Disaster Recovery Planning:
Suggestions to Top Management and Information Systems Managers

Several major disasters have occurred in the U.S. in recent years. Who can forget Hurricane Andrew, or the Midwest floods, or the California earthquakes? These disasters have refocused attention on the need for sound disaster recovery (DR) Planning.

Bo K. Wong
John A. Monaco
C. Louise Sellaro

In the past few years, the occurrence of disasters has caused serious damage to a considerable number of businesses. Some of the best known disasters, such as Hurricane Hugo, the California earthquakes, the AT&T brownout, the Chicago floods, the Hinsdale telephone switch fire, and the Penn Mutual and First Interstate fires, have destroyed many companies' information systems and often resulted in the termination of business operations.

The problem seems to be particularly threatening for smaller companies; a significant percentage of small and medium-sized companies struck by a serious catastrophe never resume operations, while a large number of those that do reopen are so weakened that they close permanently within three years of the event. These disasters have driven many companies to recognize the importance of information systems disaster recovery (IS-DR) planning.

Significant financial impact is another reason to consider DR planning. A study of manufacturing and distribution companies with annual gross

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission. www.manaraa.com

sales over $215 million revealed that a typical company will lose over $100,000 after four days without IS services and over $1 million after 10 days. The average company will lose over two percent of its gross sales within eight days of sustained computer outage. Almost 50 percent of firms that do not recover within 10 days will never recover or will go bankrupt.

There are also legal ramifications to the issue of disaster recovery planning. Many organizations are required by federal legislation to develop and test disaster plans. The Foreign Corrupt Practices Act requires businesses to take measures to guarantee security and integrity of assets and calls for suitable DR planning to avoid executive liability.

National banks must comply with the 1983 Banking Circular 177, which states that a bank must develop means to reduce the impact and/or risk of losing data processing (DP) support. A federal law instituted by the Federal Reserve Board requires that companies that electronically transfer funds in excess of $20 billion per day must show the ability to recover from a disaster within 24 hours.

In addition to financial and legal concerns, there are productivity and quality consequences to the loss of DP services. When a disaster strikes, both productivity and quality can be dramatically reduced in a product or service area that has all or most of its operations based on computer-supported functions. As a result, a company's reputation can be harmed, competitive advantage can be lost, and market share can be reduced.

Development of a Disaster Recovery Plan

Businesses interested in implementing a DR plan have many options available. Appendix A on page 33 presents a description of these various DR alternatives, as well as their advantages and disadvantages. The following is a description of the procedures involved in DR planning. All steps described are based on the actual experience of a 680-bed hospital in developing a DR plan. Every step is essential and required for a successful implementation of DR planning, and there is a high probability of failure if one or more steps are ignored.

STEP 1: Obtain Top Management Commitment

Top management commitment is vital to the success of any disaster recovery plan. The IS managers should secure top management commitment at the very outset, primarily by clearly highlighting the need for DR and the potential cost of avoiding a DR plan. This is often not an easy sell as the development of a DR plan requires a substantial commitment of resources for a period of time. Once top managers confirm the need for DR, they should appoint a DR coordinator to be accountable for directing and managing the development and maintenance of the plan. This individual will be responsible for communicating with top management throughout the process, as well as assuring that the plan is consistent with management's objectives and strategies.

STEP 2: Establish a Planning Committee

The appointed DR coordinator should establish a planning committee comprised of representatives from various departments throughout the organization. In addition, each department manager depending on the services of the computer system should be given responsibility for developing emergency procedures within his/her own department. The DR coordinator is in turn responsible for directing the strategic development of the recovery process, and the implementation and testing of the actual disaster plan.

STEP 3: Perform Risk Assessment & Impact Analysis

The planning committee's first task should be to perform a risk assessment and impact analysis to determine how long the organization could continue to operate without computer support. The risk assessment considers all possible threats to the IS, such as natural disasters, hardware and/or software error, and human error; the impact analysis includes an evaluation of the consequences of a disaster in each area of the business. Information for both the risk assessment and impact analysis should be compiled through interviews with the manager of each functional area. The output of the risk assessment and impact analysis should indicate which segments of the organization are more prone to disaster, what the costs are to protect them, and what the impact of such protection is on each. In addition, information regarding maximum allowable downtime, required backup information, and financial, operational, and legal consequences of extended downtime should be considered.

In addition to financial and legal concerns, there are productivity and quality consequences to the loss of DP services... a company's reputation can be harmed, competitive advantage can be lost, and market share can be reduced.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission. www.manaraa.com

ASM
ASSOCIATION
FOR SYSTEMS
MANAGEMENT

Presents one of their many courses:

A TWO-DAY SEMINAR

ELECTRONIC DATA INTERCHANGE

- Learn how to successfully implement EDI into YOUR company with a positive bottom line impact.
- You've heard the hype, NOW learn the specifics from a business professional!

- **Business Issues**
- **Impacts**
- **Opportunities**
- **Cost Control**
- **Legality**
- **Auditability**
- **Flexible Management**
- **Centralized Control**

A timely, action-oriented practical professional business seminar-
With answers!

SPRING SCHEDULE
DATES & LOCATIONS

BUFFALO, NY	MAY 16-17, 1994
BALTIMORE, MD	MAY 19-20, 1994
CINCINNATI, OH	JUNE 13-14, 1994
ATLANTA, GA	JUNE 16-17, 1994
CHARLOTTE, NC	JULY 11-12, 1994

Call: Joyce Mason - Ext. 121
or Paula Winrod - Ext. 122
at 216-243-6900
Fax: 216-234-2930

To register or for more details.

STEP 4: Prioritize Recovery Needs

The DR coordinator should then rank each IS application according to need for its recovery in event of a disaster. Neither size, architecture, nor end-users should be used as the determining criteria in identifying the most important applications. Instead, the prioritization should be based on how each application affects the ability of an organization to achieve its mission. Mission-critical applications should be given the highest priority in terms of recovery.

Hence, the largest or most widely used systems may not be the applications that an organization will need in the first days of a computer outage. Applications should be categorized into levels of tolerance as follows:

1. Critical: These applications cannot be performed unless identical capabilities are found to replace the company's damaged capability. Critical applications cannot be replaced with manual methods under any circumstances.

2. Vital: These applications cannot be performed by manual procedures, or can be performed manually for only a brief period of time. There is a somewhat higher tolerance of interruption if the functions are restored within four to five business days.

3. Sensitive: These applications can be performed with difficulty, though at a tolerable cost, by manual means for an extended period of time. Sensitive applications will require considerable "catching up" once DP capability is restored.

4. Noncritical: These applications can be interrupted for an extended period of time at little or no cost to the company.

STEP 5: Select Recovery Plan

There are many different types of DR plans available (see Appendix A). Once the applications are prioritized, the various recovery plan alternatives should be evaluated by considering their trade-offs among level of recovery, risk reduction, cost, and advantages and disadvantages. The plan chosen should also be based upon the risk assessment and impact analysis previously conducted. Most importantly, it should be the one that best fits the organization's overall DR objectives.

STEP 6: Select Vendor(s) and Develop Agreements

Once the recovery plan is determined, vendors can be selected and contracts developed. One is seeking vendors who can take over your processing, or at least parts of it, after a disaster. In choosing a vendor, consideration should be given to the vendor's reputation, reliability, flexibility, and service offerings. A good vendor will demonstrate the capacity to support current applications and future growth, show strong primary and backup communications capabilities, have a reasonable subscriber-to-site ratio, and demonstrate a proven track record of supporting customers during testing and actual disasters.

The contract(s) should be clearly written so both parties understand the contents. It should concisely state duration, termination conditions, testing issues, system change procedures, service levels, costs, and any other issues related to the specific agreement. A contract review will help to ensure that all promises, both verbal and written, are actually be included in the final, legally binding deal.

STEP 7: Develop & Implement the Plan

Once the plan has been defined, it is then formally developed and implemented. Top management, the planning committee, vendors, and end-users must be involved in the development and implementation process and should be informed of their specific responsibilities. The key to successful development and implementation is communication; the plan should be communicated to **all** affected departments and personnel. Application priorities and associated recovery strategies should be distributed to the appropriate departments so that each understands how it might be impacted by a disaster. In general, the plan should include organizational and vendor responsibilities, key contacts among departments and personnel, a step-by-step walk-through of the sequence of events to be followed in

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission. www.manaraa.com

the event of a disaster, training for the personnel, and issues related to physical environment, organizational control, and emergency action.

STEP 8: Test the Plan

Having an untested DR plan may be of no more value to a company than having no plan at all. The merit of DR lies not in the plan itself, but in the success of the recovery. The only way to ensure this recovery is through the development of solid testing procedures.

There are many different types of test plans. Walk-through testing is the process of identifying all of the steps and tasks necessary to successfully complete a test. Simulation tests execute a sequence of steps in the DR plan as though a real disaster had occurred. Unit testing is the process of testing individual pieces of the overall plan. Application tests include tests on all the critical applications. Parallel tests are duplications of regular processing for a particular time frame. Mock testing simulates actual disaster conditions by interrupting service and involving key users in the actual recovery process.

As many different types of tests as resources will allow should be conducted. Upon completion of each test, the results should be reviewed and compared to the objectives of the DR plan. This review serves to correct any problems or deficiencies and to implement improvements.

STEP 9: Continually Test & Evaluate the Plan

The plan should continue to be maintained and tested and a schedule should be developed for regular interval testing. Typically, applications, hardware, personnel, and operations change over time; only retesting can ensure that these components remain consistent with the plan. It is a major task keeping personnel lists and escalation procedures updated and current. Continued testing will result in properly trained staff and vendors that are well-drilled in their respective duties and responsibilities. Repeated testing can provide the experience necessary to recover from a real disaster as deficiencies in the existing recovery process are continually uncovered and corrected. All employees involved in the DR plan should regularly participate to ensure that they are well informed of their responsibilities. Every test result should be documented, reviewed by management, and communicated to all concerned parties.

In general, the plan should include organizational and vendor responsibilities, key contacts among departments and personnel, a step-by-step walk-through of the sequence of events to be followed in the event of a disaster, training for the personnel, and issues related to physical environment, organizational control, and emergency action.

Implications & Suggestions to Top Management

The successful development of a DR plan depends not only on the proper implementation of the steps discussed above, but also on the involvement of top management. In particular, top management should:

1. Provide adequate financial support. Senior executives must appreciate the fact that the loss of information due to a disaster could cause the termination of business operations. Hence, they must weigh the amount of risk their company is willing to take against the cost of implementing information recovery and business resumption measures.

2. Communicate the policies, procedures, and standards of IS-DR planning and implementation throughout the entire organization. A lack of such communication could result in the emergence of different levels of preparedness in different departments, creating a potential weak link.

3. Accept that implementation is the responsibility not only of the IS department, but of each functional department. Therefore, top management should ensure that the plan is reviewed by the appropriate functional managers and give final approval to a plan that guides the detailed planning and implementation procedures.

4. Ensure that both internal and external auditors enforce standards for recovering IS. The use of impartial, external consultants to review the technical, technological, business, and organizational aspects of the plan may help detect weaknesses that are not obvious from within.

5. Understand that objectivity is critical to the success of a DR plan. Management should be aware that politics can overshadow the pragmatic considerations of DR.

6. Recognize the stress level associated with the position of DR coordinators. DR coordinators should be rewarded not only through salary but by freeing their time from other tasks and recognizing the value of their work.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission. www.manaraa.com

Implications & Suggestions to DR Coordinators

In addition to securing top management's involvement, DR coordinators should:

1. Be prepared to "sell" the idea of DR not only to management but also to the various departments affected throughout the organization. Support and cooperation from functional departments will not exist if each department is not completely sold on the concept of DR.

2. Define the scope of the plan. This will prevent a loss of focus which can result in a plan that deviates from its mission. The scope must extend beyond the data center; after all, the ultimate goal of DR is not data center survival but corporate survival.

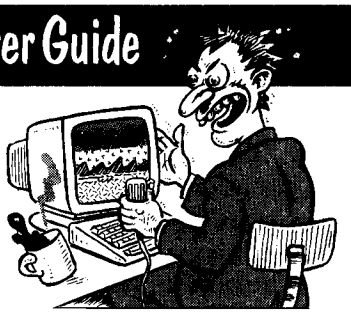
3. Consider the business side of DR as well as its technical side. Personnel issues, such as making provisions for those employees who must temporarily relocate to alternate sites, should receive attention. Public relations should also be a concern; the news media may want information, and someone will have to be the communicator of that information. In addition, customers will want to be kept up-to-date in a disaster and should in fact be made aware of DR procedures before a disaster strikes.

4. Be prepared to work with civil authorities in the event of a disaster. They can facilitate the execution of the DR plan at a time when other local businesses may be struggling to maintain operations.

5. Perceive preventative measures to be as important as the DR plan itself. No matter how sound the DR plan is, the company will always be better off if the plan is never actually executed. Ideally, a well-balanced program should be implemented that provides cost-effective support for both disaster prevention and DR.

6. Negotiate with the insurance carrier to offer reduced rates or better insurance after the plan is in place. If the plan is a good one, the company will have substantially lowered its risk. This lower risk should be reflected in reduced premiums.

The Monday Morning Computer Guide



If Cars Had Operating Systems ...

S/36 SSP Mainframe, OBV:
You get in the car and drive to the store. Halfway there you run out of gas. While walking the rest of the way, you are run over by mopeds.

OS/400:
An attendant locks you into the car and then drives you to the store, where you get to watch everybody else buy filet mignon.

VAX/VMS:
Gets you quickly and efficiently to the store, after you spend three days with the manuals figuring out how to get there.

CPM:
You get into your '58 Chevy to go to the corner market for a six-pack, but the 8" welded and chromed chain steering wheel won't boot.

AOS/VS (Data General):
You request a trip to the store, it opens a map, determines the location, places you in the car, but the instructions look like other operating systems commands. Because you aren't familiar with AOS, you tell the car different instructions and you end up in Southboro, Mass. Only to find out there is no one at DG to help you with your problem, and your kids know more than their experts. Then the nightmare really begins; you end up at TFS just in time for the Platform Committee Meeting to find out they are going to erase AOS/VS from the car.

The above is an excerpt from *The First, Advanced, State-of-the-Art, High Performance, Totally Integrated, Revolutionary, Leading Edge, High Tech Joke Book*, published by and available from Oak Ridge Public Relations (408/253-5042).

Conclusion

As long as the possibility of disaster exists, there will be a real need for companies to develop and implement disaster recovery plans. Companies that recognize this need and successfully implement a sound DR plan will have a realistic chance of surviving when and if disaster strikes. Companies that are unsuccessful in formulating a plan, or that choose to avoid the issue of DR planning entirely, run the risk of ruin in the event of a disaster.

Bo K. Wong, Ph.D.

is an associate professor of MIS in the Department of Management at Youngstown State University, Youngstown, Ohio. He has about forty publications/presentations in refereed journals, conference proceedings, and conference presentations. His research interests are in information systems quality and disaster recovery planning. He received Youngstown State University Research Professorship Award in both 1991 and 1993, and was listed in Who's Who in 1993.

John A. Monaco

is a limited service instructor of MIS in the Department of Management at Youngstown State University, Youngstown, Ohio. His research interests are in disaster recovery planning and AI business applications.

C. Louise Sellaro, Ph.D.

is a professor of Management in the Department of Management at Youngstown State University, Youngstown, Ohio.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission. www.manaraa.com