Creating Your Business Contingency Plan

By Randy Johnston and Dr. Bob Spencer

Before you begin reading this, do a simple exercise for us. Imagine that you are sound asleep in your bed, it is four in the morning, your phone rings and a panicked voice on the other end says, "Your office is ablaze!" Goosebumps yet? What is your next step? Oh, and retirement is not an option. How will you reconstruct your business? Will you survive the turmoil? Will your people, your clients, and customers? Now that we have your attention, you are ready to continue reading.

September 11, 2001, made many of us more aware of the potential threats we face daily. We know that such threats are a good reason to take proactive measures to protect ourselves. However, events since 9/11 have made us aware that the greatest threat to any business is still natural causes from violent storms, fire, or man-made causes such as chemical spills, or accidents. Finally, there are threats you must recover from that do not destroy your physical surroundings, but can be just as catastrophic, such as computer viruses, cyber crime, and employee theft.

Wrapped inside a business contingency plan is disaster recovery, the process of returning to operations following some type of failure. There are many levels of failures, from a small event that can be corrected in under an hour, to catastrophic failure that may take days or weeks—or from which you may never recover.

Recovery and minimizing loss will depend on how well you plan. Having developed and tested disaster recovery plans over the past 30 years for a wide range of businesses from financial institutions to manufacturers, we can attest to the fact that many disasters could have been prevented or loss minimized had there been adequate planning beforehand.

When we are engaged to help prepare a business contingency plan, our client often assumes that we begin and end in the computer room. This is not the case. Your recovery plan must include written procedures for all the functional areas of your organization as well as computer recovery. Getting your computers up and running may be the least of your problems. What about getting your people into work? In the case of a disaster that destroys your office, where will your people report? Where will the workspace be, and what equipment and office supplies will be available for them to use? What tasks must be done, should be done, and would be nice to have done? How long can you go without performing those less important tasks, like taking inventory or closing month end?

Volumes have been written on disaster recovery and the planning process. We have, in fact, spent hundreds of hours of classroom time giving lectures and written books that encompasses the subject. Since we don't have enough space here to do justice to this topic, let's summarize.

The Process to Manage Recovery

Begin by creating an Emergency Response Team (ERT) to define and manage the recovery process. In larger organizations with multiple locations, you may assign secondary teams to manage the recovery at each location. Responsible for conducting the overall recovery process, the ERT is typically composed of senior management from each critical area of your organization.

The next step is to write the plan. The Business Contingency Plan is a formal document that records the objective of the overall plan. Who is responsible? How will the recovery take place? Involvement and commitment to the process begins in the boardroom, not the back room. From the highest level of the organization, there must be a commitment to contingency planning. The ERT is actively involved in ensuring that this plan is created, tested, and reviewed annually.

In the development of your written recovery plan, you must define what a disaster is. There are several levels of disasters and not all disasters are catastrophic. Generally, here are the four levels of disasters you should plan for:

- **Level IV disasters** are catastrophic. The organization must have these systems in operation within 72 hours or experience significant economic loss. Level IV disasters can occur when the computer center is lost due to system failure or natural disaster (hurricane, etc.) When a Level IV disaster is declared, it is time to head to the alternate processing site.
- **Level III disasters** are severe, but not yet catastrophic. Ranging up to 72 hours, this type of emergency is monitored very closely beyond 48 hours to determine if, in fact, it will escalate to a Level IV condition. Level III disasters are expensive and can range from loss of critical components in the data center, loss in telecommunications, or loss of branch operations with portions of the organization functioning correctly.
- **Level II disasters** are very common and usually only affect a segment of an organization, such as a department, a branch, warehouse, etc. A Level II disaster is considered up to 24 hours (one full business day) and may be escalated to a Level III if *(continued on page 11)*

(*Creating Your Business Contingency Plan* continued from page 9)

corrective measures are not effective.

- **Level I disasters** are the most common and the most overlooked. These are the every day annoyances you experience. The duration of the failure is typically less than four hours and is isolated to one workstation, work group, or office. An example might be a Network Interface Card (NIC) or Network Switch that fails, bringing the users down until repaired.

By the way, there are many more Level I than Level IV disasters each year and Level I disasters, collectively, cost most businesses more money annually than Level IV disasters. Time to plan?

Once the plan is written and approved, the most important task remains, to test the plan. Failure to test the plan leaves you vulnerable to errors. Finally, management, through the ERT, should review the plan at least annually and adjust for any changes that have occurred in the business, then retest. Make sure your people are aware of the plan and know how to react.

There are six required responses to a disaster or to a problem that could evolve into a disaster. Each of these points must be addressed in the plan.

1. Identify a point of failure and determine a disaster condition.
2. Notify persons responsible for recovery.
3. Declare an emergency and initiate the Contingency Plan.
4. Activate the designated hot site (if the disaster level is appropriate).
5. Disseminate information.
6. Provide support services to aid recovery.

Now, let's focus on the format of your plan, expanding on the six points listed above. We begin by assuming that you have formed your Emergency Response Team and that you have evaluated your forms and your manual procedures. You should also have documented all critical systems, network components, and software needed to run your business' mission-critical processes. Finally, you have also listed all vendor and supplier contacts and the items you receive from them so that additional stock may be ordered in an emergency.

PHASES OF THE CONTINGENCY PLAN

The disaster recovery strategy explained below pertains specifically to a disaster disabling the main data center. This functional area provides computer and major network support to core applications. Especially at risk are the critical applications, those designated as Level IV systems. The plan must provide for recovering the technical capacity to support critical applications within 72 hours.

Summarizing the provisions of the plan, subsections below explain the context in which the organization's contingency plan operates. The contingency plan complements the strategies for restoring the data processing capabilities normally provided by the Data Processing Department. The disaster recovery phases are described as follows.

Emergency Declaration Phase

The emergency phase begins with the initial response to a disaster; this is the identification of a "point of failure." During this phase, the existing emergency plans and procedures direct efforts to protect life and property, the primary goal of initial response. Security over the area is established as local support services, such as the police and fire departments, are enlisted through existing mechanisms. The Emergency Response Team (ERT) on-call duty officer is alerted and begins to monitor the situation.

If the emergency situation appears to affect the main data center (or another critical facility or service), either through damage to data processing or support facilities, or if access to the facility is prohibited, the duty person will closely monitor the event, notifying ERT personnel as required to assist in damage assessment. Once access to the facility is permitted, an assessment of the damage is made to determine the estimated length of the outage. If access to the facility is precluded, then the estimate includes the time until the effect of the disaster on the facility can be evaluated.

If the estimated outage is less than 72 hours, recovery will be initiated under normal operational recovery procedures. If the outage is estimated to be longer than 72 hours, then the duty officer activates the ERT, which in turn notifies the chairman of the Contingency Plan Steering Committee and the director for information services, and the contingency plan is officially activated. The recovery process then moves into the back-up phase. Under some conditions, it is advisable to notify the ERT that a disaster has occurred even if the event is expected to last less than 72 hours. Your company should account for these types of disasters that are normally Level II (less than 24 hours) or Level III (less than 72 hours).

The Emergency Response Team remains active until recovery is complete to ensure that the organization will be ready in the event the situation changes.

Alternate Site Activation Phase

The alternate site activation phase begins with the initiation of the plan for outages enduring longer than 72 hours, or when the emergency response coor- *(continued on page 13)*

(***Creating Your Business Contingency Plan*** *continued from page 11)*

dinator deems that the emergency warrants activating the back-up processing site. In the initial stage of this phase, the goal is to resume processing critical applications. Processing may resume either at the main data center or at a designated "hot site," depending upon the results of the assessment of damage to equipment and the physical structure of the building.

In the alternate site activation phase, the initial hot site must support critical applications for whatever time frame is necessary to recreate a permanent site. During this period, processing of these systems resumes, possibly in a degraded mode, up to the capacity of the hot site. If the damaged area requires a longer period of reconstruction, then the second stage of this phase commences. During the second stage, a shell facility (a pre-engineered temporary processing facility) is assembled and placed in a designated area.

Recovery Phase

The time required for recovery of the functional area(s) and the eventual restoration of normal processing depends on the damage caused by the disaster. The time frame for recovery can vary from several days to several months. In either case, the recovery process begins immediately after the disaster and takes place in parallel with back-up operations at the designated hot site.

The primary goal is to restore normal operations as soon as possible. The definition of "normal" might be relative to what you can afford. Many businesses may be able to perform at a diminished level and still meet mission-critical objectives. Some time should be spent on this point as operating at full or "normal" levels might be much more expensive, or might result in additional costs that are not really justified.

The recovery phase incorporates all steps necessary to bring mission-critical functions back to a service level. This could mean restoring operating systems procedures, applications, and data (data bases) and validating all information as current before beginning. Part of the planning and procedural documentation for this phase includes documenting the time required from the moment that a Level III or IV disaster is declared and the coordinator activates the alternate processing site until the system is operational. To determine what is really needed in a reduced capacity, you should categorize all software and processes under the categories below and then concentrate on where your greatest weaknesses are.

Category I - Critical Functions

These are must-have functions, such as data entry and claims filing, environmental control, and such. Without these systems, you shut down.

Category II - Essential Functions

It may be hard to determine the difference between critical and essential. However, essential functions might be defined as billing, mailing, maintaining patient address and phone numbers, etc. You could do business for a short time, but the impact would be significant.

Category III - Necessary Functions

Functions such as accounting, financial reporting, accounts payable, and payroll (o.k. payroll might be critical!) are considered as necessary, but again you could get by for a short period of time.

Category IV – Desirable Functions

This would most likely be everything else from spreadsheets to word processing.

The final sections of your plan describe the people who manage the recovery process and their responsibilities. This will differ drastically by company. Don't forget a section on disaster recovery procedures that includes building evacuation and what to do in case of medical emergency, fire, hurricane, tornado, and so forth. Included in this section should be specific action items and names of those who are responsible.

BOTTOM LINE: THE COST

How much does disaster recovery planning cost? A great question; however, a better one is how much will it cost if you don't plan? We like the adage "Those who fail to plan, plan to fail!" The actual cost of disaster recovery and business contingency planning varies with the type of company or business and the depth you take your plan.

You must also consider the level of risk you are exposed to. If you live on the Florida Gulf Coast, what do you think are the chances of experiencing a hurricane in the next few years? We can tell you that they are very good! Therefore the business contingency/disaster recovery plan focuses on the threats of high winds, rising water, and loss of power for extended periods of time.

On the other hand, the chances of a Florida office experiencing a snow or ice storm are fairly slim, thankfully. Your plan will determine your risks from natural conditions as well as other threats, such as hazardous chemicals, theft, and so forth. All these affect your costs of developing and testing your plan.

Also, consider costs that would be out of pocket, such as hiring a company like ours to assist you in plan development, versus soft cost, where your staff prepares the entire plan. If your staff is not fully prepared, we know from experience that having someone knowledgeable in *(continued on page 15)*

(***Creating Your Business Contingency Plan*** *continued from page 13)*

developing and testing plans will save you time and money in the long run.

We hope that this article has provided insight into the preparation needed to develop and implement your company's plan. We face emergencies every day, and the more dependent our world is on technology, the more fragile we become and susceptible to failures beyond our control. It is a wise company that prepares. Getting started is often the toughest part of developing the plan. To help you, we have placed a sample business contingency plan at the web site, www.tsif.com (click on White Papers, then Business Contingency Plan). You are welcome to use this as a "jumping off" place to help you with your plan. ▲

Randy Johnston is a nationally recognized speaker, writer, educator, and consultant. He is the owner and executive vice president of Network Management Group, Inc., www.nmgi.com, and also the owner and executive vice president of K2 Enterprises, www.k2e.com. Randy has written books on systems design, technology overview and programming, and hundreds of articles on technology issues. His book, Technology Best Practices, *co-authored with Dr. Bob Spencer, is available from Amazon.com and Barnes and Noble. He can be reached at* randyj@nmgi.com.

Dr. Bob Spencer is a nationally recognized speaker, writer, educator and consultant. He is president of Twenty Seconds In the Future www.tsif.com, *and speaks internationally for K2 Enterprises, www.k2e.com. Dr. Spencer has written several books and hundreds of articles on technology, including several books which provide guidance on disaster recovery planning and risk management, published by the American Bar Association and the American Institute of Certified Public Accountants. He can be reached at* drbob@tsif.com.