CHAPTER VII

DISASTER RECOVERY PLANNING

Overview

Most organisations who have computerised their operations are no longer mere users of computers. They have become dependent on it and the failure of the computer operation would result in business interruption. It is always generally believed that catastrophies and disasters will affect other enterprises and not us!

There are any number of instances where unanticipated contingencies have occurred and businesses have got interrupted. The importance of disaster recovery plan and contingency planning can never be over-emphasised. To take the example nearer home, in February 1994, the Reserve Bank of India’s National Clearing Centre at Nariman Point had a breakdown of the computer system. The press report stated that "according to sources, the breakdown in IBM’s micro-processing-stated to be major in nature, was reported on Wednesday afternoon and necessitated a total shutdown of the sophisticated system. Since the system cannot be said to be set right till Thursday, Banks all over Bombay were advised against sending more cheques for clearance.

Clearing of cheques of more than Rs.1500 crores came to a standstill following a two-day old breakdown in the computer system. Oral requests were made to representatives of various banks in the city arriving with bundles of more than 10,00000 of cheques to take them back but without setting any reason for the same,
mystifying the banking circle in the city. It was reported that a team of engineers were being flown from Calcutta. Till Friday evening, no progress was made other than detecting the fault. While other matters of detail are of no relevance, it is of significance to note that even an institution like Reserve Bank of India had no disaster recovery planning!

Whether a disaster is natural such as earthquake or a hurricane or unnatural event such as an electrical overloading sparking a fire or normally anticipated situations of failure of hardware or failure of environmental support services. Management of those who have the responsibility for processing information on computers should have a well-tested plan for meeting such emergencies.

PROBLEM AREAS

The information technology at tremendous pace and the awareness of the advantages of utilising information technology for decision making purpose, apart from obtaining information from vast volume of data, all organisations have gone in for computerisation of different types. This has made organisations dependent on computers with the result, that such organisations would be handicapped in some way or the other, should a disaster occur.

In our country also the job opportunities and career possibilities in the information technology is occurring so rapidly with the result, turnover of personnel has become more a rule than an exception.

A study of the present scenario in general reveals that while organisations had realised that disasters can occur, there is a certain sense of complacency, arising out
of the illusion that calamities will strike only their neighbours. The documentation standards for systems and programmes are generally incomplete if not outdated. With the documentation standards, being unsatisfactory and the personnel turnover factor being high, organisations do face problems. It is due to a few dedicated old hands that the systems are running. Added to this common problem, there is no attempt made to plan for a contingency. There are no studies made as to how long an organisation can continue without a computer before business interruption occurs. Should the problem persist longer than organisations can withstand, what are the arrangements to be made. There have been no attempts made to prioritise critical applications. The utmost recovery plan that is in existence is copies of most of the programmes are made and that too stored in a separate cupboard. The cupboard is mostly in the same computer room and sometimes with the manager of the department in his cabin which is located in the same building, if not in the same floor.

Uninterrupted power supply systems (UPS) are in existence. Fire extinguishers are fixed in different locations of the computer room. Pitifully there is no continuous training given to personnel in fire-fighting. Internal auditors do not even consider it as part of their duty to see whether the fire extinguishers have been refilled.

The basic precaution of ensuring that inflammable material is not stored near or around the computer room is not observed. Thermacole boxes or thermocol material which arrive as packing material for the hardware and software is stored in the computer room itself if not in the computer library. Computer rooms in many instances do not have containerised air-conditioning. The same air-conditioning ducts run through the building as also the computer room in many instances. While open
fire may not exist in the computer room, burning of camphor on Friday evenings in different parts of the offices is not an uncommon situation.

For convenience the computer division in many instances is situated in the ground floor. While precautions are taken that water does not flow through the drain pipes and water culverts, the possibility of water inundating the computer room from clogged culverts of neighbouring organisations during rainy season is not taken care of.

The necessity for having a documented plan for disaster recovery is not appreciated, as spending effort and time "on an unlikely event" seems in their opinion futile.

The concept of insurance cover in a computerised environment as it exists now is to provide an insurance cover to the extent of the cost of the hardware purchased. In some instances, if expensive software has been purchased that cost also is included. However, the total cover for insurance in the eventuality of
i) Program being lost
ii) Program data being corrupted
iii) Fraud occuring due to failure of software
iv) Connected costs of restructuring data files
v) Loss of business due to non-functioning of the computer whether due to hardware or software fault.

Amongst other disaster due importance should be given also to the impact of an attack from virus, specially in a PC environment or a net-worked environment. There is a great vulnerability to attacks from virus. While there is knowledge about the
existence of virus, steps necessary to prevent attacks from viruses is not adequate. Instances are many when some steps are taken after an attack of virus. While the systems department does take some steps though not adequate to prevent viruses auditors are totally ignorant in their knowledge of viruses, its impact of attack of virus on computer information and programmes and steps to be taken as a precautionary measure.

In the data collected, on the assurance that anonymity will be obtained. The following information was available.

In one of the large public limited organisations which had offices all over India, the computer room was flooded with water due to overflowing of the drainage in the neighbouring building due to rain. The water level under the false flooring was namely 5 to 6 inches. The organisation bailed out the water with mugs and buckets. As already the computer installation was down for three days soon after the bailing out of the water was completed, the current was switched on wanting to use the computer henceforth. There was a short circuit due to the dampness and there was damage to the hardware and of the programs which was on the hard disk. The organisation struggled for a week to ten days recreating software and negotiating with hardware suppliers for replacement.

In one of the leading foreign banks in Mount Road, Madras certain modems and about 40 terminals were burnt out due to lightning striking one of the cables running through the open yard of the bank. It is needless to mention the crisis that the bank had to manage.

In another organisation data used to be entered into the floppy at the flock free and sent for processing to the head office 25 kms away. Several days data was
lost as the data was being transported without adequate protection in ordinary cardboard boxes in an auto rickshaw which had the motor on the reverse. The magnetic field created by the motor erased all the data which was realised only much later.

In yet another organisation which prided over the fact that it has got back up for all its programs and files, the entire operation was paralysed for more than two months. This was due to the fact the sudden rains inundated the computer room which also used the duplicate copies of the programs and files!

In another organisation due to uncontrolled and unexpected power supply problems the disk was scratched. The organisation immediately unloaded the disk opening the duplicate copy of the programs and files. The source of the problem not having been set right the disk which contained the duplicate copy was also scratched. Loss of files due to attack of virus were very many. In most of the cases where disaster strike, there was no recovery plan. The problems and crisis were only discussed in private as organisations felt that there will be loss of image. It was officially reported.

STANDARD ACCEPTED PROCEDURES

When a disaster occurs, an organisation which is well equipped to face it is able to resume normal operations by following a pre-determined recovery strategy. It is interesting to recall the California Federal when a disastrous earthquake struck California. Internal Auditor, Mr. John G. Burch, in his article Disaster Recovery Plan on moral and professional responsibility describes the experience "Calfederal". There was no time for installation to have a graceful degradation, the system is
reported to have gonedown inelegantly; they were taken totally by surprise. It is
reported that CAL FEDERAL employees under the direction of Senior Vice
President of Computing & Communications of CAL FEDERAL were able to activate
the Contingency Plan within one hour after 29 hour non-stop recovery work;
everything was back to normal. Soon thereafter there was a second earthquake; the
contingency plan had included a "HOT SITE". Hot site is a back facility which is a
computer installation which is fully equipped and is more or less a duplicate of the
existing installation. CAL FEDERAL after its second disaster recovery plan
recovered in nine hours. It is reported that the Vice-President stated that a lot of
data processing Managers, thought it won't happen to them, but I was not singled out
by God; It is a moral responsibility to have a plan.

Yet another reported case is of a Computer Centre which survived in 1992
Los Angeles riots due to the existence of an effective disaster recovery plan. Riots had
started in Los Angeles; there was extensive looting and fires were widespread. It is
reported that... the data processing centre survived the emergency unscathed".

Analysing the reasons for a successful survival of the DataCentre:

(a) Data Processing Centre had plan for emergencies

(b) Had a comprehensive and well documented contingency plan to be used in the
course of a major earthquake, as after all earthquake was another type of
emergency. This contingency plan worked out even in this type of emergency.
The plan even included stocking "earthquake bags" which contained food and
other essentials for the employees".

(c) The computer site had effective security. The first two floors had no glass and
it had no public lobby. No casual visitors were allowed entry into the building.
Linda Larsens concludes that the Los Angeles Data Processing Centre survived a major urban riot because they were well prepared for an emergency.

As against the above two instances, an example nearer home highlights a situation within our country. The Reserve Bank of India's National Clearing Centre at Nariman Point, Bombay had a breakdown of their computer for four to five days. The system could not be set right and several lakh cheques worth several crores remained stagnant. Instructions were given to bankers to prepare themselves for manual clearing as the "Clearing system was malfunctioning". It is not always that a disaster occurs but one should be prepared for the same with an effective disaster recovery and contingency plan. There should be standard policies and procedures issued by the Management covering the following aspects:

i. Contingency Planning Process
ii. Risk analysis
iii. Strategy for contingency planning
iv. Documentation
v. Testing
vi. Risks and controls
vii. Audit considerations

The need for Management's awareness for a contingency plan should and is arising out of the following factors:

i) Information is a valuable asset of the organisation
ii) Unlike previously computers are spread all over the organisation.
iii) Organisations are depending upon computers and not mere users.
(iv) Computers capability to contribute to decision-making process.
CONTINGENCY PLANNING PROCESS

As the adage "Prevention is better than cure" goes, it is better to have preventive measures to avoid a disaster rather than struggling after a disaster to bring normalcy. The preventive steps may be classified under the following three heads:

(a) Organisation
(b) User involvement
(c) Administrative procedures

(a) Organisation

The most important step is to have a team which has:

(a) Centralised responsibility
(b) Adequate visibility
(c) Appropriate authority

It is necessary that there should be one leader who is the primary responsible authority for co-ordinating and maintaining the contingency plan. It is essential that all the departments in the organisation are made aware of the fact that the organisation is intending to develop a contingency plan. As the users and the departments are made aware for the need to have a contingency plan, awareness for potential risks is spread. As the project leader has to liaise with the different departments, senior management should vest the project leader with appropriate authority and communicate the same to others in the organisation.
(b) User involvement

Users should be closely associated with the development of contingency plan. They should be involved in assessing the risk resulting from a disruption as users are the best judges and they would be able to assess the associated risks better. The useful functions that the users could perform would be:

(i) Make analysis

The users should evaluate the impact of the failure of computer systems on their business function. They should make a fair assessment of their time when they can manage without computer processing. Users must be closely associated in the process of identifying and prioritising critical applications.

Users and the system staff need to work very closely to decide on procedures in the case of a computer breakdown and also the procedures which need to be adopted to get back to the computer systems.

Administration

As already mentioned one person should be selected as the leader; his responsibility should include developing a planning methodology, develop plans to implement the policy especially an organisational structure, training the staff, reviewing the process and reporting to the management, maintain the plan, co-ordinate the others involved in deciding the plan. A planning methodology should be used to ensure quality, security, consistency, comprehensiveness and maintainability".
Risk Analysis

It is extremely important to identify and prioritise critical applications. The applications which need to be restored and the order in which they need to be restored should be settled.

The factors which contribute to the criticality of the applications are need to be studied carefully.

The next step would be to evaluate the threat of disaster to the computer facility.

ANALYSIS AND FINDINGS

A sample survey of 30 organisations was conducted. The questionnaire utilised for this purpose is enclosed. (Table 8.1) The response from all the 30 organisations was analysed. The information was personally gathered by me from the organisations. In addition, had a discussion with the five leading firms of auditors to ascertain the audit procedures followed in connection with the Disaster Recovery Plan of their clients' organisations which were extensively using computers for preparation of management information as also financial statements for audit certification. (Table 8.2) The findings as gathered from the sample of organisations surveyed are as follows:-

(i) There were no standard policies or guidelines for the organisation regarding contingency plan or DRP.

(ii) None of the organisations had any remote safe background storage vault for storing the programs systems, documentation or important data.
(iii) None of the organisations had an insurancy policy which covered anything other than the cost of the hardware.

(iv) None of the organisations had applied their mind regarding the legal responsibility that may arise for non-performance should a disaster strike the organisation. In the absence of any DRP or policies or procedures provided by the management, there was no documentation for DRP.

(v) All the organisations had copies of the programs backed up. However, these programs were not stored in most of the cases in a remote place away from the computer installation.

(vi) In most of the cases, the computer programs and critical data were copied and stored in the systems manager's cabin which was part of the computer department.

(vii) In most cases it was also found that thermocol packings and cardboard boxes which were arrived with peripherals or computer stationary were stacked near or around the computer installation without the least awareness that these being combustible material should never be stacked near the computer installation.

(viii) There were no documented evidence regarding key personnel to be contacted in case of a disaster.

Informal discussions provided the information that the organisations did have situations when disasters did strike them in the following areas:-

* Disk crash
* Virus attack
* Water leakage
* Hardware failure
Software getting corrupted.

In all the above situations, the organisations did have problems and they resorted to a "Crisis Management". Strangely this had not resulted in any permanent action being taken by way of formalising the DRP and contingency plan.

Apart from these findings, survey results of Messrs Coopers Lybrand are enclosed. (Table ) These findings are no reported cases in our country. There are no reported cases as yet of loss incurred due to disasters striking the organisations. However, it should be noted that there were blasts in Delhi, big fire in multi-storeyed building which affected amongst other organisations Bharat Heavy Electricals Limited, earthquake in Bombay and bomb blast in Bombay which affected any number of organisations and their computer operations. In Madras, lightning struck a multi national company which affected more than forty terminals. More recently hardware problems in the Reserve Bank of India clearing House operations is a case in point.

AUDIT

The discussions with the auditors revealed that their areas of operation and activity did not include evaluating the adequacy of a DRP. This has been confirmed also by all the 30 organisations which were included in the survey. The auditors have been ignorant of the need to review the adequacy of a DRP. The auditors while they are aware that they need to value all the assets and certify their existence, somehow as yet have not realised the value of information and computer support for their organisations.
SUGGESTIONS FROM THE POINT OF VIEW OF THE ORGANISATIONS

The organisation should realise that contingency planning for information systems is an important element of internal control to ensure computer data and resources would be available in case there is disruption of any nature to computer operations. Contingency planning is an important management planning. The contingency planning process should include the following:

Contingency planning

* The plan should ensure the continuity of the organisation's operations.
* Should minimise recovery times
* Must support the Business Recovery Plan
* Fulfill legal obligations

Risk analysis

This involves identification of exposures and threats that the organisations may be exposed. Hurricanes, earthquakes, bomb blasts in our own country are no longer an unlikely probability. These aspects need to be provided for.

Critical applications need to be identified by evaluating its impact on the organisations from the point of view of

(a) Legal obligations
(b) Interruption to service to customers
(c) Potential loss of revenue
Assess insurance cover

Insurance cover should not just be only for the cost of hardware. The exposures that the computer organisations is likely to have needs to be studied and covered.

Documenting the plan

It is unanimously accepted that the success of a contingency plan depends to a great extent on the quality of documentation. The documentation should clearly have the following:-

(i) The names and contact addresses of the main members of the recovery team
(ii) The details of recovery plan.

These plans should include the specific activities that need to be meticulously performed to minimise recovery time loss from disruption. List of important files that need to be restored to continue processing and procedures for recovering those files from back up tapes and disks.

It is not uncommon to have problems on pay roll or dividend warrant runs at the most critical period. It would be advisable for such critical applications to have even hard copies of important data.

The details of all equipment that would be needed to fully rebuild and reprocess needs to be inventories.
Forms and supplies

The contingency plans should have full details regarding specific forms that would be needed to continue critical applications.

Example: Pay slips, dividend warrants, invoice forms, contract forms etc. The importance of contingency plan lies in its periodic testing. It is necessary that the plan should be tested. However, it should be realised that unless the plan is fool-proof, testing of the plan may result in the disaster itself. Maintaining a contingency plan is an on-going process. It should be continually maintained, tested, evaluated and updated.

Review of insurance coverage

The insurance coverage should be adequate and upto date. The more important aspects for which the insurance should have cover would be

(i) Cost of equipment whether purchased or leased
(ii) Coverage for mechanical and electrical breakdowns which may result in loss of data or programs
(iii) Coverage for fraudulent or dishonest acts of employees
(iv) Coverage for loss of data and software

The policy should preferably cover the equipment at its replacement cost. It would be advisable also to provide for coverage for the following:

(i) Loss of documents
(ii) Cost of reproducing data
(iii) Injuries of personnel
AUDIT

The auditor should necessarily verify whether there is contingency or a DRP. If there is a DRP, he should bring with the contents to ensure that the standard accepted contents as discussed under documentation are all included. The auditor should pay special attention to the following aspects:

(i) Accuracy

While the plan may be in existence as to how accurate it is needs to be verified.

(ii) Currency

It is extremely important that the contingency plan is current as an out dated plan is no plan.

(iii) Testing

It would be advisable for an auditor to test a plan. It would be more effective if it is combined with a scheduled testing of the organisations. This would give him an opportunity to personally evaluate the effectiveness of the plan. In the absence of testing a thorough walk-through of the important aspects of the test plan would be adequate.

AUDIT OF DISASTER RECOVERY PLAN

More organisations have ceased to be mere users of audit processing facilities. The appreciation of changes of Information Technology has been so great that most
organisations are dependent upon computerised information. They are no longer mere users.

In view of dependence and reliance on computers and computer information it is not unlikely that should disaster strike the computer, the organisations may run around. Information is an asset and it requires to be safeguarded. Computer installations may be struck by disaster - human or by an act of God. The human element may be by way of intentional or un-intentional corruption of data and programs, fraud, sabotage etc. Fire, fraud, earthquake, lightning are other situations which affect the computer operations and disable it totally or partly. It is the responsibility of the auditor to verify the adequacy of the disaster recovery plan. He should ensure that there is a written documented plan which lays down the various procedures which would enable the organisation to recover from the disaster within a critical time-frame.

Eg. Reserve Bank of India incident, earthquake at California.

It is necessary for the auditor to be aware of what are the ingredients of DRP or a contingency plan with specific reference to the particular environment he is auditing. Being aware, he is expected to evaluate the adequacy or otherwise and give a report on the same.
## TABLE 7.2

### DISASTER RECOVERY PLAN

1. **Are standards, policies and guidelines regarding the contingency plan or DRP available? If so, are they adequate?**
   
   ( ) Yes - adequate and upto date  
   ( ) Yes - Reasonably adequate and upto date but need improvement  
   ( ) No - Not available.

2. **Have you checked whether the organisation has a remote, safe documents storage vault and valuable documents stored in the same?**
   
   ( ) Yes - verified and found to be in order  
   ( ) Yes - the vault does not have a latest and important documents.  
   ( ) No - No such check made.

3. **Have you checked whether there is an insurance policy to cover the computer hardware and software?**
   
   ( ) Yes - checked the policy. It covers both  
   ( ) Yes - only the hardware  
   ( ) No

4. **Have you checked from the angle of legal responsibility to ensure that the vital documents are handled satisfactorily and retained for sufficient time?**
   
   ( ) Yes - checked with the legal department  
   ( ) Yes - from my judgment  
   ( ) No

5. **Have you checked the existence of any contingency plan? Is it well-documented?**
   
   ( ) Yes - well documented  
   ( ) Yes - discussed with EDP staff  
   ( ) No