1

DEFINING THE PROBLEM

BUSINESS CONTINUITY CONCERNS

Common areas of exposure to a disaster for a business include:

- Telephone communications
- Computer processing
- Vital facilities
- Critical operations

Telephone Communications

Telephones are often taken for granted; they are seldom out of service except for brief periods, such as immediately following a storm. Older electromechanical telephone switching equipment was extremely reliable. However, consumer demand for more sophisticated service has resulted in a conversion from electromechanical to software-controlled switching systems. The advantage of such systems is that they are easily modified to provide more sophisticated options to customers. The downside is increased vulnerability to periodic interruptions in telephone service owing to software malfunction. Every time computer software is changed, the risk of error increases—error that may lie dormant for months until the weakness is exposed. Moreover, it is unrealistic to expect all software changes to be sufficiently tested to preclude failure. Many of the features are new, and models for testing are, by definition, incomplete. Therefore, it is appropriate to prepare a contingency program that will provide minimum voice communication capability during a stabilization period.

Computer Processing

Financial service organizations cannot operate for more than a day or two without computer processing, as they need this capability to service transactions.

Yet for many other organizations, this is not the case. Although many businesses are dependent on computers for day-to-day operations, it is incorrect to assume that they could not operate without this support during a relatively brief disaster recovery period that might last a week or two. The difficult part is focusing on the right issue—keeping the business running, rather than keeping the computer running.

Operating without Computer Processing Capability

Manufacturers can be exposed to several problems if computer processing is inoperable. However, careful analysis usually concludes that although inefficient, product still can be manufactured and shipped without normal computer processing support. Alternate interim processing strategies and prerequisites for manufacturing without normal computer support need to be negotiated with functional managers. Prerequisites, such as starting points, need to be included in the contingency program to ensure that they will be available when needed. For example, it is not that storeroom inventories cannot be updated without an on-line computer; the problem is lack of a "starting point" or, in other words, a record of what the inventory file looked like when the computer outage occurred. So if a prevention program includes daily responsibility to store off-site a duplicate copy of the storeroom inventory file, immediately following a computer disaster the file could be printed at another location and delivered to manufacturing as a snapshot of inventory locations and availability. Receipts and disbursements could easily be updated with a simple personal computer (PC) spreadsheet until normal computer processing is restored. See Exhibit 1.1 for vital manufacturing support functions.

Headquarters operations can also be exposed to problems if computer processing is suddenly inoperable. However, careful analysis again usually concludes that although inefficient, business still can continue and customers can still be serviced without normal computer processing support. It helps to look at administrative business functions and what alternatives are available to get the job done without computer processing.

EXHIBIT 1.1 Vital Manufacturing Support Functions

- Take orders
- Schedule production
- Order material
- Receive and store material
- Control inventory
- Pick items
- Manufacture
- Ship
- Invoice

Insurance providers are concerned about issues such as new business underwriting; determining "in force" for claims adjudication; beneficiary information; and exposure for coverage that would have been canceled under normal circumstances. In each of these instances, there are alternative strategies that, although inefficient and cumbersome, can be used to ensure business continuity until computer processing is restored.

Distributors need strategies for taking and processing orders that are normally entered into computer databases, identifying kitting requirements, producing picking documents, inventory management, producing shipping documentation, and handling returns. The question to be asked is not "What problems would you have?"; it is "If confronted with this situation, what would you do to maintain market share and service customers until normal operations resume?"

Associations and agencies are concerned about membership services, legislation and public policy, publications, research, education and training, call centers, and government regulations. In most instances, the overriding consideration is to seek solutions for operating temporarily without normal computer processing capability that will not require continual funding, such as a computer hot-site agreement, but would ensure continuity in servicing members, volunteers, and staff during a stabilization period.

Interim processing strategies for meeting administrative responsibilities without normal computer support need to be negotiated with department managers. The window of *expected* outage must be determined. For the most part, information systems managers consistently agree that they could restore computer processing capability within 10 working days (14 calendar days). So the question to be asked of department managers is not "How long can you do without . . ." or "What do you need . . ."; managers tend to understate and pad the first question, and in response to the second question tend to ask for more than they need. Both questions beg answers and initiate thought processes that are not conducive to cost-effective contingency programs and invite discussions and deliberations that require further documentation and maintenance expense. The only question to ask line managers in relation to doing without normal computer processing is "What alternate strategies could be used to continue functioning for approximately ten days without computer processing capability?" When *that* question is asked, 99 percent of the responses are positive, that is, department managers are willing to accept operating at less than 100 percent efficiency and admit what could be done to meet the challenge of temporarily working without computer processing.

The simple psychology and willingness of contingency planners to "stick their necks out" and insist on establishing a reasonable limit to an expected computer outage will, in turn, have the positive effect of persuading line managers to admit how they could survive. Establishing this "window" up front is the key to a collaborative solution. But also remember that in establishing the window, information systems managers must also accept some risk and not pad their expected recovery capability. The question is not "When are they absolutely positive beyond any reasonable doubt that computer processing will be restored?"; rather, it is "Given emergency conditions, working 24 hours a day, seven days a week, with adequate resources, when is it likely that computer processing could be restored?" On-line connectivity can wait because there are other solutions available, but being able to process data is the important requirement. See Exhibit 1.2 for a list of typical administrative business functions.

Computer processing problems could be caused by a myriad of conditions. Power grids could fail due to unanticipated drops in demand (as users of questionable systems delay initializing operations, either because corrective work has not been completed or because of other concerns) which are so severe that the power companies must bring down and reconfigure power systems grids nationally. Failures of

EXHIBIT 1.2 Typical Administrative Business Functions

- Inventory management
- Order processing
- Scheduling
- Billing
- Receivables
- Payables
- General accounting
- Payroll
- Human resources
- Data processing

satellite communications, HVAC (heating, ventilation, air conditioning, and cooling) systems, automated processing equipment, and computer hardware or software are all possible. The broad and diversified nature of this potential problem is such that testing cannot ensure that some systems might not fail.

One-time potential problem issues have two dimensions. The first is to identify steps that need to be taken to reduce the likelihood of computer-dependent operations from being interrupted and monitoring compliance with those programs, within reason. Without careful oversight by informed senior management, this approach can wind up being a boondoggle for consulting firms—fear tactics, an inordinate amount of "analysis" and "weigh it by the pound" reports, endless meetings, and a large consulting bill.

Most important, however, is to develop a fallback plan that will ensure business continuity even if computer-dependent operations are temporarily inoperable. Experience and common sense suggest that a fallback plan is the safety net that needs to be in place, and organizations that already have a facility contingency program already have one. It just needs to be dusted off and modified slightly, and it can easily be used as a fallback plan. Conversely, if an organization does not already have a contingency program for loss of computer processing, now is the time to prepare one because it will solve both problems. Chances are that if there are failures, they will be isolated and will be corrected in a matter of days, if not hours. See Exhibit 1.3 for a fallback plan development strategy.

EXHIBIT 1.3 Computer Processing Fallback Plan Development Strategy

- Identify computer-dependent vendors and services.
- Identify business functions dependent on computer processing.
- Fund and monitor a prevention program.
- Obtain senior management's approval of a corporate policy and strategy for a fallback plan.
- Develop "what if" interim processing strategies for all potentially affected business functions to protect market share and support customer service, even if normal computing capability is not available for a few days.
- Add a prevention program.
- Add an incident recovery plan.

Vital Facilities

The loss of buildings resulting from fire and other accidents is not a new threat. Nor are there any miraculous solutions. Insurance is still the most cost-effective answer. Business failure following a disaster is normally caused by a loss of assets, such as a manufacturing facility, distribution center, or office building, or an inability to support vital business functions following a disruption in normal processing capability. An inability to support vital business functions immediately following a publicized disaster can be devastating when this information is in the hands of competitors. If orders are "lost," customer service communications lines are inoperable, or inventory availability records become unreliable, even if only for a few days, it can result in a significant loss of market share, particularly with the 20 percent of a company's customers who make up 80 percent of its revenue. Most organizations have not adequately addressed the issue of how to keep the business running if a plant or office building is inaccessible for several days. In other words, the concern is not what to do if assets are destroyed, but how to continue to operate a business if primary work locations are temporarily inaccessible or unusable.

In many production and manufacturing facilities, losing normal computer processing capability would have a serious impact on efficiency, order processing, scheduling, and tracking orders, but it would not destroy the ability to somehow manually shepherd product through the manufacturing and shipping process. Efficiency would suffer; record keeping would become a nightmare, excess inventory would have to be ordered (and worked off later) to avoid stock-outs, and production rates would drop, but product would get out the door.

Losing access to an entire production facility or one critical operation could, in many instances, bring manufacturing to a halt. Without alternate solutions to ship product until operations return to normal, business failure could result. It is this possibility and its impact on cash flow that demands that companies have contingency programs for loss of normal computer processing capability and "what if" strategies for a temporary loss of access to production facilities.

Raw material and component parts might be sent to alternate manufacturing sources; components might be purchased instead of manufactured; excess regional production capacities might be temporarily leased; "second-choice" production alternatives might be approved; inspection and quality control procedures might be changed; and some items might be shipped direct. The important issue is for manufacturing managers to take the time to "think through" which alternatives are most likely to work and which are most cost-effective. It is important that these alternate production methods or "what if" strategies be documented in writing so that: (1) their workability can be validated annually; (2) any prerequisites, such as maintaining daily backup copies of inventory status reports or files off-site to support alternate manufacturing methods, can be identified and inserted into a prevention plan; and (3) crisis management activities, such as using the most recent stock status reports as a basis for insurance claims, are added to the incident recovery plan.

Only a Computer Recovery Plan

Which comes first, the chicken or the egg? Which comes first in contingency planning? Recovering lost technology or keeping the business running? *The business continuity program should come first.* In fact, data processing plans to recover technology that are developed before interim processing strategies are explored normally result in an excessive amount of resources committed to redundant computer processing capability. Auditors are becoming increasingly critical of the lack of business continuity programs and are beginning to emphasize this area more than the loss of computer processing technology. After all, what good is a restored computer if users are unable to keep the business running immediately following a disaster? If you are just getting started in contingency planning, you should address the business continuity issue *before* you worry about redundant computer processing capability.

Current Program May Not Work

Less than 25 percent of business organizations have a workable contingency program. Some programs look good on paper—but would not work if they had to be implemented. Programs that are not viable usually have three things in common:

1. The focus is on keeping the computer running rather than on keeping the business running.
2. No one has taken the time to identify alternate procedures to support functions that *normally* rely on computer technology but could actually survive a stabilization period using alternate methods.
3. The program contains unnecessary detail and professes to cope with problems that are typically nonexistent.

Exhibit 1.4 lists common reasons why many contingency programs will not work.

EXHIBIT 1.4 Common Disaster Recovery Plan Problems

- Focus on recovering computer technology at costly hot sites, rather than on sustaining business continuity until temporary computer processing capability can be restored locally
- Lack an awareness and education program that enables functional managers to understand the importance of their input and are willing to participate in program development
- Do not explore alternate procedures that could sustain vital business functions (that normally are dependent on centralized computer processing) until computer processing capability is restored
- Provide excessively detailed procedures when guidelines are all that are needed

CHARACTERISTICS OF A SOUND PROGRAM

A contingency program should be reviewed annually to ensure compatibility with business practices and to integrate lessons learned from new disasters and test results into more cost-effective solutions. Many times it is helpful to have someone other than the individual who developed the program to conduct such a review. It is difficult to be objective when reviewing your own work.

A *corporate contingency program* approved by senior management is a requirement. This document should emphasize that (1) providing 100 percent redundancy for all types of physical disasters is simply not practical; (2) documenting detailed alternate procedures for an infinite number of combinations of possible disasters is also not realistic and would create a "monster" to maintain; and (3) departmental managers are the architects of "what if" interim processing strategies that will serve as guidelines to ensure business continuity following a disaster.

Assumptions under which a program is developed should be stated to clarify expectations and avoid excessive documentation. Examples of assumptions include:

- Qualified personnel will be available to execute the program.
- Healthcare agencies and institutions will be operational.
- A building evacuation plan exists.
- Inefficiencies are expected during a stabilization period.
- Incoming telephone calls will be rerouted within two hours.

A prevention program should reflect disaster prevention responsibilities; ongoing education and training requirements; testing programs; other sound risk management practices; and any additional measures required to support relocation strategies, interim processing strategies, or technology restoration plans. The primary purpose of a prevention program is to reduce the likelihood of a disaster, such as physical security programs, and to take steps that will minimize impact, such as storing computer files off-site, if a disaster does occur.

An incident response plan should ensure an organized response to a facility-related disaster and provide for the rapid rerouting of incoming phone calls and a strategy for restoring computer processing capability. It also includes relocation strategies, minimum staff required during a stabilization period following a facility disaster, notification for personnel and customers, damage assessment, and media management.

Interim processing strategies, in the absence of other instructions, will be used to maintain business continuity if facilities become inaccessible following a facility disaster. Emphasis is on retaining market share, servicing customers, and maintaining cash flow. Business continuity strategies should have been developed by discussions with department managers familiar with existing business practices and alternative options. These strategies should also include functioning without normal computer support (computer operations may not be restored for days) and with minimum staff if relocation is needed.

COST-REDUCTION OPPORTUNITIES

The most costly mistake that a business can make in developing its program is to have it aimed at keeping technology running instead of keeping the *business* running (Exhibit 1.5 provides an action plan for cost savings). Contingency programs that are *not* cost-effective usually have three characteristics:

1. Program focus is on keeping technology running rather than on keeping the business running.
2. No one worked with functional supervisors to develop alternate procedures to support vital business functions until normal processing capability is restored.
3. The program fails to recognize that businesses could continue to function for a week or two without normal computer processing capability.

Cost-reduction opportunities exist due to individual mistakes that alone sound innocuous but, in combination with other related mistakes, spell bad financial judgment. First, an error in interpretation of the Foreign Corrupt Practices Act by accounting firms led to criticizing clients for “lack of a computer disaster recovery plan.” That criticism was misdirected. What was actually needed was interim

EXHIBIT 1.5 Action Plan for Cost Savings

- Initiate a cost reduction project.
- Have outside specialists (other than those who developed the existing plan) conduct a plan evaluation.
- Focus only on sustaining cash flow and servicing customers during a disaster recovery period.
- Deal with business functions, *never* with computer systems.
- Work with functional line managers and first-line supervisors to analyze options.
- Develop cost-effective guidelines that will sustain vital business functions.

processing strategies to be used in the event of a disruption in normal data processing technology. Placing undue emphasis on computer technology, instead of business continuity, was the mistake. Because the focus was on the wrong issue, it led organizations to assign project responsibility to the wrong department. Had the objective been business continuity, project responsibility might have been assigned to a staff person positioned to facilitate a strategic plan. However, with the focus on computers, responsibility was assigned to data processing personnel, who are normally not trained in the synergistic process used to develop strategic programs.

In many instances, these errors resulted in technical solutions being substituted for sound business judgment because the situation was defined as a computer problem that needed a computer solution. The result for many organizations has been excessive expenditures for redundant processing. Taken over a period of 20 to 30 years, this amounts to millions of dollars being wasted. Exhibit 1.6 provides a brief synopsis of why cost-reduction opportunities exist.

EXHIBIT 1.6 Why Cost-Reduction Opportunities Exist

- Initial program focused on getting the computer running quickly at costly computer hot sites rather than waiting a few more days to restore operation at a cold site
- Plan development responsibility assigned to data processing rather than to a staff position
- Lack of specialized problem-solving process that continually links the low probability of occurrence with the need for cost-effective solutions

How to Contain Program Development Costs

Minimizing contingency program development costs centers on five interconnected issues: (1) plan development sequence, (2) mind-set, (3) assumptions, (4) communications, and (5) a specialized problem-solving process. If any are missing or not dealt with appropriately, development costs will be excessive, the end product will not be of good quality, and it will take forever to complete the project.

Plan development sequence means positioning and selling senior management on a corporate contingency planning policy and strategy, and documenting this corporate policy and strategy in writing *before any other activities are undertaken in the program development process.* If this is not the first step, then problem-solving practices are used, which are totally inappropriate. For instance, conducting a "business impact analysis" to determine what is critical *under normal conditions* is unproductive. A definition of *critical* is needed. In a contingency planning context, critical is not what receives the highest priority under normal operating conditions because we are not worried about operating under normal conditions. We are concerned about which business functions will be so impaired as to threaten business continuity following a disaster because they lack alternate strategies to operate under those conditions. What is critical at the time a physical disaster occurs depends on what alternative strategies can be used to support that business function. If a particular business function has alternative methods to service customers for a two-week period when computer processing is inoperable, then there is nothing critical because business continuity is not threatened.

The worst mistake is to begin a contingency program project by developing a computer recovery plan based on an assumption that the business could not operate for two weeks without normal computer support and that prioritizes application recovery based on the wrong definition of critical, as described in the last paragraph. It takes someone with seasoned contingency program experience to prevail in establishing the proper development sequence. The benefit, however, is that a program can be completed in 30 days and at a fraction of the cost.

Mind-set is the philosophy under which a contingency program is developed, and failure to document the proper mind-set in a corporate contingency planning policy and strategy will result in false starts, lack of cooperation, and unnecessary expense. For instance, the objective of the program should be "survival," not "business as usual," immediately following a physical disaster because the latter demands ongoing expenditures that annually take away from the bottom line and are not justified given the low probability of a disaster. A more cost-effective mind-set is to reduce or eliminate reoccurring expenditures, such as computer hot-site fees and testing, and instead authorize expenditures on an as-needed basis when and if a disaster actually occurs.

Remember that a contingency program is only a reference document. Managers will decide specifically what to do at the time a disaster occurs, depending on how much damage is done and what the prognosis is for reentering the building.

Communicating effectively can have an impact on completing a contingency program on a timely basis. Repeated communication of corporate contingency program policy and strategy to senior executives, department managers and key supervisors, and to staff developing a program is extremely beneficial. (Remember, individuals quite often do not comprehend information presented only once.) It constantly reminds them of the need to control program development costs, presents a "road map" that keeps them on the path to timely completion, and acts as a deterrent to a natural tendency by everyone to include too much detail.

Contingency planning for disasters requires a different problem-solving process than is used to solve other business problems because of the low probability of a disruption to business continuity due to a physical disaster. Traditional problem-solving techniques used by most consultants and corporate staff involve lengthy fact-finding studies, as well as addressing and resolving issues in painstaking detail. This is because the problems being addressed will affect the everyday operation of a business. This is not true for a facility contingency program. Because it is extremely unlikely that a serious disaster will ever affect a specific site, there is no justification for lengthy studies to gain consensus on what is most critical or for formulating detailed plans. Interim processing strategies need to be documented for all business functions regardless of their relative criticality, and detailed documentation is inappropriate. The contingency planning process is a specialized strategic planning methodology designed to address this need and

EXHIBIT 1.7 Guide to Contain Program Development Costs

- Prepare a program development "road map."
- Assume a mind-set to minimize program development costs.
- Document assumptions on which a program is based.
- Communicate often to executives and line managers.
- Authorize a program development process designed to minimize program development costs and enable a prototype program to be completed in 30 days.
- Use internal resources to roll out a prototype program to other locations.

to minimize program development costs. See Exhibit 1.7 for a guide to contain program development costs.

Where to Look for Cost Reductions in an Existing Computer Disaster Recovery Plan

For organizations with a computer disaster recovery plan, there are three areas that should be examined:

1. Plan maintenance
2. Backup computer hot-site subscription fees
3. Backup computer hot-site testing

Exhibit 1.8 indicates major areas that should be investigated for cost reductions.

EXHIBIT 1.8 Where to Look for Cost Reductions

- Maintenance
- Scope
- Amount of detail
- Documentation structure
- Backup communications
- Cumulative cost of backup processing subscription fees over a 20- to 30-year period
- Testing costs, including disruption to normal duties

Plan Maintenance

Maintenance expenses are directly related to the volume of material, level of detail, and documentation format. A great deal of "Do we really need to include this?" kind of thinking is required when a program is under development or being evaluated. If this approach is not taken, issues that should be left out will be included, thus adding unnecessarily to maintenance costs. The objective is to leave out of a program those issues that can be dealt with at the time a disaster occurs or that cannot be specified until the impact of a specific disaster has been assessed. Remember that the specifics of many emergency response activities cannot be determined until after damage assessment of a specific disaster or incident.

Preparing a quality program that clearly and concisely addresses only relevant issues requires considerable experience, good business orientation, and a structured format. One problem is that most software documentation packages demand detail that is not needed; in fact, it gets in the way of doing a good job.

Hot-Site Subscription Fees

Backup computer hot-site requirements should be examined for cost-reduction potential. In today's cost-sensitive business environment, computer hot-site and cold-site subscription fees can be a source for large, ongoing cost reductions.

For most organizations, other than banks and communications providers, backup computer contracts with hot-site vendors are a waste of money. They are not needed, because in a crisis such as a disaster, a computer operation usually can be restored within a one- to two-week period somewhere, somehow, and most functional supervisors can find other ways to keep vital business functions running until processing capability can be restored.

Testing

The cost of resources tied up in the testing of backup computer hot-site operations can be considerable. The cost of planning, preparing for tests, scheduling, arranging transportation, testing, evaluation of results, and sustaining corrective action programs can drain an organization of resources that should be used to address daily operating requirements.

Audit Concerns

Auditors are becoming increasingly concerned about the viability of contingency programs (Exhibit 1.9 lists some of these concerns). Because the data processing department is an organization's focal point of information technology and the department most conspicuously vulnerable to a disaster, management most often looks to data processing personnel to develop data center restoration and application recovery programs. This approach is *not* appropriate for developing "what if" interim processing strategies.

Data Center Restoration and Application Recovery

The data processing department should address data center restoration and application recovery; however, the development of interim processing strategies is best accomplished by specially trained professionals.

Developing "What If" Interim Processing Strategies

The heart of any worthwhile program is the development of interim processing strategies. This requires awareness and education and involves a highly specialized problem-solving process. In most instances, it is not realistic to expect in-house personnel (data processing or any other department) to serve in this role. Effective interim processing strategies are not a data processing problem; they are a corporate issue, requiring an organizationwide problem-solving process.

EXHIBIT 1.9 Audit Concerns

- Lack of awareness and education
- Department managers not sufficiently involved in developing alternate procedures
- Contains unnecessary detail
- Not testable
- Technology oriented rather than business oriented
- Not cost-effective

Involving Department Managers

The most serious mistake is to develop alternate strategies for how specific administrative functions or manufacturing operations will operate during a stabilization period following a disaster, without the understanding and support of line managers who would have to use them following a facility disaster. Department managers are the only ones who have the knowledge of what alternate strategies might be both workable and practical. They are also the ones with on-the-job knowledge that can be most creative and resourceful in analyzing these options. The way that department managers are approached about participating in developing a facility contingency program can make the difference between cooperation in searching for cost-effective solutions or protecting their own interests. Most department managers are overworked and have to be selective about what projects take up their valuable time. They focus on getting things done and, as a result, have little time for a strategic planning project like helping to develop interim processing strategies, particularly for a theoretical disaster that is unlikely to happen.

Department managers need to be dealt with carefully and respectfully if their cooperation is expected. Conduct executive briefings specifically for them. Keep the briefings concise, no longer than 30 minutes. Explain the company's exposure to a facility disaster; explain that such a disaster might affect the company's ability to stay in business and that alternate strategies to service customers and maintain market share need to be developed. Windows of expected outages for operating without normal computer processing support and the building's inaccessibility should be resolved ahead of time and discussed in the briefing. Never ask "How long could you do without?" because it causes the department managers to go on the defensive, rather than being cooperative because they have no frame of reference (window of expected outage) within which to be creative. This is a crucial step because windows of expected outage psychologically permit department managers to "get their arms around the problem" and deal with it in a positive manner.

If windows of expected outages are not stated up front, department

EXHIBIT 1.10 Involving Department Managers

- Conduct briefings for department managers.
- Explain exposure to business continuity.
- Describe expected outage windows for computer processing and building accessibility.
- Take notes on alternate interim processing strategies.
- Summarize business continuity strategies.
- Obtain department manager's approval.

managers will be unwilling to stick their necks out to develop alternate strategies because the problem statement is too broad. Finally, do not ask department managers to write anything down. The individual developing the program should take notes and summarize the managers' suggestions in short concise statements, with no editorializing or detailing "how" they will be done. The capabilities and judgments of the department managers are adequate, and anyway, the "how" will depend on the specific nature of a disaster, and no one knows exactly what that will be. Interim processing strategies should be reviewed and approved by the department managers. See Exhibit 1.10 for involving department managers.

NEED FOR COST-EFFECTIVE SOLUTIONS

The low probability of a disaster means an obligation to search for the lowest-cost solution. It does not make economic sense to allocate the same level of resources to solve a problem that has a high probability of happening as one that will probably never occur. If you do not continually make a strong case for this mind-set, it will be forgotten, and well-intentioned individuals will select solutions that are sophisticated and costly. It is easy to rationalize expenditures conceptualized in good faith, unless there is an overriding project philosophy to *contain costs.* This cost-control philosophy should be embedded in the program development methodology so that every solution is examined in search of more cost-effective answers. Assumptions and generalities must continually be challenged in light of the overwhelming interest in *low-cost* solutions.

Allocating resources to develop a contingency program is a difficult task, made even tougher by the fact that it is virtually impossible to cost-justify how much to spend. There is a big difference between conducting a risk analysis or business impact analysis and cost justification. It can be calculated with reasonable precision how much would be lost per day if a particular production line could not operate. However, because there are no reliable probability statistics on the impact of specific disasters on *business continuity,* the cost-justification calculation cannot be completed.

This difficulty is compounded by the fact that cost-conscious executives are reluctant to commit funds for a *detailed program* for an event of which the scope and dimensions are unclear, such as a sudden disaster. This is because most plans imply precise logistical and procedural commitments that translate into high maintenance costs. Given the low probability of a disaster and the high cost of redundancy, the goal following a disaster should be to stabilize operations. The real challenge lies in developing cost-effective alternate procedures to support vital business functions until normal processing capability can be restored. Loss of efficiency during a disaster recovery period should never be used to justify spending more money than necessary on alternate interim processing strategies that would be in effect for only a few days.

BACKUP

When a service fails, the primary responsibility of the provider must be *recovery.* The primary responsibility of the user is *continuity of operations.* When there is a power blackout, the consumer worries about how to get along without electricity, whereas the public utility is concerned about how to restore electricity. Similarly, data processing is responsible for a backup power supply should electricity fail. The materials department, however, is responsible for a contingency program for inventory control if the computer fails, Included in this rationale is the somewhat less obvious fact that users have far more choice and flexibility than the provider. In general, the only strategy for the provider that will serve all users is instant recovery. If that can be achieved, then, by definition, there has been no disaster. The problem is that maintaining duplicate facilities is prohibitively costly.