

# Practice Makes Perfect

## Planning for Disaster Recovery

By Richard Dolewski

The events of September 11 were not an act of nature nor a computer system failure. Over the past months we have gone from being horrified to angered. We saw that this was something nobody could have ever planned for. If we look past the tragedy, this is the sort of thing a Disaster Recovery Coordinator would have to anticipate and prepare for. We plan to recover our business when we lose our data or access to our data. The goal of companies today is to accept no tolerance for downtime in their business. Information is an asset of our company which we cannot afford to lose.



Business disasters happen any time, anywhere and do not need the magnitude of a major disaster to cause serious damage to a business. In fact most disasters can be as simple as a corrupted database, or accidentally erased files in a specific application, or a complete network failure. These scenarios can negatively impact the bottom line profits of any organization. What you need is a disaster recovery plan. A disaster recovery plan is usually referred to as the DRP. It is a set of processes developed for your company outlining the actions to be taken by your IT staff to quickly resume operations in the event of a major service interruption or outage. By establishing a firm list of activities to be followed, an organization can minimize potential losses incurred by downtime. Once developed, the plan should be implemented, tested, tested and tested on a regular basis to reflect the dynamics of your computing environments.

We fool ourselves by thinking disasters never happen to us. For years I have had the opportunity to study disasters first hand and the one common similarity with all of them is that no one ever believes that it will ever happen to them. As a Disaster Recovery Planner, it pains me to see an organization take all the necessary steps to anticipate and plan for a disaster and then place the plan on the shelf or the network drive and forget about it. Was it just a means to get an auditor off your back? Developing a plan itself does not guarantee success. You must test drive to ensure success. You have to test it!

How many professional sports teams do you see taking the field without any preparation. The most talented teams do not assume "we have the skills" or "practicing would be a complete waste of time". Different parts of the team need to practice working together, to improve performance, determine what works and most importantly – plan for the unexpected.

### INTERESTING FACTS

- \* Database failures account for 6% of all application outages, totaling about \$3 billion per year in downtime costs. [1999 Standish Group research]
- \* Unscheduled system downtime significantly affects business for 98% of companies. [1999 International Data Corporation (IDC) survey]



Richard Dolewski

In the event of a systems failure, your Disaster Recovery Plan requires flawless execution and teamwork. Your Disaster Recovery team needs to practice, or in IT terms, TEST. You may have the best written plan money can buy, the best personnel, but the whole reason you put the plan in place was to prepare for the unexpected. Why would anyone assume that in the event of a disaster everything will run smoothly? The answer is you cannot. Your staff needs to know in advance what actions they need to take and how to execute them.

**Testing has several objectives:**

1. To ensure the accuracy, completeness and validity of recovery procedures.
2. To verify the capabilities of the personnel executing the recovery procedures.
3. To validate the information stored in the Disaster Recovery Plan.

4. To verify that the time estimates for recovery are realistic.
5. To ensure that all changes in the computing environment have been reflected in the Disaster Recovery Plan.
6. To familiarize IT personnel with the Disaster Recovery Plan and its procedures.

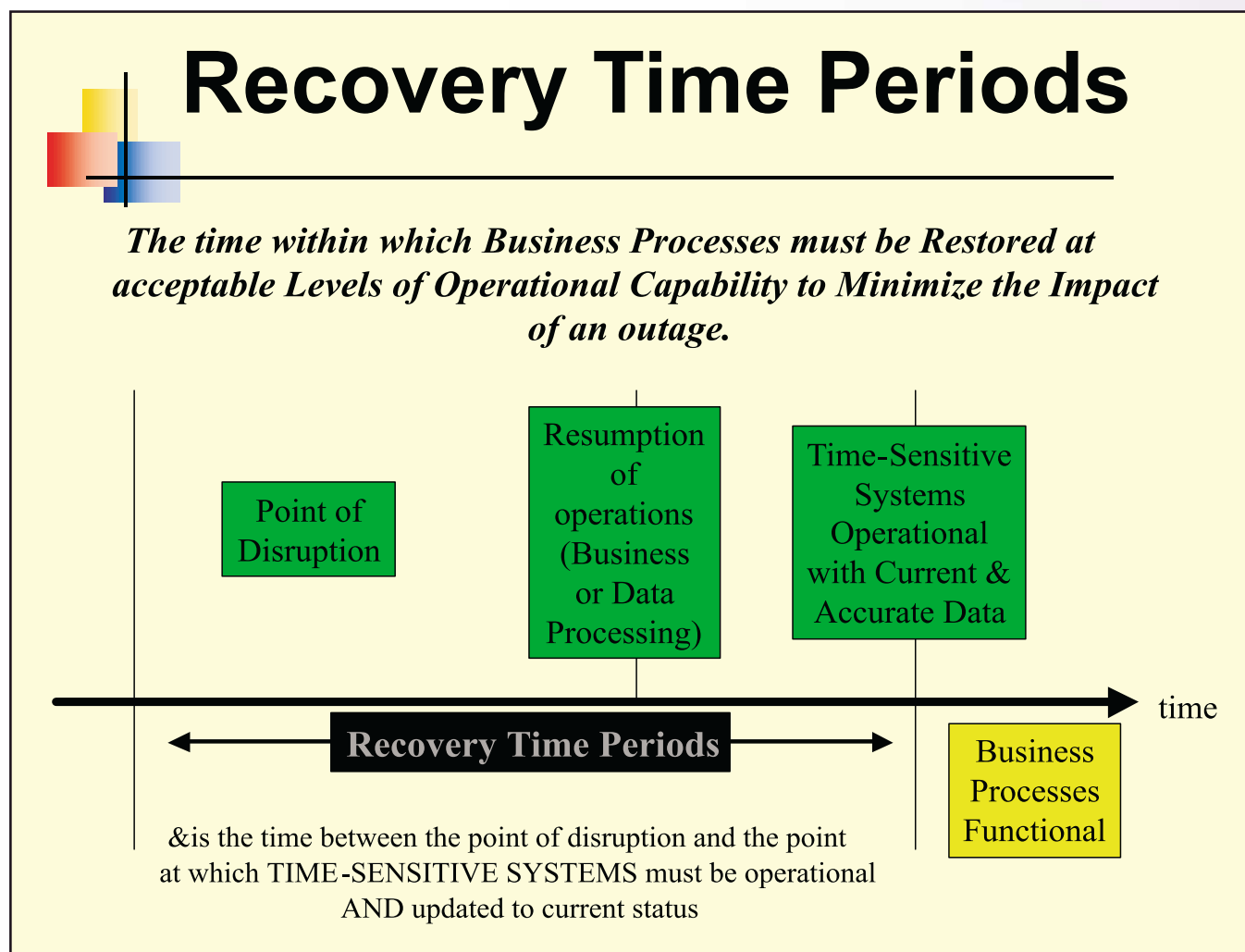
**Testing Overview**

Testing must be viewed as a continuous process. Testing of the DRP can range from simple reviews of this document to complex technical tests of your company's ability to restore the multiple computing environments quickly, either locally or at alternate facilities. However, it is not sufficient assurance of a Plan's success to conduct only a technical test once a year. You should incorporate a variety of tests designed to exercise all components of the plan. I recom-

mend two categories of testing, Active and Passive, to ensure accuracy of the plan.

*Active testing* requires that the procedures under review be executed exactly as written. For example, testing the procedure for declaring a disaster with your hot-site vendor in Toronto, and arriving with all the required backup tapes and restoring the systems. Each step would be executed fully and the data would be tested thoroughly by end user departments to validate recovery.

*Passive testing* does not exercise the procedures of the plan. A passive test is a walk through of the procedures, typically with the members of the IT Recovery Team jointly reading and reviewing the procedures literally page by page. A dry run of a procedure often clarifies the steps of the procedure.



Twice a year, the Disaster Recovery Owner (one of your many hats) will outline the testing objectives and develop the test plan for the computer systems recovery. The test plan will include a combination of active and passive tests of the DRP. The test plan shows the planned tests with their timing, duration, staff resource requirements and explanatory comments.

As a general guideline, IT should conduct tests as follows:

At least once a year, the IT Technical Recovery Teams will conduct an incident-based walk through of the Disaster Recovery Plan. This passive test will verify that the Plan is consistent with the team members' expectations and that it can work regardless of the type of disaster.

Twice a year, the Technical Recovery Teams will need to test their ability to recover at a hotsite or your duplicate data center site with an active technical test. In the second test you should test the recovery of the Network infrastructure. Yes... that other important piece of the puzzle.

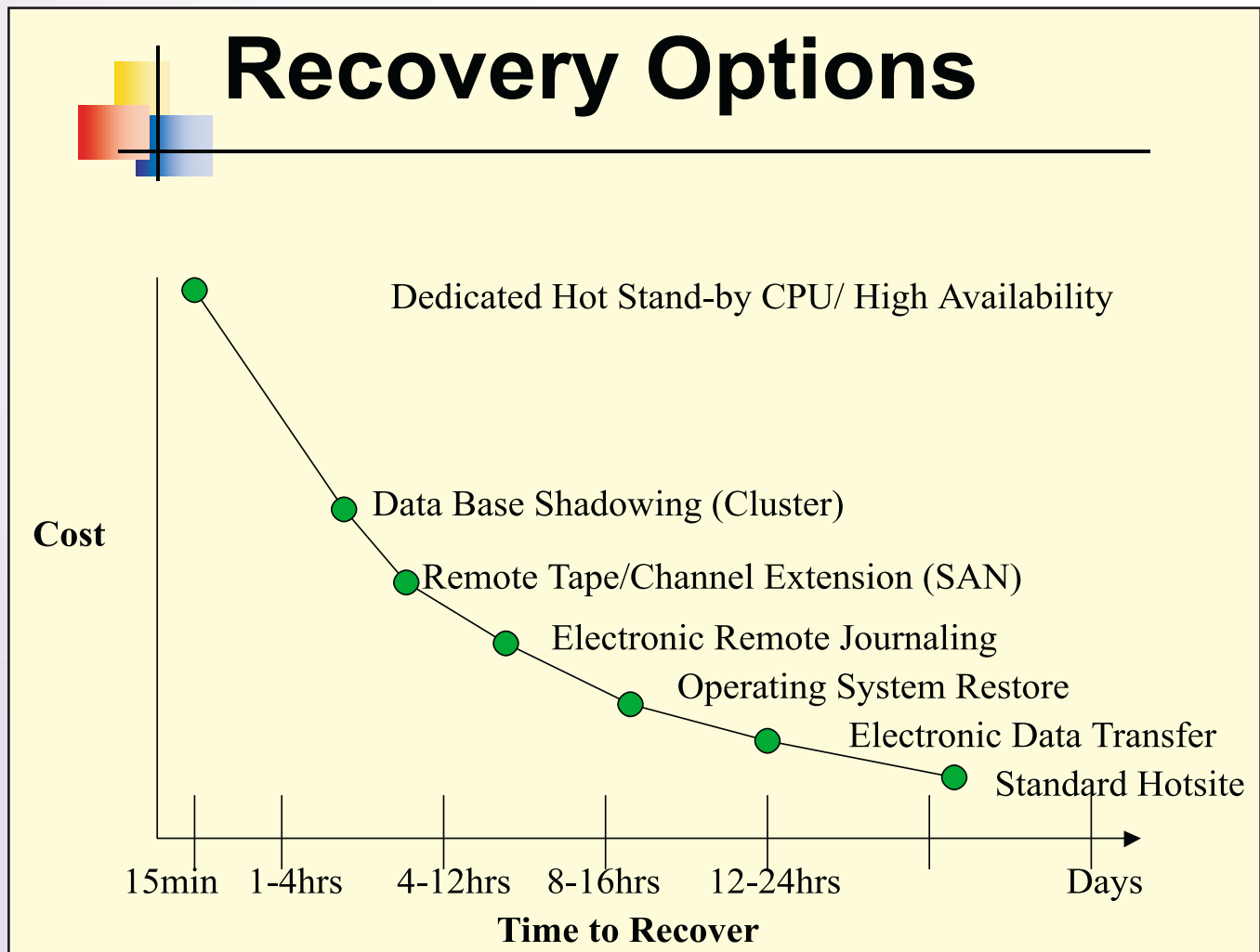
### Passive Testing

The Disaster Recovery Owner is the chairperson for a controlled walk through of the Disaster Recovery Plan's procedures. Your responsibilities for a walk through include developing the scenario that will be used during the walk through. The scenario for the walk through should be formally documented. Typically, it would be a series of handouts for the participants. The first handout would describe the disaster, its timing and impact. As the walk through progresses,

additional handouts would describe how the events of the disaster have progressed. For example, in a fire scenario, the first handout would be quite vague on the extent of the damage. The second handout would offer more information outlining the extent of the damage. The third handout could introduce a complicating factor such as the Fire Department's concerns for the safety of the physical structure of the building thus making access to the computer room impossible for an extended period of time.

Example of sample scenarios include:

- A fire denies use (either completely or temporarily) to the central computing facility. Thirty five remote offices become affected.
- The local Telephone exchange office has an extended power failure. The external network is down and will



be down for the next day. Voice service is completely disabled. All equipment in the computer room is still functional.

- A pipe bursts in one of the washrooms over the weekend. The computer room has 3 inches of water under the raised floor.

Passive testing is conducted with all participants of an IT Recovery Team and additional primary participants may be invited depending on the scenario to be tested and the components of the plan to be tested. Participants will bring their **current** copy of the DRP with them. Each participant is assigned a specific role (or set of roles) to play in the disaster scenario. Normally, the primary role for a participant would be the one he/she would play in a real disaster. From time to time, you may wish to have participants switch roles for cross training purposes. Ensure you test the obvious and do not skip items such as:

- Telephoning staff members in the DRP to validate the contact numbers.
- Telephoning vendors after normal business hours to ensure that their hotline and service numbers are correct and manned.
- Executing the notification, escalation and assembly tasks on a non-business day.

Rules for the walk through are simple:

- Using only the DRP and the formal scenario descriptions decide which tasks to execute.
- The primary resource role player verbalizes how he/she would proceed to execute the procedure using the scenario and the required information.
- Each task and procedure is then jointly approved or modified.

As the scenario progresses in the walk through, there may be changes and clarifications necessary so that the scenario walk through can achieve its objectives. Sometimes the scenario does not unfold as the Plan Manager expects. The debriefing should include a recap of the action points noted during the walk through. Every participant should leave the walk

through with a copy of the handwritten list of action points.

The summary report should contain:

- The objectives of the walk through
- List the participants
- Summarize the scenario(s)
- The scenario definition handouts
- Summarize the changes for the Computer Contingency
- Plan and schedule for their completion

### Active Testing

There are a wide variety of active tests that can be performed. Examples include:

- A full technical test of restoration of production application systems on the iSeries and other mission critical hardware.
- A technical test of LAN & WAN.
- Switching the High Availability solution and the users to the alternate facility and testing the validity of the data.

A technical test demonstrates your ability to move processing into the recovery facility within the required time. Planning for the test will proceed as follows:

1. At least sixty days in advance, schedule the test with your hot site provider. Notify participants of the plan of your selected date and time.
2. Meet with IT Recovery Team to establish test objectives thirty days prior to the test date. This will determine the participant's requirements for the test. The test schedule can also be developed.
3. One week prior to the test, publish the test plan to participants. Confirm your test date.
4. Initiate the transfer of tapes from offsite tape storage office to the Recovery Services facility.

The role of the Plan Manager during a technical test is to:

- Ensure that each objective is fully realized.
- Ensure that each test participant follows the procedures from the DRP as precisely as possible.

## Things to do When Mid-Range is Your Business Partner: #24

# COLLECT YOUR THOUGHT FOR THE DAY

Hey - you've got the time to make sure it's a really good one.

Because, at Mid-Range, we're experts at keeping your iSeries 400 - AS/400 operating at peak performance. From CRM, BI, Lotus, Web Development, iNotes, ERP & Supply Chain solutions / hardware upgrades and performance tuning through logical partitioning, operational support / education and disaster recovery we have what you need.

So you get more time to concentrate on your business.

*And your flashes of genius.*

**MID-RANGE** 

*Working For Your Peace of Mind*

Call: 1-800-668-6470 [www.midrange.ca](http://www.midrange.ca)

- Document changes necessary to make the procedures of the DRP work.
- Record problems and their resolutions as they arise.
- Record the duration of each of the procedures.
- Summarize all the change to the DRP.

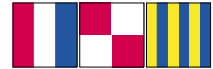
These exercises will help change Senior Management's perception and yours. Many times testing will reveal the non-technical issues of the plan. We in the IT industry are generally technically sound in our work, but it's the "procedural stuff" that will bite us. A common thing I find is Management's inability to declare a disaster properly, their unfamiliarity

with crucial procedures. Testing creates a safe "make believe" situation that is free of embarrassment. Everyone can demonstrate their abilities and understand the relative importance of these procedures without suffering damage or great costs.

Making a management commitment to regular testing, validating and refreshing your DRP can protect your company against the greatest risk of all – COMPLACENCY. Today's computing environments that face rapid business and technological changes, the smallest alteration to a critical application or system can cause an unanticipated failure that they may not be able to recover from if they do not test.

It's true that disasters, even simulated ones don't happen often. It is usually true that without testing your DRP preparedness you will not find out if it will work when that big one hits. Make NO mistake about it, disasters cause tough times for an organization. Companies have suffered and survived them, but only when they have tested. Test because your business depends on it. Backup & Recovery can be a good experience if you **plan** and more importantly if you **test**. [TIG](#)

Richard Dolewski  
[rdolewski@midrange.ca](mailto:rdolewski@midrange.ca)  
 905-940-1814  
 Mid-Range



© The 5th Wave, www.the5thwave.com

