DISASTER RECOVERY - PLANNING FOR THE UNPLANNED!

A major data processing disaster is something most operations organizations never experience. However, there are various degress of severity for disasters ranging from complete loss of facilities, equipment and records, to temporary malfunction of time-critical equipment. The author proposes to first discuss the types and levels of potential disasters siting various case study examples (including one which happened in his own facility). Then, the author will identify the key elements necessary to develop a Disaster Recovery Plan, emphasizing how to prepare a DR Plan that is realistic. Last, the author will discuss approaches for periodically testing the DR Plan.

Disaster Recovery - Planning for the Unplanned!

Richard A. Savaiano
Principal
Industrial Management Associates
Manhattan Beach, California

INTRODUCTION

Although a major data processing catastrophe is something most organizations never experience, there are various degrees of severity for computer center disasters. These range from temporary malfunctions of time-critical equipment to complete loss of facilities, equipment and records. Disasters such as fire, flood, environmental problems, hardware and software problems, and sabotage can and do happen. Management often tends to ignore these possibilities. If management reviews the impact of data processing operations disasters, and consciously chooses not to plan for such major disasters, then perhaps the risk is not serious enough to warrant taking precautions. However, with today's corporate dependancy upon computer centers and information processing, the more typical situation indicates that when the computer center goes down, all company work is affected.

PURPOSE OF PRESENTATION

The purpose of this presentation is threefold:

1. To emphasize the need for and the importance of Disaster Recovery Planning.
2. To identify the key elements of a Disaster Recovery Plan.
3. To describe an approach for insuring that the organization's Disaster Recovery Plan will work.

In today's competitive, fast-moving, constantly changing business environment, the importance of computers and information systems is quite evident. However, it is estimated that less than 50% of the Fortune 1000 companies have a plan in place to insure continued availability of these valuable corporate resources. In addition, it is estimated that only one-half of the disaster recovery plans in place are workable. For smaller companies the percentages indicate an even worse situation.

POTENTIAL TYPES OF DISASTERS

Disasters occur infrequently, thus management may tend to deemphasize the immediate need for a recovery plan. The potential causes of disasters range from unique

and unusual weather conditions to deliberate employee sabotage. The list of typical causes include fire, storms, earthquakes, structural collapse, power failures, water damage, massive equipment failure, excessive heat and sabotage. The following three cases emphasize the need for Disaster Recovery Planning.

Company A:

A 300-watt light bulb was left burning over night in a supposedly fireproof tape vault for a large government computer center. The ceiling material next to the light began to smolder. The next morning when a computer operator opened the vault door to retrieve required tapes, the oxygen from outside the vault caused the fire to ignite in seconds. Attempts to turn off power to the computer center failed because the only power shutoff switch was located in a remote area behind the fire. Thus, fire personnel were pouring water on electrical equipment that was still running. Before the fire was over, the entire computer center was destroyed.

Three major problems contributed to this disaster. First, the material used in the vault should have been fireproof, not merely fire resistant. Second, the master electrical shutoff switch should have been located near

an outside door. Last, the computer center should have been designed to allow easier access by fire personnel. Proper Disaster Recovery Planning would have identified these problems.

Company B:

In the early morning hours a fire started in the warehouse of a medium-sized manufacturing company. Before fire personnel arrived, the blaze spread to the administration building of the company. Upon review of the damage, the president of the company quickly realized that most of the company's accounting records, as well as all of the data processing system, had been destroyed. The loss put the company out of business.

The major problem at this facility was the lack of a Disaster Recovery Plan and the associated remote site storage of critical and necessary information. With the proper backup facilities and procedures in place, the company could have survived.

Company C:

A machine caught fire in the production area of a small manufacturing plant. Because of the close proximity to highly combustible material, fire personnel reacted

promptly and efficiently dispensing thousands of gallons of water into the manufacturing facility. Water also flooded the adjacent administrative offices and the computer center. Fortunately, an alert computer operator followed the published emergency shutdown procedures eliminating the potential for fire and electrical damage in the computer room.

The next day, computer service personnel inspected all computer equipment, giving the go ahead to start up the facility only eight working hours after the fire. Published and practiced disaster procedures prevented a potential crisis.

Examples of disasters and potential disasters, such as the ones discussed here, re-emphasize the need to establish a Disaster Recovery Plan. An IBM study shows that over a ten year period from 1968 to 1978 there were more than 350 major data processing catastrophes.

PHASES AND ELEMENTS OF A DRP

The most important element of any Disaster Recovery Plan is the identification of the critical company functions. The primary objective after a disaster should be to restore

these critical functions. To accomplish these objectives, the designer of a Disaster Recovery Plan must understand two things: the phases of events in Disaster Recovery and the key elements contained in a Disaster Recovery Plan.

The Five Phases in Disaster Recovery are:

1. Preparation
2. Protection
3. Recovery
4. Critical Operations
5. Normal Operations

The Key Elements Contained in a Disaster Recovery Plan Include:

1. Introduction and Assumptions
2. Staffing
3. Hardware
4. System Software
5. Application Software
6. Data Files
7. Facilities
8. Operational Procedures
9. Transportation
10. Supplies

TESTING YOUR DISASTER RECOVERY PLAN

A major downfall of many Disaster Recovery Plans is the lack of a periodic review and testing of the procedures. A disaster should be simulated so that the recovery procedures can be tested, insuring that backup facilities work in the event of a crisis. Successful operation at an alternate computer site, using remote site backup equipment, programs, files and documentation is insurance to minimize the impact of a real disaster. Specifically, periodic testing verifies the availability of an alternate site and insures the compatibility of software. In addition, data records, supplies and operational procedures are checked.

SUMMARY

Disaster Recovery Planning is a function that many organizations will never use. However, for those who choose not to spend the time and effort developing and maintaining a DRP, the potential risk is high.

As evidenced by the examples of computer center disasters, the time of an emergency is not the time to develop an emergency plan. The likelihood of a serious computer disaster in any one company during a year is slight. However, with the increasing dependancy of businesses upon computer centers, distributed processing, executive workstations and timely information processing, the need for a recovery plan is great. Once a disaster strikes, your alternatives are limited. As a data processing manager, now is the time to PLAN FOR THE UNPLANNED!

SELECTED REFERENCES

1. Friedman, Stanley. "Just in Case ... Planning for a Disaster," Small Systems World. April, 1983, pages 28 - 31.

2. Perry, William E. Computer Control and Security. New York, New York: John Wiley and Sons, Inc., 1981.

3. Porter, W. Thomas and William Perry. EDP Controls and Auditing. Boston, Massachusetts: Kent Publishing Company, 1981.

4. Tarrington, Gary and Walter Ulrich. "Insuring the Unthinkable," Computerworld. August 24, 1983, pages 48 - 51.

5. Van Tassel, Dennis. Computer Security Management. Englewood Cliffs, New Jersey: Prentice-Hall, Inc., 1972.

BIOGRAPHY

Richard A. Savaiano is a principal with Industrial Management Associates, a management consulting and systems development firm located in Manhattan Beach, California. Specializing in the design, development and implementation of management solutions, Mr. Savaiano provides consulting services to a wide range of clients. In addition, Dick is a frequent speaker at management conferences, educational seminars and association meetings. He can be reached at (213) 545-3929.