage, we can draw upon six categories of information that are crucial: management, surveillance, literature in terms of documentation and reports, logistical knowledge, personal, and community knowledge. The second consideration is the human factor. Patoli [7] indicates, and for our purposes, that the human factor is broken into four interrelated areas: management and administration, technical expertise and other related activities, IT users, and e-training. Four more major areas for Phase 1

---

[*] *Emails:* Arockiasamy@unizwa.edu.om, Johnhaynes@unizwa.edu.om

follow: databases, artificial intelligence (AI), Decision Support, Expert Systems, GIOs (Geographical Information Systems), and research projects [7].

Phase 2: Disaster Relief Operations. In this phase, responses are activated as immediately as possible after the disaster is detected. The main areas in this phase are: people tracking systems, critical situation telemonitoring through sensor devices, and management (including medical) through mobile technology, and decision support systems, and finally [7].

Phase 3: Post-disaster Rehabilitation. In this phase, it is possible that medical considerations such as people suffering from depression and stress need to be considered. The main areas in this phase are: public health threats entailing early warning systems, disaster recovery medicine, and general reconstruction procedures [7].
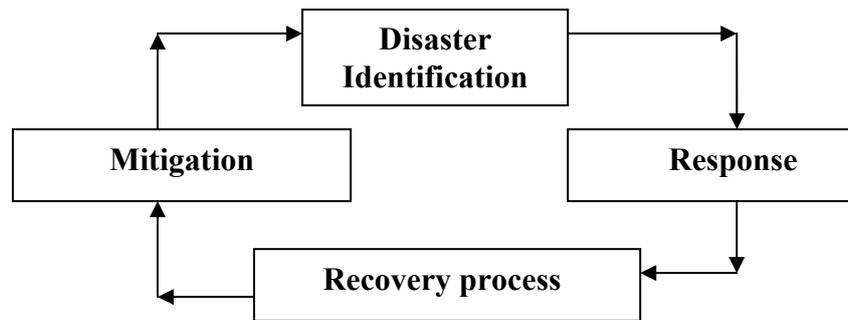

Figure 1: Disaster recovery cycle

The other key issue, which must be considered very strongly, is the disaster recovery strategy (a combination of Phase 2 and 3 as indicated above) but importantly in addition where alternate procedures are utilized. This plan should identify the use of alternative mechanisms from different sites (especially out of country, as indicated above), if the usual location is unavailable for providing the solution to the specific disaster. Moreover, consideration must be given to confirmation that potential risks have undergone reasonable detection measures within the processing environment. "***The most successful Disaster Recovery Strategy is one that will never be implemented; therefore, risk avoidance is a critical element in the disaster recovery process" [5].***

A System for the development of disaster recovery as an ongoing process of planning, developing, testing and implementing the recovery procedures must be enacted. Also, processes to ensure effective resumption of important business functions in the event of unexpected problems [3] should be effected.

Thus the following applies:

- Critical information identification
- Back-Up methods
- Recovery plans and tools
- Implementation methods
- Testing methods
- Maintenance plan and procedures

2. Background Study

Natural disasters (floods earthquakes, hurricanes, etc) are very difficult to prevent and measures such as good planning can certainly assist in helping reduce risks and/or avoid losses. Next, consider the disasters created by man (eg material spills, infrastructure problems, or all kinds of terrorism etc). Thus, in this case, surveillance planning is crucial in order to avoid or reduce the losses from those events.

Some examples of these types of disasters are as follows:
- A person, who lost a laptop with the only copy of his thesis
- A girl, who lost her research papers in the lab fire
- A Payroll system failed, a day before the salary day

- The recent tsunami or Gonu or earthquake etc

Most companies allocate a budget of between 2% and 4% regarding disaster recovery planning, particularly with loss of IT infrastructure and data in mind. According to current statistics, with a major loss of business data, 43% of businesses never reopen, and 51% close within a couple of years, with only a 6% long-term survival rate after the recovery. So effective planning requires significant investment of money, time and effort for ensuring the avoidance of losses, etc, in the event of disasters [4].

3. Disasters and Recovery Process

Proposed recovery measures will help derive a possible plan for any organization in the wake of situation where it demands a strategy to overcome these disaster problems. The control measures will follow various steps indicated below.

Prevention; **Detection; Recovery**. Note it needs to be ensured that these controls are always documented and regularly tested.

Suggested strategies for data protection:

- Backups are to be made and send to other sites included out of country regularly.
- Backups are to be made to disk in-situ and automatically copied to other sites.
- Precautionary measures must also be utilized with an objective of attempting to prevent a disaster.
- Generator back-up power supply is required.
- Preventions for fire or detection mechanisms.
- The utilization and maintenance of Anti-virus software plus other security measures.

Seven steps to recovery plan

- Top level management coordination

Top management must support and should be involved in the development of recovery process.

- Establish disaster management Team

Create a team for managing disaster and they must oversee the development and implementation of the plan.

- Perform risk assessment

Potential consequences and impacts by functional areas of organization

- Set critical system priorities

Identify and organize various threats and prioritize those logically and evaluate carefully.

- Design recovery plan

The content of the plan must include critical business functions and operations necessary to maintain.

- Train people

The training plan to reduce actions and make business continuity

- Communicate your plan

Provide recovery details to your business community

The recovery plan ensures the continuity of crucial business processes with respect to crisis situations, but top level management can use the recovery procedures and plans for further survival. Furthermore, the plan should provide for an effective procedure for control of all activities associated with a crisis situation without affecting the public and shareholders. There is a need, of course, to regularly update the plan by authorized staff with a Business recovery process in mind. There are two essential parts to the plan: identification and recovery. The former constitutes Disaster identification technology in the event that a disaster takes place in central area of data processing center. For Disaster Management an adequate technology must be developed, maintained, and exercised by organizations to survive without unnecessary difficulties. It is clear that very few people plan for their organization survival, and this should be strategic and tactical. However, the final corporate plan is a foundation upon which it was built for survival.

4. Some Specific Technologies for Disaster Management

Haynes et al [8] note that Artificial Neural Networks [9] can be very useful tools not only in Disaster Recovery but in assessing the possibility and extent of a disaster. One of the main constraints however, is the amount of time utilized to collect data, however Haynes et al [8] note at page 1307 [8]: "with advances in online real-time collection techniques, the advantages and future potential of ANNs is very promising". And while Haynes et als' comments applied to telemedicine, it is telemedicine within the context of Disaster Management Recovery. Furthermore Haynes et al [8] at pp 1306-1307 note other technologies that can greatly aid in Disaster management Recovery, such as GPS technologies, predictive Artificial Intelligence, advanced wireless sensor systems. Haynes notes at p 1305 [8] that "success or failure of a disaster response often is determined by timely access to communication and reliable information", hence these and other specific purpose technological devices are only as good as the up-to-date information that they possess.

5. Conclusion

We have considered what constitutes a disaster and accordingly we have identified key points of discussion and recommendations with respect to Pre Disaster Preparedness, Disaster Relief, and Post Disaster Rehabilitation in terms of recommended systems of disaster strategies. These strategies – of importance for Oman – referred to maintenance, testing and implementations and examples of types of disasters with consequence recommendations including a 7 step recovery plan. The fundamental idea of a successful Disaster Management plan, as we have explicated in the paper, is importantly, developed by people. Moreover, we have argued, the corporate Disaster Management planner needs to strategically and relentlessly manage the process. Hence the disaster planning is truly a crucial element of the over-arching business plan of any organization or Government. All of the recommendations in this paper are definitely of importance for Oman.

6. References

[1] Boroski, Doran. "Protect processes as well as investments in disaster recovery plans" http://www.computerworld.com/storyba/0,4125,NAV47_STO68345,00.html

[2] Jon William Toigo, "Disaster Recovery Planning: Strategies for Protecting Critical Information Assets", 2nd Edition, Prentice Hall, 2009.

[3] Radeke, Michelle "Prepare for Effective Data Backup and Recovery" http://www.workz.com/content/543.asp

[4] The Business Continuity Institute http://www.thebci.org/frametrial.html

[5] Wrobel, Len, "Components of a Successful LAN Disaster Recovery Plan" http://www.disaster-resource.com/content_page/nuggets.shtml

[6] Wold, Geoffrey H. "Disaster Recovery Planning Process" http://www.drj.com/new2dr/w2_004.html

[7] Patoli A.Q. Role of telemedicine in disaster management, *eHealth International Journal 2*(2), Retrieved February 5, 2008. http://www.ehealthinternational.net/

[8] Telemedicine and Information Technology for Disaster Medical Scenarios, Encyclopaedia of HealthCare Information Systems, edited by Nilmini Wickramansinghe and Eliezer Geisler, Volume III, MRI-Z, pp 1303 – 1310, IGI GLOBAL publishers, New York.

[9] Kumar, K., & Haynes, J.D. Forecasting credit ratings using an ANN and statistical techniques. *International Journal of Business Studies,* May 2004.