

**Report
a
Problem**

The CPA Journal

The CPA Journal Online
June 1994

Planning for disaster.

by Smith, L. Murphy

Abstract- The string of natural and man-made disasters that had recently devastated US businesses underscores the importance of disaster recovery planning (DRP). In addition to a general emergency plan, companies must also have computer contingency plans to protect critical information from loss, destruction, theft and other risks. An effective DRP should provide for the recovery of vital records, alternative telecommunication systems, evacuation of disabled employees, housing arrangements for the recovery team, food service and alternate sources of supplies. A computer contingency plan, on the other hand, should have emergency, back-up, recovery, test and maintenance plans. Adequate computer contingency planning should help firms to quickly regain their capabilities to process information and get back in business.

- [Search](#)
- [Software](#)
- [Personal](#)
- [Help](#)

Much has been learned from disasters such as the World Trade Center bombing and Hurricane Hugo. Planning for their occurrence is the key. The authors discuss disaster planning in general and computer contingency planning in particular.

In recent years, U.S. businesses have endured several well-publicized natural and man-made disasters causing losses amounting to tens of billions of dollars. Most recently, southern California suffered a major earthquake, with after shocks resounding throughout its hills and valleys. Where natural disasters fall short, mankind is known to fill the breach. The terrorist bombing of the World Trade Center resulted in hundreds of millions of dollars in damages, as well as loss of life. While last year's flooding in the midwest was less dramatic, the slowly rising waters were just as devastating. During the four years preceding these calamities, Hurricane Andrew smashed South Florida and portions of Southern Louisiana; a major earthquake caused massive damage in the San Francisco Bay area; and Hurricane Hugo struck Charleston, South Carolina, devastating the surrounding area.

When Hurricane Hugo slammed into Charleston, South Carolina in September 1989, Hugo's path of destruction was well documented by the news media. Eighteen people were killed in South Carolina, 36,000 homes were damaged or destroyed, crops valued at \$50 million were wiped out, and trees valued at \$1 billion were toppled. The 24-county region that felt the main force of Hurricane Hugo sustained about \$5 billion in damages.

How well have businesses been prepared for these disasters? Disaster contingency planning in general and computer contingency planning in particular have been put to the test. The disasters demonstrated that the ability to recover from a major natural or man-made disaster is crucial to a firm's survival. Deloitte and Touche was able to shoe horn its World Trade Center operations into its other New York City office during the weekend following the World Trade Center bombing. What has become clear is that businesses must implement corporate-wide disaster recovery planning (DRP) that transcends data processing issues alone. DRP is a major corporate responsibility. The CEO must understand the major risks to the company and the potential consequences of disaster. Proper DRP addresses the needs of all departments and involves personnel from all areas of the company. Responsibility for DRP is not the sole responsibility of MIS management.

The Nature of Disaster Planning

The World Trade Center disaster, perhaps as no other, dramatically elevated the importance of disaster planning beyond computerized systems. The issue was not just keeping the computers running, but how to communicate to customers, employees, and others who interact with an enterprise that suddenly vacates its premises. Once vacated, where will business be transacted the next business day? What will be the source of cash flows for rental of temporary facilities, computers, and phone equipment? Many dislocated businesses gave thanks to cellular phone technology, which allows communication without phone lines.

Temporary Facilities. Effective disaster planning will consider several options for temporary relocation and facilities:

First, a company may have a branch or division close by the disrupted location that can be used as the hub for resuming business activity. This was the solution for Deloitte & Touche, and news reports indicated this arrangement was used by a number of New York City area firms affected by the World Trade Center bombing. If this arrangement is not possible, perhaps a reciprocal agreement could be arranged with another business to share its business location for a brief period of time.

A new breed of business has recently sprung up that provides back-up facilities to dislocated operations. The space may be a warehouse-like facility in a lower rent district, but it can quickly accommodate staff and employees working with temporary equipment.

Another option is to acquire and maintain a back-up site to serve as the center of business activity. However, the cost of this final option may be excessive.

Communications Alternatives. Communications would also be part of the comprehensive plan. There will be the need to notify employees and customers about the new business location. The firm should maintain a listing of all employees including their home addresses and telephone numbers. The list should be periodically updated to ensure its accuracy. With this information, employees can be informed of the new location.

A similar approach could be used to advise customers about a new business location. However, for many companies, the size of their client listing might prevent this approach. In that case, the media could be used to aid in the notification of clients. Radio and newspaper advertisements should be considered. If notification is extremely critical, television ads are another option.

There are several other issues a firm might face when recovering from a disaster. They include telecommunication needs, equipment other than computers, and necessary materials and supplies.

Additional phone lines may be necessary if a location is shared with another firm. If a new location is leased or purchased, telephone service must be established. Equipment such as calculators and typewriters, as well as furniture and fixtures, may be needed. Various types of material and supplies also will be required.

Risk Analysis. The CEO and major corporate vice-presidents should spend time learning emergency preparedness. A comprehensive risk analysis will point out the impact of major disasters on a corporation's bottom-line. Thus, senior management is more likely to give approval and long-term commitment for DRP that transcends established organizational boundaries. When such commitment is given, senior management is more likely to include the cost of the DRP as a line item in the overall corporate budget on an on-going basis.

Guidelines that will assist corporate management in the disaster recovery planning process include the following sources:

- * The Federal Emergency Management Agency's "Disaster Planning Guide for Business and Industry."
- * The American Red Cross.
- * Publications of the San Francisco Bay Area Earthquake Preparedness Project.
- * The Computer Planning and Recovery Planning Institute (PO Box 81151, Wellesley Hills, MA 02181).

The above sources should enable companies to develop procedures to identify potential major disasters, estimate the losses from a disaster, and develop a comprehensive disaster recovery plan before an emergency occurs. Such comprehensive planning requires the collaboration of accountants, attorneys, management, data processing personnel, engineers, and others who can collectively identify disaster-related risks.

Matters to Consider

A DRP should include the following considerations that are often not part of a computer contingency plan:

- * Appoint a disaster recovery manager to incorporate the computer contingency plan into the overall broader DRP.
- * Incorporate into the DRP loss of voice communications. Loss of voice phones is synonymous with lost revenue. Considerations should be given to 800 lines, WATS, special circuits and software defined networks, and other special call-handling equipment. As noted earlier, portable cellular equipment is a possible quick fix.
- * Telecommunications have become more electronic and thus more vulnerable to power problems. Develop alternative telecommunication plans, such as communicating among workers on home PCs.
- * Establish a vital record recovery plan.
- * Establish guidelines to evacuate disabled employees when elevators are inoperable.
- * Do not rely on only one supplier. Establish alternate sources of supplies.
- * Provide housing arrangements for the firm's recovery team.
- * Provide for food service at the backup recovery site.
- * Establish travel arrangements for recovery personnel stationed at the recovery site.
- * Establish guides for relocation of paper, film, and magnetic records.
- * Notify employees when and where to return to work after a disaster strikes.
- * Provide contractual arrangements with clean-up crews to remove debris.

Finally, the firm should periodically evaluate its insurance to replace destroyed assets, provide necessary cash flows, and compensate for lost revenues from downtime. The first two are essential, while the last can be minimized, or even eliminated, depending on the vitality of the disaster recovery plan.

EXHIBIT1

COMPUTERDOWNTIMERESULTINGFROMHURRICANEHUGO

DowntimeNumberPercent

1-15days2087%

16-60days29

2-4months14

Total23100%

EXHIBIT2

FIRM'SPROCESSINGCAPABILITYAFTERHURRICANEHUGO

Accounting

DataProcessingNumberPercent

Processalldata522%

Processsomedata417

Processnodata1461

Total23100%

EXHIBIT3

TYPEOFAUDITINGFIRM

FirmTypeNumberPercent

National522%

Regional417

Local1357

Noreponse14

Total23100%

How Many Firms Use Computer Contingency Planning?

Following Hurricane Hugo, a survey of 71 companies was conducted in the Charleston, South Carolina area. Each company had sales in excess of \$1 million. The companies were selected from a Dun and Bradstreet listing.

Each selected company was mailed a questionnaire requesting information about its computer contingency plans and related factors, including its ability to process critical

accounting information after Hugo. A total of 41 usable questionnaires were received and analyzed. An analysis of the questionnaire responses disclosed that 18 (44%) of the companies had a computer contingency plan in place before Hugo, while 23 companies (56%) did not. These results were not unexpected. An earlier study of 12 years ago suggested companies typically do not maintain computer contingency plans. Little has changed in the intervening years.

Firms Without Computer Contingency Plans

The survey of Charleston area firms did not address all disaster recovery issues, but focused only on the computer contingency plan. The computer contingency plan is one of the most critical components of disaster recovery planning and is particularly relevant to external auditors. The 23 firms without computer contingency plans faced a variety of problems after Hurricane Hugo.

Computer Downtime. All firms without a computer contingency plan reported a shutdown of computer operations as a result of Hurricane Hugo. Twenty firms reported computer downtimes ranging from one to 15 days, two from 16 to 60 days, and one firm's computer was inoperable for two to four months. Computer downtime is summarized in Exhibit 1.

With inoperable computers and no contingency plan to quickly restore normal processing activities, the firms were faced with the problem of how to process critical accounting information.

Ability to Process Accounting Information. The 23 firms without a computer contingency plan encountered various problems associated with computer downtime. Most companies were unable to process critical accounting information while their computers were shut down. Only five firms were able to process all critical accounting applications. Four companies were able to process only some significant accounting applications, and 14 firms (or 61%) were unable to process critical accounting information. Exhibit 2 summarizes the firm's processing capabilities.

The firms without contingency plans were audited by different types of auditing firms. Exhibit 3 provides a breakdown by type of auditing firm.

Computer Contingency Plans

To protect vital accounting information from loss, destruction, theft, and other threats, a company should prepare a comprehensive computer contingency plan. The computer contingency plan should have the following component plans:

- * Emergency
- * Back-up
- * Recovery
- * Test
- * Maintenance

The emergency plan indicates actions to be taken immediately after a disaster. An important aspect of this plan is the preparation of a contingency organization chart, showing the name of the contingency manager and primary contingency coordinators. The responsibilities of the contingency manager and contingency coordinators should be explained clearly.

The second critical aspect of a computer contingency plan is the preparation of a back-up plan. This document is an important element necessary for recovery. The selection of a back-up alternative requires careful planning. The company should consider the following alternatives: utilization of data processing service bureaus, another company's computers, or a vendor's computers. To ensure a compatible computer is available on short notice, a mutually agreeable contract between the company and the other organization providing back-up facilities should be prepared.

The third aspect of the computer contingency plan is the preparation of a recovery plan. The company should assess its ability to restore critical accounting information within an acceptable time period. A competent recovery team is a significant part of any recovery plan. The names, telephone numbers, specific assignments, special or alternative training needs, and other essential information of each team member must be shown on the recovery plan. A section should indicate which recovery team members are responsible for establishing the timetable for the recovery operations and who decides if outside, temporary personnel are needed to complete the recovery on schedule. Also, the recovery plan should include procedures for coping with the non-availability of data processing personnel.

Even with the most elaborate recovery plan, it may take as long as one or two days before a back-up site can begin any type of accounting information processing. Such a delay requires the company to focus its efforts on processing those computerized accounting jobs essential to the survival of the organization. Consequently, the recovery team must prioritize accounting applications that must be processed at the expense of all others. By identifying those accounting applications deemed critical and by further evaluating the resources required to sustain those critical accounting applications, decisions are more easily made regarding alternative work locations, schedules, back-up facilities, software needs, data preparation needs, personnel needs, security, and documentation requirements.

The computer contingency plan must be periodically tested to discover and eliminate problems. This is the fourth component of the contingency plan. Many potential problems can be eliminated by developing a test strategy. The most effective way to determine if the contingency plan works is to conduct simulations of actual disasters. Test results should be reviewed by individuals that took part in the test. The results of the review should be utilized to identify any flaws in the contingency plan.

Finally, the company should ensure procedures are devised to keep the contingency plan current. This is the fifth component of the contingency plan, plan maintenance. Any necessary changes should be integrated into the documented plan, based on the simulated disasters. A plan of action should be prepared for the implementation of changes to ensure even greater protection from disasters.

Benefits of Computer Contingency Planning

A computer contingency plan is classified as a corrective control. It is not designed to prevent or detect various disasters, but rather to limit losses resulting from commonly occurring disasters. Assuming disaster strikes, the presence of a computer contingency plan enables a company to quickly restore its capabilities to process critical accounting information, and to provide services and products for its customers efficiently and effectively. Preparation of such a plan forces a company to prioritize accounting applications into critical and non-critical categories. Thus, the company is able to continue processing critical accounting information, ensuring that it will not temporarily nor permanently cease operations.

Statements on Auditing Standards and Contingency Plans

SAS No. 60, The Communication of Internal Control Structure Related Matters Noted in an Audit, was issued in April, 1988. SAS No. 60 provides the auditor should communicate to

the audit committee or its equivalent "reportable conditions" and provide recommendations for corrective action. SAS No. 60 defines a reportable condition as a significant deficiency in the design or functioning of the internal control structure that could adversely affect an organization's ability to record, process, summarize, and report financial data. Any reportable condition should be included in the management letter provided to the client at the conclusion of each audit engagement.

Some professionals believe the lack of a computer contingency plan by a company that processes significant accounting information by computers is an example of a reportable condition as defined in SAS No. 60. In any event, when an auditor discovers a lack of a computer contingency plan, it is recommended that a comment and recommendation for corrective action be included in the management letter.

Michael J. Cerullo, PhD, CPA, is a professor of accounting and R. Steve McDuffie, DBA, CF, is an associate professor of accounting, both at Southwest Missouri State University. L. Murphy S. Murphy, DBA, CPA, is the Price Waterhouse Teaching Excellence Professor of Accounting at Texas A&M University. He is an editor of The CPA & The Computer column of The CPA Journal.

[Home](#) | [Contact](#) | [Subscribe](#) | [Advertise](#) | [Archives](#) | [NYSSCPA](#)

The CPA Journal is broadly recognized as an outstanding, technical-refereed publication aimed at public practitioners, managers, educators, and other accounting professionals. It is edited by CPAs for CPAs. Our goal is to provide CPAs and other accounting professionals with the information and news to enable them to be successful accountants, managers, and executives in their practice environments.

©2008 The New York State Society of CPAs. [Legal Notices](#)