CONTINGENCY PLANNING -- THE AUDIT PROCESS

Leslie A. Virgilio
OFF-SITE, Inc.
32 Ellicott Street
Batavia, New York 14020

Disaster Recovery is the ability to continue your information processing when your facilities for doing so are unavailable. Situations requiring recovery can be natural disasters, industrial accidents, human relations, and hardware failure. None of these are recoverable without a Contingency Plan. The Disaster Recovery Strategy protects against the improbable. Contingency Planning prepares you for the inevitable.

Companies should insure their computer hardware for the replacement costs involved. Along with this policy they may also have an "ability-to-operate" clause which guarantees them some income should they have to close business due to data processing failures. Most insurance policies protect against immediate financial loss due to disaster. Other losses such as client base, reliability of service, cash flow, payroll calculations, and reporting capabilities are not recoverable on insurance policies.

Auditors are now requesting that part of their clients corporate profile be a Contingency Plan and Disaster Recovery Strategy. Some organizations may even be pressured by government agencies to prepare such a plan. Yet, when companies are asked whether or not they have a Contingency Plan for their Data Processing needs, the answer is often, "Yes, we back up our system and store our tapes at a remote location." The problem with this answer is what do you do with those tapes if your machine is unavailable to use due to a disaster situation? Several options are available.

One option is a Private Backup Site. These sites are owned by the business involved. To be of full benefit in the case of a disaster, this site should be in a different location than the original. There are two types of private backup sites: "cold" and "hot". A "cold" site is a fully equipped computer facility, without the computer. Only electrical power, air conditioning, and telecommunications equipment exist. When disaster strikes, the computer and required peripherals must be obtained, installed, and tested. Although relatively low in cost, the "cold" site has the disadvantage of a lengthy implementation. A "hot" site is a fully equipped computer facility with an identical or very similar computer system to the original, already installed. Obviously, the most desirable system from an operations standpoint, this alternative is extremely expensive. Another drawback to this alternative is the easy justification for using the system/facility for other uses. This eliminates the 100% availability for disaster recovery.

A second option is a Mutual Backup or Reciprocal Agreement. A Mutual Backup Agreement can be between two businesses, or between two different computer sites within the same business, with similar system configurations. They agree to back up one another should a disaster occur. The businesses are usually located near each other. To eliminate competition, the companies are usually in different industries. Although there is little or no cost to the agreement, there are several drawbacks. Few corporations will allow a second or third level manager to form a binding contract on a handshake. There are very few sites with sufficient excess capacity to operate a second business without curtailing their own operations. Will your CEO allow his business to fall behind to allow another company to use his hardware? Further, the most critical phase of Disaster Planning is testing. This is the step most commonly omitted from mutual agreements. For these agreements to <u>really</u> work, companies would have to have far more computer capacity than their businesses require.

A third option is the "Cold" Backup Site, which is similar to the privately owned cold backup site. It is an "empty shell" facility owned and operated by a company in the business of data disaster recovery. Cold Sites bring up the term "Allowable Downtime". How long can you be without a computer? How long will it take to "warm up" a cold site? Is it conceivable that a hardware configuration sufficient to support operations can be delivered, installed, and made operational within a sufficient amount of time to keep the company running efficiently? An open purchase order with a vendor for delivery of a complete configuration only guarantees purchase of the equipment, not that it will be delivered when needed.

A fourth option is a Remote Site. This type of facility depends on telecommunications. Dialing into a computer system can create problems for the users. The number of external forces working against the ability to exchange information are staggering: weather, traffic accidents, power failures, and load switching just to mention a few. Also, you must be sufficiently supplied with modems, at reasonable working speeds, and terminals to be able to use the Remote Site.

A fifth option is a Mobile Site. The Mobile Site again brings up the term "Allowable Downtime". Alot of computing power can be put in the back of a truck, but how soon can you get it where it is needed? And at what cost?

Another option is the Hot Backup Site. This situation is probably the most acceptable solution to disaster recovery. It is a fully equipped computer facility, owned and operated by a company in the business of disaster recovery. Although there can be competition for its use, disaster recovery companies can often compensate by having multiple CPU's and/or multiple hot site locations. Often, the disaster recovery facility can also accommodate users by having terminals/workstations for people to use.

The choice of where to recover must meet the needs of the company. Hewlett-Packard has provided us with computing hardware compatability unsurpassed in the industry; an interchangeable operating system. For the most part, any software will run on any machine just by using two MPE commands: RESTORE and RUN. Therefore, any of the above options will work.

Assuming you have solved the hardware problem, what about your users? A workable Disaster Recovery Strategy and Contingency Plan requires not only hardware to continue operations, but also a transferable set of software and users.

What then should the approach to Auditing and Contingency Planning be? Ask yourself "What's wrong with the existing methods of preparing for a disaster?" The answer is simple. We write up a set of procedures, document systems, define requirements, ignore the users, put it on a shelf and never look at it again. For a Contingency Plan to work, the document must become a useful tool; something that will be a part of our daily operations and decision making. If it is used daily, it will be updated. Having current information is the only way any Contingency Plan can work.

Basic DP Audits are offered by most public auditing firms as part of the annual Financial Audit. These audits cover procedures and data flow, usually tracking specific portions of information in order to understand their source. This information should be incorporated into the Contingency Plan. However, a complete plan must also include the mechanics of operation. It must be developed by individuals who know and understand the computer systems being utilized as well as the information processing needs and methods of the organization. The only way to truly accomplish this is through the Data Processing Audit. This Audit includes complete definition of the Data Processing System, both manual and computerized. Identification of each application and the subsets of these applications are also defined. Within the subsets, key personnel, special requirements such as source documents and output forms, as well as the relationship between applications, are revealed.

It is not good enough for the Contingency Plan to tell us only what to do when a system fails. It must guide us when the individual component parts of the system go astray. These component part failures come in a variety of ways. The most common in any organization is key user vacation time and extended sick leave. Moreover, from a computerized standpoint, if data becomes corrupted or application software fails, which related applications will no longer function? As mentioned earlier, we are dealing with the inevitable. People will change jobs. Hardware systems will fail. Processing will need to be stopped. By understanding the interrelationships and needs of the data processing function, it becomes possible to prepare for these inevitable situations.

Contingency Planning cannot be restricted to the computerized flow of information. It must include those manual procedures required to supply the flow and support those which are computer dependent. In the event of a complete systems disaster, such as fire, it is also necessary for the Contingency Plan to identify which applications are critical to daily business; which applications need to be put into place first. Fortunately, the Data Processing Audit identifies the applications most critical to the organization and, of these, what other applications are dependent and which are related. We now have the ability to put into place portions of the overall system versus restarting of the entire process.

There are several factors that should be considered when doing a Data Processing Audit. These include: hardware resources utilization & requirements; primary & secondary systems support equipment; vendors; forms; software applications; personnel -- duties, responsibilities, back-up and schedules; emergency calling; subordinates; risk analysis -- resources, environment, personnel and software; critical processing timetable; allowable downtime. Let's look at each of these critical areas independently.

HARDWARE RESOURCES UTILIZATION AND REQUIREMENTS

When evaluating hardware resources for disaster recovery planning, we need to know what the minimum requirements needed to be able to function in a contingency mode are. In order to determine that, we need to know current hardware configurations, including: operating system MIT; computer series; megabytes of main memory; number of printers and LPM speeds; number of modems and baud rates required; number of Mux. channels; number of INP boards; number of modem links; number of tape drives and BPI speeds; disc space utilized; number of terminals needed and if any special terminals are needed for added memory or graphics capabilities; special equipment such as bar code readers and optical scanners.

PRIMARY & SECONDARY SYSTEMS SUPPORT EQUIPMENT

For each site location, we need to know about the environment. What type of power control equipment do we have? What type of environment control equipment? Who are the vendors, the contacts? What company provides our power source? Do we have fire protection? If yes, what type? Halon, water sprinklers? What type of structure is the computer room? Are there fire walls? If there is a fire outside the computer room, how much time do we have before the computer room catches fire as well? All this information is vital to be able to rebuild the type of facility you currently have and/or to be able to salvage what currently exists. These factors also determine the disaster risks and survival abilities.

VENDORS

Computer supplies and other equipment needed to run your systems may also be inaccessible in a disaster situation. A list of vendors with purchase order numbers, inventory lists, and other information is crucial to facilitate replacements. Information about software vendors is needed as well. Does the company provide telesupport and/or site support? Who is the primary contact? Has the vendor given approval for the use of their software on an alternate machine? You want this information easily accessible.

FORMS

Identification of forms must also be done. What are the forms used in the applications? Who is the vendor? What is the order unit of measure? What is the monthly usage? What is the order lead time? Where are the forms stored? What applications use the form and what is the consumption by the application? Forms identification not only applies to preprinted output forms. It should include manually prepared source documents that are needed.

SOFTWARE APPLICATIONS

Software applications can have one of three characteristics. They can be dependent, independent or associated. Independent applications are those which will function as self-contained units regardless of the existance of any other applications. Dependent applications are those which require interaction between two different applications for the purpose of decision making. Associated applications are those which utilize portions of other systems in a passive manner. For each application, dependent and associated applications must be identified. Each application user must be identified as well as their duties and responsibilities. Back up personnel must be assigned to each user. Who are the in-house technicians? Is there a vendor software engineer? If yes, who is it? Where can he/she be reached and at what hours? What type of application are we running? Finance, order entry, etc. What languages is the application written in? What types of files does it require? If it's a purchased application, have any of the programs been customized? How many terminals are needed to run the application? How many megabytes of disc spaces? How many people? What is the Allowable Downtime? Which computer installation is used for this applications processing? For each subset of the application, the transaction volume and required transaction turnaround time must be defined. The critical processing times of each subset must also be defined, as well as the duration. We also need to know what special equipment, whether computer or non-computer, is needed to run each application successfully. For instance, when running accounts payable, the checks may need to be printed on a special printer, bursted by a burster, folded and sealed by a folding machine and then stamped by a postage meter. We need to define if the equipment is critical or merely useful to the processing. A most critical question...has the vendor approved use of the software at an alternate site in a disaster situation? Does the application require special forms? If yes, are they critical or just useful?

PERSONNEL -- DUTIES, RESPONSIBILITIES, BACK-UP, SCHEDULES
Who are the key people in the information flow? They know who they are, but how many of us have assumed responsibilities, out of necessity, that our direct supervisors are unaware of? The relationships between people and their work are similar to the relationships between hardware and software and between software applications. Knowing how the people relate to the work performed is just as important as knowing how the hardware and software relate to each other. This is the mechanics of operation, the manual process required to support the electrical process.

EMERGENCY CALLING
An Emergency Calling List is a list of all key people, in call-priority order. Supervisory personnel should be given the highest call priority since they should be the first to be notified in the case of a disaster.

SUBORDINATES
All key personnel need to be listed by their supervisor. In the case of a disaster, each supervisor needs to know who they need to contact and what the appropriate phone numbers are.

RISK ANALYSIS -- RESOURCES, ENVIRONMENT, PERSONNEL, SOFTWARE
This area is very critical. There are several ways of reducing the risk of a disaster from protection of computer data to protection of data center operations; from protection of vital user records to insurance. A successful risk analysis will identify areas that are lacking. Areas that, if not taken care of, could be partially responsible for a data processing disaster.

CRITICAL PROCESSING TIMETABLE
Critical processing periods are designated for each system and/or subsystem. This information indicates how long an application can be unavailable before it is needed again. It will also indicate how long the application needs to run to successfully complete. Since this information varies from day to day, it is more or less represented in calendar form. Special processing periods (end of

month, quarter, etc.) are also specified. All this is taken into consideration when making judgments about data recovery.

ALLOWABLE DOWNTIME
How long can the company survive without a computer system? The allowable downtime can be dependent on the day of the week, day of the month, and/or time of day. Typically, allowable downtime is the length of time between the running of critical applications.

With all this related information pulled together, the Contingency Plan emerges. But more than just a Contingency Plan, you also have an Audit Report that defines the mechanics of operations, the relationships of applications, the key users and their schedules, and the special requirements required to support the electronic flow of information. A document that, because it is used on a daily basis, will be kept current.

Preparation for the inevitable must begin with foresight. If we are to protect our business, and ourselves, against catastrophe and limit disaster, our data must be sound, our plan current, and our resources assured. The steps that must be taken are: making provisions for the replacement costs of data processing equipment, including the facility itself; auditing and documenting the data processing situation; updating the document as required; selecting a recovery site and binding it with a contract; and testing, at least once a year, to make sure the plan works. Anything less, and the prepartion for the inevitable could turn to disaster.