MCAA Management Methods Manual

Bulletin No. CP 8
File: Corporate Planning

Bulletin

Disaster Recovery

Getting Your Business Back in Operation after a Disaster

Overview

Every company should have plans to deal with emergencies and disasters. Plans well executed could save lives, minimize loss of assets, and even save the entire business. A catastrophic event to your building does not need to result in catastrophic losses for your business.

How well you are prepared for such an event will make all the difference in assuring business continuity and having peace of mind. Being prepared means having:

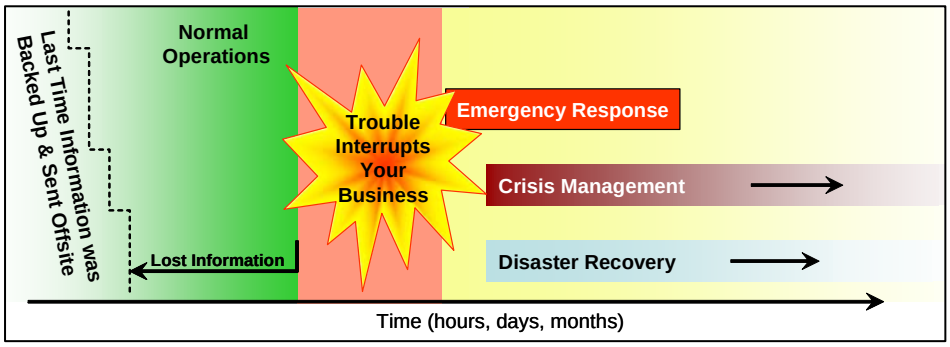
- A strategy to protect or duplicate vital resources
- A plan to respond to emergencies
- A plan for recovery from a disaster, including access to vital resources
- Resources to support your recovery plans

Often, for convenience, **Emergency Response** and **Disaster Recovery** Plans are written as a single document. However your plans are written, they need to be current and thoroughly familiar to managers and certain staff who will lead the organization in the recovery effort. This MCAA Management Methods Bulletin will guide you through developing a **Disaster Recovery** plan or improving an already existing plan.

This bulletin corresponds well to various public standards, including ANSI NFPA1600, BS25999, HIPAA Security Rule and Sarbanes-Oxley guidelines that may pertain to your business.

Emergency Response vs. Crisis Management vs. Disaster Recovery

This MCAA Management Methods Bulletin is about **Disaster Recovery**. The differences



between **Emergency Response, Crisis Management** and **Disaster Recovery** are often confusing, and it is important for you to understand those differences. The above graphic depicts a timeline showing when each of these plans is utilized after a significant event causes an emergency, crisis, or disaster:

Starting at the left, note the dotted line that represents times during normal operations that information (hard or soft copy) critical to your business is backed up from one media to another (usually disk to tape) and the backup copy is sent and stored off site in a safe

location. Different data are backed up at different times. When a business interruption occurs and critical information is lost, backup copies from different points in time are then available for use in staging a recovery. The time between the last backup and the interruption is a period during which new information may have been added but is no longer available. That data is now lost, and any information that is not an affordable loss must be recovered from paper files, business partners, clients, etc.

Emergency Response

Typically, a substantial interruption to business operations is followed quickly by your **Emergency Response**, as shown in the table above. Steps are taken to protect employees, notify local emergency units, assess the situation and salvage physical assets where possible.

Crisis Management

This is followed immediately by **Crisis Management**, which involves contacting employees and suppliers, taking steps to prevent further damage and secure facilities, and dealing with customers, stakeholders and the press. Sometimes, a "crisis" is not operational and does not affect a facility, such as incidents related to sudden market shift, product failure, labor relations, executive succession, public perception, or a cash crisis. Each of these incidents requires executive intervention and serious attention and falls into the category of **Crisis Management**.

Disaster Recovery

If the incident is an operational interruption, such as by fire or flood, we consider this a "disaster," and **Disaster Recovery** protocols go into effect, as described below. **Disaster Recovery** is the subject of this bulletin.

In the section below, we define the elements in the chart and discuss how they relate. Later, in the section *Why the Difference Matters to You*, we discuss how you would need to respond.

Definitions

For the purposes of this bulletin, the meanings of certain terms are detailed as follows:

Emergency: an urgent, usually unexpected occurrence requiring immediate action prior to the decision to declare a disaster.

Crisis: an unexpected de-stabilizing event that may threaten an organization's personnel, revenue, reputation or ability to deliver customer service.

Disaster: any significant disruption that forces a mission-critical business function to relocate, at least in part, to a location different from its normal location, on a temporary or permanent basis.

NOTE: A "disaster" falls into the "crisis" category; an "emergency" can develop into a crisis. Many crises are not *operational*, such as *product failure, labor relations, adverse international events,* or *sudden market shift*. A "disaster" is always a crisis, but it is only one type of crisis.

SAMPLE SCENARIO: It is mid-morning and severe weather is predicted. Decisions need to be made about whether employees should be sent home. This is an ***emergency***, for which immediate action (decision-making, preparation for the storm and communication with personnel) is necessary. If the storm hits hard, the facility may be damaged and workers may be frightened. This is a ***crisis***, where senior management must deal with employee concerns and welfare, communication with clients and vendors, possible first aid, facility repair, productivity, and a host of administrative issues. If some or all of the business processes need to be moved to another facility, the scenario becomes a ***disaster***. It requires logistics for workforce mobilization, notification of personnel, distribution of supplies to the recovery site, and allocation of technical resources, such as computers and telephones.

Why the Difference Matters to You

Emergency Response is about people – their safety, their emotional well-being, and their behaviors under pressure. (It is not about business resumption.) It is also the period of time during which the determination is made as to the extent of the potential impact and the

type of management response that is appropriate under the circumstances. Emergencies require short term response.

Crisis Management is about organizational control during a crisis. It provides for executive, employee, client and vendor inter-communications, problem resolution protocols, common language among decision-makers, administration, and coordination of service continuity activities. It also addresses public and customer relations immediately following a serious incident. It typically follows the **Emergency Response** and is longer term.

Disaster Recovery is about re-establishing and sustaining the flow of mission-critical business processes to serve business objectives at an alternative site. With continuous process flow, a business can maintain a strong financial basis, keep its good reputation, comply with regulations and the law, and serve its clients.

Your plans for **Emergency Response** include fire drills, notification of personnel during severe weather, dealing with medical situations, suspicious activity at your office, elevator failure, bomb threats and the like. **Disaster Recovery** efforts typically come into play once the emergency has been or is being handled. This bulletin on **Disaster Recovery** focuses on business resiliency and continuity. We discuss **Emergency Response** and **Crisis Management** only as they relate to **Disaster Recovery**.

A Word about Pandemic Response Planning

A pandemic is a worldwide epidemic. There has been a good deal of press for the past few years about the potential for the H5N1 virus (also known as "Avian Flu" or "Bird Flu") to become transmissible between humans. To date, the virus seems to be contagious only from birds. Severe pandemics occur approximately three times per century and generally kill millions of people. It is a serious matter on a personal level, since the current mutation has killed more than half of the people it has infected. The virulence of the virus is likely to diminish if it mutates to a human-transmissible form, but it will still be dangerous.

Such a pandemic could have a serious impact on businesses, and most large corporations are considering how they would respond to the unavailability of large percentages of personnel for several weeks. Epidemiologists estimate that the U.S. workforce could be diminished by 30 to 60 percent during an H5N1 pandemic.

As we have defined "disasters" as the need to move functionality to another location, pandemic response does not fit neatly into the **Disaster Recovery** arena. However, it is not to be taken lightly, and you may want to consider the matter in your **Crisis Management Planning**. There are things you can do to mitigate the impact of a workforce outage and also preventive measures you can take to limit the spread among your employees. This is a complex, separate topic that lies within the scope of **Crisis Management Planning**.

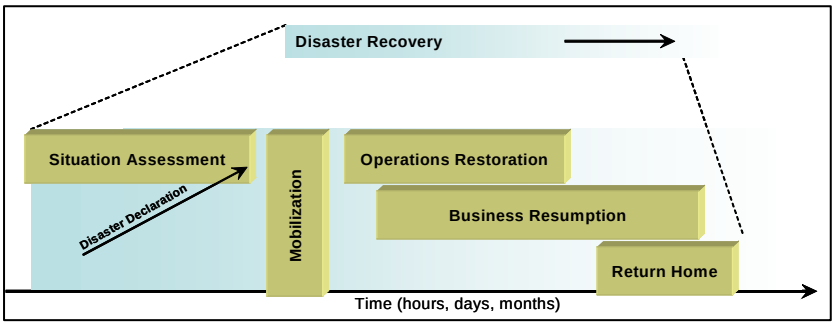
What You Need for Disaster Recovery

The Disaster Recovery Process

To recover from a catastrophic event that causes a disaster, you need to know:

- How to get out (**Emergency Response**)
- Where to go when you do (**Disaster Recovery**)
- What you'll need when you get there (**Disaster Recovery**)
- What to do after you arrive (**Disaster Recovery**)
- What to tell employees and others (**Crisis Management**)

In the diagram below, we focus on the **Disaster Recovery** process. This process is represented by the bar labeled **Disaster Recovery** in



the diagram on page 1. In the diagram above, we show additional detail.

Once the **Emergency Response** is in progress, principally for the safety of personnel, a team can begin to assess the situation. This assessment may result in the "declaration" of a disaster. It is important to restrict *authorization to declare* to high-level executives, since the resulting movement of function and people could be an expensive proposition.

As soon as a disaster is declared, employees must be mobilized to set up functionality at an alternative site. This is largely a technical matter with assistance from your facility and administrative departments. If you have subscription services from vendors who provide recovery services, they need to be contacted to activate the services you've been paying for. For example, if you have been subscribing to a recovery site, they need to prepare for your arrival. Your off-site data storage services vendor needs to move the latest data to your recovery site.

At your alternative location, technicians need to set up, configure, connect and test equipment, install software as needed, and prepare the site for use. Once the site is ready for use, your workers need to execute their recovery plan roles – sending the right people at the pre-planned times and knowing what to do when they get there. Meanwhile, technology personnel continue to prepare for more arrivals and support the employees who need special help adjusting to the new environment.

Returning home shifts recovery steps into reverse and requires just as much care.

Strategy

This section summarizes six areas important in recovering resources to maintain business strength in the face of disaster: **Information, Tools, Workspace, Processes, Plan Maintenance,** and **Funding**. Following these summaries, we provide a level of detail that may help you to write your **Disaster Recovery Plan**.

Minimizing Information Loss: Business information is stored in many forms – computer readable data, ledgers, paper files, books, and human memory. It is difficult to recover the latter if people perish, but most other information media are recoverable if you plan appropriately. There is some information you can reconstruct or do without and some you can obtain from outside entities (publishers, regulators, vendors, competitors, etc.), but much information critical to the business requires pre-disaster protection from permanent loss.

Tools to Continue Operations: Consider the tools you need every day to produce the results clients expect and that you need to run your business. Without computers, trucks, and flat-bed printers, could you produce those results? Could you continue to operate?

Place for People to Work: Your field personnel would continue operating even if your headquarters were unavailable – provided headquarters functionality could be sustained and office workers could continue to support field operations. Therefore, office workers need a place to work. Some employees might be able to work from their homes if the technology and controls are in place to make that possible.

Knowing What to Do: This is the recovery plan document that tells people where to go, what to do when they get there, who is accountable for what, what resources are available for recovery, and what information you will need, such as phone numbers of recovery team members, other employees, and vendors.

Rehearsing and Maintaining the Plan: Shortly after any recovery plan is declared complete, it is out of date. If your business is like most, things change daily. Your plan needs to be maintained in a form that is easily modifiable and easy to re-distribute. Most plans are maintained online in whatever word processing software is used in your company. Even with a current plan, however, it isn't much use if people don't know what it contains and how it should be used. The best way to accomplish this "orientation" to the plan is by staging a simulated incident for employees to experience. These rehearsals are usually called Table Top Exercises.

Funding the Recovery Effort: Insurance coverage could help you financially during and after the often painful experience of recovering your business functionality. Moreover, having adequate coverage could get you back on line quicker.

The following sections detail the above strategy areas…

Minimizing Information Loss – Data Recovery

Most business executives understand that there is some information they cannot afford to lose. If that information resides only in certain people's memories, you know it must be documented to protect it. Even outside of a business disaster, people can become unavailable, and their unavailability should not be cause for the business to suffer. If the information is only in paper files and it is critical, you may need to copy those files (electronically by scanning or on more paper) and store the copies offsite. Similarly, electronic data can be lost if it is not backed up and stored in some form at another location. Consider the diagram on page 1 of this bulletin. Working backward from the business interruption event, note that the amount of data lost depends upon the last time that data was backed up and sent off site. There is a technique called "data replication" that can shorten that time-frame to subseconds, so that virtually no data is ever lost because at any given moment, the data just entered was immediately sent off-site over a remote network. You may consider this capability for extra-critical data.

Data shared with clients or business partners may not be lost if your facility is lost, but you need to ensure that your clients or partners know of this dependency and would be ready to help you replace that data in the time you would need it following a disaster. Likewise, if the data you cannot afford to lose includes books, professional documents, selected magazine articles, product information, and off-the-shelf computer program disks, make sure you know how to get this information in the time needed by listing the items you receive from vendors, book-stores, etc. as well as corresponding contact information. Maintain this list off site.

Tools to Continue Operations

If you have accounted for the recovery of data you cannot afford to lose by backing it up and storing it off site, you have taken the most important step to recovery. However, you now must consider where you will restore that data.

For backup data on computer tapes, you will probably need to load those down to disks, and you will need computer "servers" to process the information and make it accessible to employees and possibly to clients and vendors. You will also need computer networks (LAN for "Local Area Network" and WAN for "Wide Area Network" where *local* means *in office*), which consist of equipment and telephone lines. For telephone lines, you will need telephones and the centralized in-office equipment that runs those phones. Printers and scanners also are needed and must be connected to your computers, and photocopy machines that do not require computer connections are just as important. These things are basic to your technical services that will need to be restored, but tools are not just about computers and phones.

Do field personnel park their business-owned trucks in your office parking lot? If you lost the office building and the equipment stored nearby, assume that you could lose that equipment. Ask your field supervisors to make a list of essential equipment that field employees need and that are typically stored in the office or just outside. Then, have someone investigate how long it might take to replace this equipment. If the replacement turnaround time is longer than the time you would need the equipment, you might consider having extra equipment standing by, storing your equipment in another place, or distributing your equipment across multiple sites.

Place for People to Work – Alternative Workspace

Your business cannot function without people. As obvious as that sounds, even large corporations forget that their people need a place to work, and that place must be equipped with resources that people need – computers, file cabinets, desks, phones, high-speed networking equipment, etc. Furthermore, if

certain groups of people need to be near other groups in order to be productive, separate hotel rooms, for example, may not work.

You are well advised not to plan for enough alternative workspace to accommodate all personnel immediately following a disaster. The more you pre-allocate, the higher the cost. Consider how many people you will need in the first few hours, the first day, the first week, etc. If you are using a commercial recovery-site, negotiate for lower subscription fees in exchange for higher occupancy fees at the time of a disaster. The latter should be covered by Extra Expense Insurance.

Knowing What to Do – a Documented Plan

The most important recovery plan is the one that tells people what to do at the time of a catastrophic event. This plan should be as clear and succinct as possible so that anyone following the plan is not distracted by unnecessary and extraneous instructions and facts. For example, when a disaster occurs, few people are concerned about how the plan was maintained or tested or who backed up the right data and how it was sent off site. Those elements of preparedness belong in a supporting plan.

Rehearsing and Maintaining the Plan

A plan untested is better than no plan at all – but not by much. Testing the plan at the time of a disaster allows no room for failure. At the very least, the technology components of your plan should be tested. Other tests are possible, including notification tests and Table Top Exercises to give key employees a top level view of the plan and a chance to practice it under safe circumstances where mistakes are allowed.

Plan maintenance procedures need to be set up so that the plan is updated periodically. Names and contact information will change, vendors may change, and the need for recovery resources may increase or decrease. Review and update your plan at least quarterly, and keep in mind that the more often you update the plan, the smaller the number of updates.

Funding the Recovery Effort – Insurance

No amount of financial compensation after a disaster will ensure that you will be able to continue critical business functions. Only a proper, viable plan with supporting resources will make that possible. However, insurance coverage could provide financial resources that will help you to fund the recovery effort and ease the strain during difficult times. Having adequate coverage may help you to recover more rapidly from a catastrophe. The following types of insurance apply to operational crises:

Extra Expense Insurance: This type of insurance is designed to pay for expenses you would not ordinarily incur unless you had a disaster. For example, it covers fees to: retrieve data from an offsite storage location, use a recovery site for equipment, or occupy alternative workspace.

Business Interruption Insurance: This type of insurance pays only for "loss of profit" due to an outage. It does not cover all revenues that you might incur by not doing business. Furthermore, you will need to document for the insurance company exactly how much profit you would have gained had the disaster not occurred.

Insurance to Cover Loss of Assets: This type of insurance is designed to pay for the loss of assets specifically identified in the insurance policy. Typically, it does not cover consequential losses. For example, if you are able to put a value on certain data, but the loss of that data causes major business disruptions that result in other losses, the insurance company will pay only for the value you assigned to the data.

A common question: "Will a recovery plan reduce my insurance premiums?" Not likely, but you should speak with your insurance agent. We do not recommend doing recovery planning to reduce insurance premiums. Taking preventive measures may help. Do what your business requires to ensure the ability to survive. If other benefits follow, so much the better.

Standard Methodology

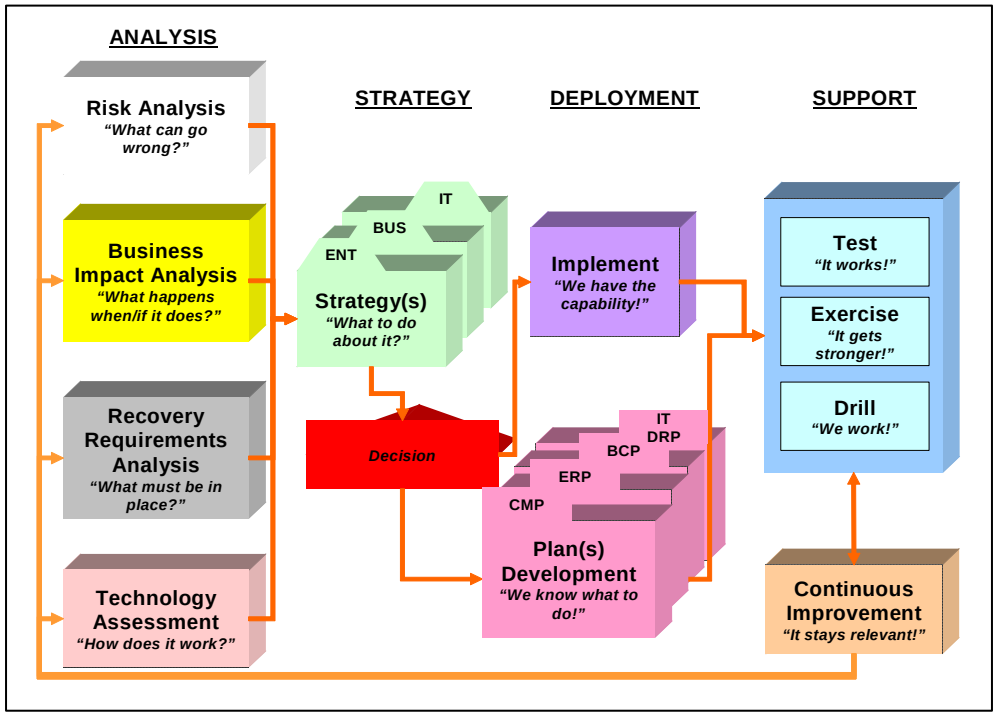
Large and small organizations have similar needs in arriving at a recovery strategy. You need to know, for example, the kind of damage a disaster could do to your business. Large corporations conduct a formal "Business Impact Analysis" for this purpose. In smaller firms, it is possible to do such analysis more intuitively, but you still need to be aware of what you can and cannot afford to lose. Corporate contingency planning has evolved over the past decade to employ planning tools to achieve a specific order of objectives. The following diagram, formalized by Eagle Rock Alliance, illustrates this order of objectives.

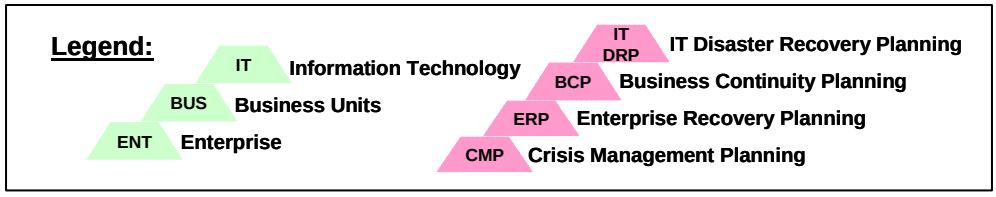
The Simple Approach – a Quick Start

The simple approach to **Disaster Recovery** Planning is to ensure the ability to survive. Cover your greatest exposures first with a simple plan – not necessarily well-documented – and put a program in place to gradually build upon that plan. Protecting your greatest exposures is a 1-2-3 process:

1. **Protect your employees** with training in **Emergency Response** procedures.
2. **Protect critical information** by having data backed up and cycled off site regularly.
3. **Protect business processes** by arranging for an alternative location where your most critical people can operate temporarily.

The nemesis of the simple approach is thinking that you need a full-scale recovery plan tomorrow. Not true. As with any business function, you need to start somewhere. Strive for progress, not perfection. You can tune your most basic program as you have time and funds.





Shortcomings of the Simple Approach

Once you have started with the simple 1-2-3 approach, take a breather, but do not stop there. As Will Rogers asserted, "Even if you're on the right track, you'll get run over if you just sit there."

While you were developing the first simple, *business survival* plan, you may have found items that you would like to have that are better than mere survival. You may want, for example, to ensure the ability to position your business for continued profitability. When you consider the issues beyond mere survival, some questions will occur for you: What can go wrong, and what might you lose when it does? (See the "Standard Methodology" diagram to the left.) What would I need to

have in place to minimize disruption to critical processes, and how would the recovery technology work?

The simple approach is a great start, but not the end of the road. Ultimately, it's smart to have a comprehensive and well-documented plan.

If You Do NOT Have a Plan…

You may not have a documented plan, but even if you have not started with the "simple approach," you probably have the basis for a "strategy" in mind. Most organizations do. For example, you may have thought about the need to back up critical information and store it at an off-site location. You may have actually arranged this activity but do not consider it part of your **Disaster Recovery Plan.** You may have considered where critical personnel might work if your primary location were to become unavailable. Even if you have only thought about these things or are just beginning to consider them based upon this Bulletin, you are headed in the right direction. Consider the 1-2-3 Simple Approach above to get started, after which you can rest assured that you've postured your company for a *good chance* to survive in dire circumstances. Having accomplished that feat, you've bought yourself some peace of mind and some time to take the next step. Following are some things you can do to ensure survival.

Beyond the Quick Start

- Check out free resources, such as www.ready.gov for **Emergency Response**.
- Assign a planner or planning team from within or outside your firm.
- Identify your greatest risks.
- Develop a strategy to deal with the greatest risk.
- Write a plan to document the strategy.
- Implement the plan.
- Socialize the plan among the stakeholders.

What to do next

See the next section of this Bulletin.

If You Already Have a Plan…

Your existing recovery plan may be all that you need. It may cover those exposures which you consider to be the most damaging and most likely. You may feel that your organization can handle smaller risks without significant planning or preparation. On the other hand, previous planning may have been constrained by limited funds or insufficient time to plan, or maybe you thought it was enough at the time but have a different perspective today.

Plans are typically dynamic and are always subject to change as business circumstances change. It is usually worthwhile to perform a regular review of your plans.

Improving Your Plan

The first thing you need to do is to take stock. Where is the plan meeting business objectives and where is it not? If you have a plan and resources to back it up, you are spending time and money on the ability to recover from a disaster. Improving that plan may cost *more* time and money, and you need to know what you are protecting so that those resources are not spent unnecessarily.

Upon serious reflection, most contingency planners agree that their recovery plans protect high-level corporate objectives, namely to maintain:

- Fiscal strength (revenues, investments, assets)
- Customer service and a positive corporate image
- Legal compliance (regulatory, contractual, etc.)

Your business processes support those objectives. Which processes are most critical in doing so, and how much downtime can you afford for each of those processes and still meet corporate objectives? This is what a Business Impact Analysis is about.

You can perform a formal analysis or make some "educated estimations" about process downtimes. Be careful in your estimations, as they will play an important role in where you focus your recovery planning energies. A few years ago, a large service organization began

to heavily fund recovery of their billing process, assuming that it was the most critical element in generating revenues. Upon further analysis, they realized that loss of billing for as much as a month would only DEFER revenues – which the CFO asserted was acceptable, but that lost customer service (their call center) could result in permanent loss of customers and a much greater loss of revenue in the long term. The result of this new understanding was a shift in funding recovery of the more critical process. The lesson learned was not to be deceived by what APPEARS to be obvious.

Once you truly understand where to focus your planning efforts, your next step is to determine what it would take to recover critical processes within your estimated acceptable downtimes. Given that you already have a plan, this next step may involve shoring up existing recovery resources, or you may wish to revamp your strategy entirely. If the latter, you'll want to consider the options available to you. "Alternative Site and Backup Options," beginning on page 11, provides a list of recovery options and what they mean. For you to select judiciously from the options, you might research the field of reliable vendors, determine which viable options match your preferred strategy, and perform a cost-benefit analysis. Costs vary widely among vendors, so it is wise to do your research completely – and negotiate!

The options listed in this bulletin are of a general nature – to provide basic understanding. A truly comprehensive analysis of recovery options viable for your situation should be performed by your technical personnel after your business needs are defined. Make sure that your technically oriented personnel are in synch with the business need so that they do not over-estimate or under-estimate the technical requirement. For example, if your data-loss tolerance for a particular system is two days, real-time remote replication is probably over-kill and needlessly expensive. Similarly, do not ignore new technologies, such as wireless solutions, that enhance flexibility greatly for little additional cost.

One final note about improving your plan: being recoverable in the face of a regional type outage is more than just recovering your own capabilities. You need to consider your supply chain. Will your most critical vendors be able to provide supplies when you need them? You might wish to check with your vendors to determine how resilient they are to a regional outage.

Reviewing and Exercising Your Plan

Your **Disaster Recovery** plan is a dynamic document that needs to be in constant synch with changing situations and business needs. Most plans are reviewed at least semi-annually. A review can be as simple as an internal audit or as complex as a full-scale recovery exercise.

A good way to determine where and when your plan needs to be improved is by testing it regularly. Benefits of exercising your plan run the gamut from raising awareness to validating the interplay of all recovery components. It includes notification tests, equipment component tests, network switching, data restoration tests, and table top (simulation) exercises. The latter is becoming increasingly popular in exercising **Emergency Response** and **Crisis Management** as well as **Disaster Recovery** but usually involves some external skills in design and facilitation. The payoff, however, is in considerable participant understanding and "buy-in" at all levels of the organization.

Who Owns the Plan?

In a small business, the owner of the business is often the owner of the plan. The owner has prime responsibility, but usually holds others accountable for such matters as ensuring that backups are sent off site regularly, that the plan documentation is kept current, that recovery procedures are tested, that vendor contracts are maintained, and that information about the plan is communicated to critical employees. Often, these accountabilities are given to one person. Industry analysts indicate that in most small firms, Business Continuity Management reports to the CEO, another high-level executive, or the Board of Directors.

Solutions and Costs

Solutions to recovery issues vary greatly from company to company. They depend upon potential impact and your tolerance for risk.

The chart on page 11 contains some options from which you might choose for recovery site and information backup.

The combination of solutions you choose will contribute to the cost, and while this cost varies from business to business, there are rough estimates you might consider for planning purposes. The cost of maintaining a Business Continuity Program is often $1,000 to $2,000 per employee and usually less per employee at the higher end due to economies of scale. It includes:

- Fees to an off-site storage vendor
- Employee time to sustain the program and/or consulting fees
- Contractual fees for Recovery Site for equipment and/or workers
- Quick Ship contract and/or special recovery equipment
- Document scanning or copying
- Time and materials to disseminate information and exercise the strategy

Want more?

If you search the web using keywords like "small business disaster planning," you will find a host of sources that recommend methods and templates for **Disaster Recovery** Planning. A word of caution is advisable here. Beware of "one size fits all" planning templates and forms. Here are two websites you might browse to get additional perspectives on Business Continuity Planning:

Website	Site Sponsor / Owner	Benefit
www.era-1.com	Eagle Rock Alliance, Ltd.	Browse the site to see what's generally available in Business Continuity and Corporate Resilience; also contains links to other sites that provide sample plans. For samples, go to: www.era-1.com/samplesSB.htm
www.ready.gov	Department of Homeland Security	Go to "Downloading & Ordering All Ready Publications" to find documents that might apply to your business.

Alternative Site and Backup Options

Data Center Equipment and Network Recovery

Option	Data Center Equipment and Network Recovery
1. Company Internal Reciprocal	Use of existing local company facilities to re-distribute and/or deploy additional mission-critical equipment and networks (supporting multiple business processes) amongst them.
2. Company Alternative Data Center – Internal Hotsite	Alternative, existing company data center outside the local area (region, state, country) that can be used to house additional equipment designated for testing and recovery purposes only.
3. Commercial Hotsite – Shared Subscription	Fully equipped, secured, environmentally conditioned and operationally ready data center offering a variety of specific hardware platforms ready for almost immediate use when the service provider is notified of a disaster. Facilities are pre-emptible by another subscriber having a simultaneous requirement for hotsite services.
4. Company Mirrored or Redundant Data Center	Alternative company data center that totally replicates the primary data center.
5. Commercial Hotsite – Dedicated Subscription	Fully equipped, secured, environmentally conditioned and operationally ready data center offering a variety of specific hardware platforms ready for almost immediate use when the service provider is notified of a disaster. Hotsite use is generally for the duration of the disaster, but could be limited to 6-8 weeks by some providers.
6. Company Alternative Data Center – Internal Cold Site	Alternative, existing company data center outside the local area (region, state, country) that can be built-out at post-disaster time with salvaged equipment from the disaster site, or built-out at time of disaster with acquired equipment.
7. Quick Ship by Third-party or Vendor	This strategy is essentially what its name implies, the shipment of computer and network equipment quickly. Most third-party leasing vendors provide this as a recovery solution to their customers. Customers are charged a priority equipment search fee and the normal leasing charges plus a premium once shipment is requested.
8. Commercial Cold Site Subscription	Empty, secured, environmentally conditioned data center with office space, voice and data communications lines, and electrical power, etc., ready for computer and network equipment to be moved in. Often such equipment is provided through a contract with an equipment leasing company, or via the third party or vendor quick ship option. This strategy is usually coupled with a hotsite subscription, if occupancy of the hotsite is limited to 6-8 weeks and no other options are available to the company.
9. Commercial Mobile/Porta-Site Subscription	For smaller hardware configurations or emergency office environments, there are mobile computer/office environments available. The difference between these two is that mobile sites are stand-alone units on mobile trailers, whereas the porta-site is transported to your facility and constructed upon delivery.
10. Reciprocal Agreement	Contractual agreement between two or more local (trusted – non-competing) independent companies that allows for the use of a portion or entirety of each other's data centers in the event of a disaster.
11. Commercial Real Estate Purchase, Rental or Lease	Acquisition of local space suitable to house a data center environment, and build-out at time of disaster or post disaster.
12. Do Nothing	Do nothing! Accept risk?

Work Area and Voice Recovery

OPTION	WORK AREA AND VOICE RECOVERY
1. COMMERCIAL RECOVERY SPACE SUBSCRIPTION	Fully equipped (in-stages), secured, environmentally conditioned and operationally ready recovery space suitable, configured and available for an office / workstation environment in the event of a disaster. Access to recovered business systems is also an integral part of this offering. Voice recovery must be pre-arranged with the provider and their local telecommunications carrier for types of services (PBX, wireless, ATM, DSL, 800-900, Centrex, trunk-hunt, calling features, etc.), and the number of lines and sets required. An alternative, but limited, solution to voice communications could be cellular phones held by key recovery personnel. Additionally, a central point of control (command center), known as a "Recovery Command Headquarters (RCHQ)," is required for recovery operations This space / room is where the Recovery Command Team manages and communicates the progress and status of recovery operations. This RCHQ requires all of the amenities of a work area or business recovery facility. Sometimes this solution is coupled with a hotsite subscription, as an additional measure for recovery space in the event of a catastrophic situation.
2. COMPANY RECOVERY SPACE – LOCAL	Alternative, existing, local company space suitable, available or pre-emptible as an office / workstation environment in the event of a disaster situation. This facility is known as a "Business Recovery Facility (BRF)," and can range from fully equipped and configured to pre-designated space only. Candidates for BRFs are existing conference rooms, testing & learning labs, and spare offices. Other ways to accommodate this strategy is office / workstation sharing amongst employees, and having the ability to work from home. Voice recovery must be pre-arranged with the company's local telecommunications carrier for the switching / translations of numbers and services from the disaster affected locations to the BRF. In some instances, company trained staff can perform this work, if the equipment is on-site and operable. Additionally, a central point of control (command center), known as a "Recovery Command Headquarters (RCHQ)," is required for recovery operations.
3. COMPANY RECOVERY SPACE – REMOTE	Alternative, existing remote (in the region, out of state) company space suitable, available or pre-emptible as an office / workstation / RCHQ environment in the event of a disaster situation. All other requirements as stated above apply to this solution.
4. RECIPROCAL SPACE	Contractual agreement between two or more local (trusted – non-competing) independent companies that allows for the use of a portion of each other's available office / workstation environment in the event of a disaster. This solution requires that each company have the spare space, compatible equipment, secured environment, voice and network capabilities, etc. to accommodate a pre-specified number of seats.
5. COMMERCIAL RECOVERY SPACE ACQUIRED ATOD	A strategy that is identical to pre-subscribing to commercial recovery space, except no prior arrangements have been made, time to recovery of personnel may be beyond acceptable downtimes, and the solution is not testable. This solution is only practical if unplanned space is required in the aftermath of a disaster, and no existing local or remote company space is readily available.

Data Backup and Restoration

OPTION	DATA BACKUP AND RESTORATION
1. COMMERCIAL OFF-SITE DATA BACKUP STORAGE SUBSCRIPTION	Storage of tape or disk backups to a secured, climate-controlled, fireproof media vault or room at a storage facility maintained by a commercial media storage provider. The media storage provider's facility could be local, in the regional area, or out-of-state.
2. COMPANY OFF-SITE DATA BACKUP STORAGE	Storage of tape or disk backups to a different physical company location. Depending on budget and geographical risks, off-site storage could be a company's building next door or their branch office facility across town. A better choice is a secured, climate-controlled, fireproof media vault or room at the company's owned/leased facility.
3. COMMERCIAL ELECTRONIC VAULTING, A.K.A. ADVANCED RECOVERY SERVICES SUBSCRIPTION	A technology that sends backup data directly from the company (subscriber) site to a service provider's remote hotsite facility. This very costly solution requires that direct access storage devices (DASD) or a Library Storage Module (LSM) be dedicated to the subscriber, preventing the service from being shared with other subscribers. Also required is a communications network having proper bandwidth between the sites. Data backup and recovery is nearly immediate, company controlled and unrestricted.
4. COMPANY ELECTRONIC VAULTING	A technology that sends backup data directly from a company's primary site to a company's secondary site. This costly solution requires that direct access storage devices (DASD) or a Library Storage Module (LSM) be in-place at the secondary site. Also required is a communications network having proper bandwidth between the sites. Data backup and recovery is nearly immediate, company controlled and unrestricted.
5. DISK-TO-DISK REMOTE COPY	A technology that operates at the disk volume level and is significantly less complex to set up and administer than host-based replication. This is the most popular solution used today. The solution benefits from capturing all application environment changes. A drawback however is the lack of transaction knowledge and potential for data corruption in the event of a disaster.
6. MIRRORING	A technology that maintains a replica of databases and/or file systems by applying changes at a company's or commercially provided secondary / recovery site in lock step with or synchronous to changes at a company's primary site. Due to its synchronous nature, mirroring requires significantly greater network bandwidth than shadowing. The Maximum Acceptable Downtime (MAD) for supported business processes is approximately 20 minutes to several hours, while the data-loss tolerance is reduced to the loss of uncommitted work.
7. SHADOWING (REMOTE JOURNALING)	A technology that maintains a replica of the database and/or file systems, typically by continuously capturing changes and applying them to a company's or commercially provided recovery / secondary site. Shadowing is an asynchronous process, thus requiring less network bandwidth than synchronous mirroring. The MAD is relatively short, typically 1 to 8 hours, while the data-loss tolerance is as up-to-date as the last receipt of any online transaction.
8. DO NOTHING	It is often appropriate not to back up data that can be regenerated from electronic sources that will become available following a disaster. For example, reports maintained on electronic media may be regenerated from the original data once that data is restored at a hotsite.