Disaster recovery planning as an element of risk management for natural disaster systems

Akram keramat

Faculty of science, Islamic azad university, dezfoul branch
E-mail address: a.keramat@iaud.ac.ir

Abstract

Recently, businesses have been losing tens of billions of dollars because there have been various natural and man-made disasters. However, the disaster recovery plan(DRP) and system that have been put in place have proven important means of reducing the risk of damages to businesses,in particular. The DRP can minimize and in some cases, eliminates the risks through technical, management or operational solutionst. However, it is virtually impossible to eliminate all risks. Information technology systems, for example, are vulnerable to a variety of disruptions from a variety of sources. In many cases, critical resources may reside outside the organizations control(such as telecommunications or electric power), and the organization may be unable to ensure their availability. This study propose a model for disaster recovery planning as an element of risk management. Thus, an effective disaster recovery plan in the form of contingency planning, execution and testing are essential to mitigate the risk of system and service availability. We have developed a global model for disaster recover planning and management known as the dream model which can be customized and applied to a variety of disasters prone systems such natural, imergency, IT/network/security, data recovery and incident-response systems. The main aspect of this model has been currently used and evaluated in departments in IRAN. Our approach to data collection and evaluation include a combination of ethnography, grounded theory, and questionnaire , which we believes , is more effective .

Keywords: *Disaster preparedness, Recovery/Reconstruction, Risk identification, Emergency management*

1. Introduction

It is widely know that many businesses have in the last few years suffered greatly and lost tens of thousands of dollars on account both man-made and natural disasters. Man-made disasters have included: the bombing of the world trade center and government buildings as well as the corruption and damage to various information technology systems and their data, information and processing. Natural disasters have included: the earthquakes in southern California and san Francisco bay area, hurricane hugo and Andrew and floods in the mid-west.(1) .

Disasters like these could clearly take place in the future and it is for this reason that one needs to consider if the incorporation of a disaster recovery plan(DRP), and system could be an effective means of protecting businesses from different types of disasters. It is possible to argue that all businesses and information technology departments should be involved in disaster recovery planning,implementing, testing and updating. Furthermore, the use of DRPs should be encouraged so that in time all information technology departments come to accept such systems as a necessity. At times,certain information technology and automated

information systems are prone to interruptions that can greatly disrupt the efficient running of such systems.

If the information technology contingency plan was to be adopted by businesses, this problem could be resolved and this would put in place useful technical procedures that ensure systems recover quickly from any troublesome disruptions.

It is the DRP that determines what planning practices should be implemented by businesses in order to creat an efficient information technology contingency plan. Although such practices are on the whole sufficient for most business,it is important to acknowledge that some businesses may need to make use of other practices to deal with certain extra needs.This article does not take into account the DRP for supercomputers and wireless networks, but even so that majority of the practices put forth are applicable to these systems.Our earlier work has focused on a more generic mode for emergency-response system and contingency planning for natural disaster and IT.

2. A model for disaster recovery planning and risk management process

Risk management has been widely used in various projects. However, risk management for NDS is more complex and harder to predict contingencies. Therefore, this section aims to structure DRS as part of risk management process for NDS.

A variety of procedures is adopted to appropriately identify,control and reduce risks to information technology systems. Fallara(2003) has proposed a similar approach to disaster recover planning as part of the risk management as they are crucial to any disaster recovery. However, we have proposed a more structured approach to disaster recovery planning as an element of risk management.In order to effectively manage risks to information technology contingency planning, it is necessary that the following risk management actions are taken: firstly, it is important to investigate whether the concerned system has any weaknesses that could lead to it being damaged or destroyed and subsequently to take the required precautions. There are three types of threats in particular that could harm weak or insecure systems:

- Natural: this includes fires, floods, tornados and hurricanes.
- Human: this involves terrorist attacks, human mistakes and risk from hackers.
- Environmental : this includes software gaining errors,equipment ceasing to work and power failures.

In this work, we have developed a global model for disaster recover planning and management known as the DREAM model which can be customized and applied to a variety of disasters prone systems such natural, emergency, IT/network/security, data recovery and incident-response systems. The main aspect of this model has been currently used and evaluated in departments in Iran. Our approach to data collection and evaluation include a combination of rthnography, ground theory, and questionnaire, which we believe, is more effective.

Secondly, it is essential to asses any residual risks in order to form an effective contingency plan . Figure 1 shows disaster recovery planning: which shows the process of putting into place the necessary security precautions, forming a contingency plan and putting the DRP into action when any incident occurs. It is important that analyses of risk to information technology systems are taken to ensure that the risks to information technology systems are properly identified. In this way, it is possible for risks to be allocated with a risk level that

predicts how high at risk systems are to various threats and how serious such threats may be to systems.

The measures put in place to deal with risks clearly have to be constantly examined and updated by the people in charge of information technology contingency planning since information technology systems may constantly be forced to face new dangers from various threats. Information technology contingency planning involves a large range of measures than DRP to help information technology systems survive disaster. In particular, information technology contingency planning need to be focused on guaranteeing tat organizations and businesses are able to survive disasters as well as lans for ways of dealing with any disasters that may hit information technology systems,businesses process and facilities. Although there has been no general consent on what would constitue effective information technology contingency planning, the fact that there is an inbuilt link between information technology system and business processes shows that every plan should take into account the two at the same time to ensure that the two work effectively alongside one another. Generally , Figure 2 shown the disaster risk management process(cycle).

The DRMP consist of four main processes/stages such as identifying and analyzing risk,etc.explain the diagram as it appears on the picture and then discuss sub-processes/stages within those categories. It is composed of following main elements:

- Risk location and examination: this involves assessing the cause, nature and behaviour of the threat and in particular, determining how serious it.
- Knowledge management: this involves raising awareness about potential risks, putting in place education and training programs, extensive research on ways of preventing disasters.
- Political commitment to a disaster reduction policy: this includes ensuring that laws are drawn up to ensure that such policies are adhered to.
- Taking active measures to reduce risks: this could include planning and building protective structures like dams and dikes.
- Cautionary methods for disasters: this could include ensuring that people are supplied with the knowledge and information required to take the necessary precautions against disasters.
- Preparation for disasters: this include making sure that people are able to cope with any disaster that may occur. For example, this could involve creating a suitable plan to evacuate people from buildings.
- Repairs and rebuilding: this includes seeing to it that areas that have been hit by disasters are repaired and that the people affected by disasters are given the required assistance so that they may deal with whatever situation they may be in .

The above main elements can lead one to conclude that disaster recovery management involves firstly actions taken prior to a disaster. It is essential to assess what risks businesses or places may be prone to and to put in place the required measures to ensure that businesses and places are defended effectively against such risks. Secondly, disaster risk management involves actions taken at the time of a disaster including assisting those areas and people involved in disasters. Thirdly, it must involve taking action after disasters occur and it must ensure that the necessary repairs and reconstructions are put in place to improve the areas hit by disasters. It is essential to take into account the technical capabilities, costs and the social and environmental consequences when assessing ways of reducing risks.(1) and not just the

actions taken prior to disasters, which is at times the only concern of disaster risk management. (2)

The business continuity plan(BCP) and disaster recovery planning (DRP) strategies. The business continuity plan may be designed generally for all the main business processes or specifically for a single business process. It also takes into account the value of information technology systems to business processes.

Although the DRP does not take into account small disruptions that information technology contingency plans often treat,it does very often include a plan designed for information technology systems and can be used as a way of restoring target systems, applications or facilities in more suitable locations. If required by a business or organizations, several DRPs may be included with the BCP. Risk management template is one of the structured means of identifying risk elements, impact factors and relevant actions required .(table 1)

Our impact factor consist of a number risk levels:

Critical which is a highest form of a risk and therefore immediate action is required.

- High
- Medium
- Low

3. Effective disaster recovery plan DRP

It is clear that teamwork is essential for the creation of effective disaster recovery programs. This section proposes disaster recover plan,which is essential to structure DRP activities. It is essential that teams working on such programs must adhere to health and safety guidelines and must be briefed. On exactly what the requirements are for the businesses or systems that need protection from disasters. It is crucial that teams also take constantly monitor what protection is needed by examining whether there are any new potential threats: this means that teams must constantly be assessing whether the resources they have to deal with disasters are sufficient for creating effective disaster recovery systems.

It is important that there are three separate phases of disaster recovery planning. It is essential that there is one team that examines what requirements are needed to prepare systems and businesses for disasters. Another team that actually puts in place and manages a disaster recovery plan; and a third implementation team that carries out the action. Figure 3 shows DRP team management and the detailed phases are:

- Phase 1 requirements what is meant and what is to be done
- Phase 2 team to creat and manage a disaster recovery plan
- Phase 3 implementation team to take action

It is essential that an assessment is made of what sort of skills need to be possessed by the team members of each phase and also what resources are required by every team. A coherent structure also needs to be put in place so that every team know exactly what is objectives and responsibilities are; this is essential for the smooth and effective running of the disaster recovery plan. Various developments to the traditional hot site disaster recovery business took place in the 1980s, which was partly due to the fact that compute hardware was becoming cheaper and that technology was centred largly around personal computer.

Although these plans in the 1980s were able to deal with the use of mainframe computers, it was not until later that plans were put in place to take into account communications networks.

Indeed the plans designed today differ greatly from the 1980s as it is now a requirement that managers prepare themselves for any potential risks and computersystems need to be able to operate at all times. This means that if any disaster should occur,it is essential that the systems affected are restored in a number of hours instead of days and that any lost date is fully restored.

Such changes are mainly due to various government regulations, union contracts and the damends from customers. Today,technology plays a massive role on most businesses with various companies having both local and remote basis connections to their main computer.

4. Evalution and validation of the model

This section will explain the evaluation model was conducted those who were involved realized the different situation emerged from involving different types of participants. According to fledrich, et al 2007 focuses on gathering data about the usability of a design or product by specific group of users for a particular activity with a specified environment or work context. The environmental problems can be considered as a contributed element of causing instability. It hinders economic developments;displaces populations;contributes in the increase of weapons of mass destruction;and enhances the growth of undesirable elements.

As far as Iran is concerned, it is considered one of the most environmental troubled regions. It suffers from water shortages, hazardous materials, oil spills in the gulf, shipping incidents and transmission of new diseases. Disaster recovery management activity model and the contingency and continuity-planning model for recovery actions have been discussed in interview questionnaire. The requirements of workforce safety will be also explored. In addition to that, advices suggestion on how the emergency managers could be developed, and yhe way to creat excellent communication and co-operation with involved organizations and individuals will be presented. This model provides an explanation of the use of emerging technology, the role of people and their culture, and global support.

It is vital to understand and analyze the operation of power within the context of evaluation in order to identify the approaches, tools and methods which can contribute in improving the practice of information system evaluation. According to the questionnaire, less that 25% of the managers believe that the organization did very well in handling the disaster contingency and around 14% only said the organization very poor in handling the disaster contingency.(Figure 4)

This paper encourages emergency managers to apply business continuity plan and disaster recovery plan along with other newer technologies in the work . It offers ideas and possible actions, which can be adopted by the emergency managers when dealing with disasters.

For that reasons, the paper will present issues such as business continuity plan(BCP), disaster recovery plan(DRP), workforce, education, information technology facilities and insurance.

It gives example of how to apply business continuity plan and disaster recovery plan t lowest cost.

5. conclusion

Today disaster recovery plans have developed significantly since their early days when it was the company data center that provided the most protection.

They are now able to ensure that all the main operation components are protected by the innovative usage of a corporate-wide risk management approach. Many lives and vast amounts of money can be saved if disaster plan is designed, so long as all the phases of the planning procedure are stuck to and developed.

Indeed emergency and security management programs may only be truly effective if the plan is properly designed. Teamwork ad cooperation between all members of an organization is essential for preventing disaster and it is clear that good contingency business planning effectively depends on everyone preparing for disasters and responding immediately to them .

6. References

1.Espone monitoring committee.,2005, the spatial effect and management of natural and technological hazards in Europe

2. Fallara,p., 2003, disaster recovery planning, IEEE potential,vol 22, issue 5

Table 1. Risk assessment template for recovery plan

Critical aspects	Impact factor	Recover/contingency plan	Team responsible
Evacuate people from the place of incident such as a building	Critical	Call emergency evacuation team of professional experts	Establishment manager

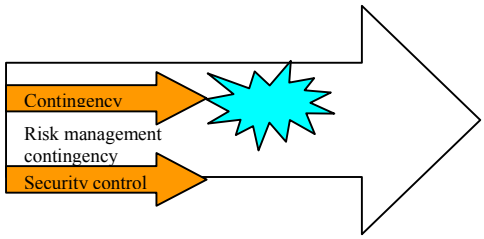

Figure 1. disaster recovery planning

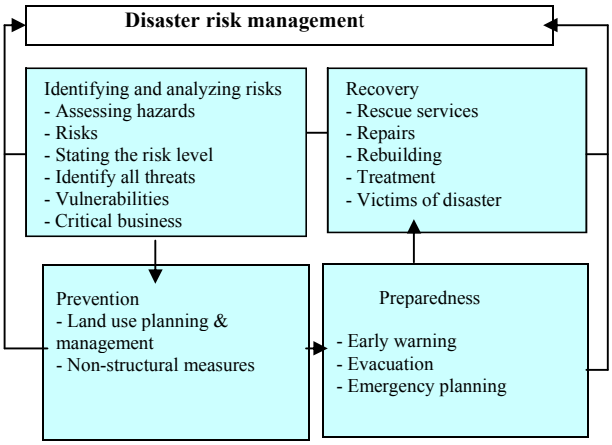

Figure 2. The disaster risk management process

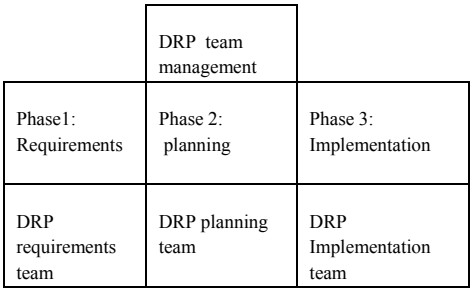

Figure 3 . Effective disaster recovery planning cycle

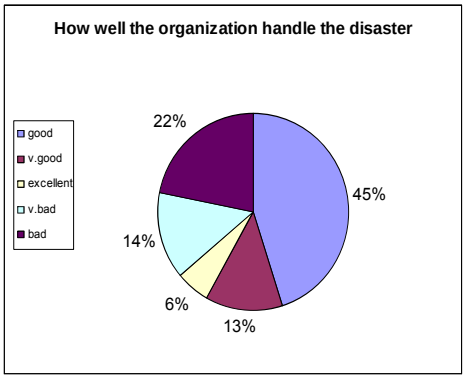

Figure 4. How well the organizatio handle the disaster