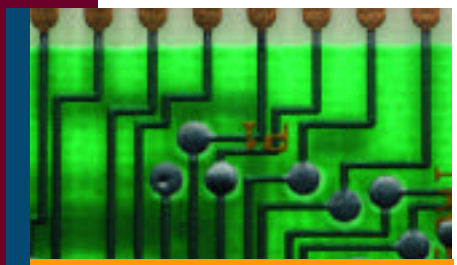

Finding the Weak Spots in Your Disaster Recovery Plan

BY LEO A. WROBEL

Often, in disaster recovery planning, notification procedures, documentation and communications are overlooked. This article examines these omissions as well as several other common weak spots in a recovery plan.

TRY this on for a nightmare: It's 3 a.m. Sunday. Your phone rings and the caller notifies you that there has been a huge gas explosion at your place of employment. The building is still in flames and appears to be a total loss. The fire department is still on the scene. Since you are the MIS manager, the caller requests you mobilize your recovery team immediately.

With this, you hang up the phone and call your number one technologist, Jim. You know it will be next to impossible to recover without Jim's help. He is the only one who knows where all the wires run. He is the only one who knows what equipment inventory you have and the vendors'contact numbers. You say a silent prayer to yourself that Jim is in town.

On the second ring Jim's wife answers. You explain. "There has been a terrible explosion and fire at the data center. The building is on fire and is a total loss! I need Jim to come to work immediately!"

With this, Jim's wife breaks into tears and wails, "Jim is at work!" Now you have two problems to deal with.

I've used this example many times in the past since it dramatically underscores several points:

1. **The Importance of Scripting Critical Callout Procedures:** In the previous example, Jim may have been out with his buddies and used work as an excuse. But can you imagine the anguish to a spouse when they receive a call like that in the middle of the night? In the worst case, a death or injury, do you feel qualified as a grief counselor? Would you want to be in that position? If not, now is the time to arrange for how that will be handled.

2. **Documentation of Recovery Plans:** Don't you think the manager in the example wishes he had made recovery planning more of a priority, at least insofar as documentation is concerned? Is your equipment inventory safely stored off site and understandable to more than an inner circle of technologists?

3. **Reliance on Key Persons:** Is there a "Jim" in your organization? I've found this to be a very common problem, particularly in network environments where the a "lone ranger" LAN administrator is present. But what about the rest of the organization? What if you lost your telecom manager? Do you feel qualified to explain to your staff what a Data Link Connection Identifier (DLCI) is so as to be able to re-establish PVCs (permanent virtual circuits) in the frame relay network to bring up the regions? To many of you, it may sound like I am giving you double-talk, but your telecom manager would understand the previous sentence in his or her sleep. But, would anyone else?

These points correspond to the three common omissions, weak spots or "holes" in today's recovery plans:

- notification procedures
- documentation
- command, control communications (CCC)

While each of these topics is an article in itself, this article will examine these omissions as well as several other common weak spots in a recovery plan.

TAKING STOCK OF YOUR DISASTER RECOVERY PLAN

How well does your recovery plan mesh with everyone else's? You may not realize it, but your corporate contingency plan is really the sum total of many subordinate plans. The sections might include things like the following:

- **Facilities** — who owns the building, interfaces with the fire department, etc.
- **Security** — who handles security (i.e., looting afterward, etc.)
- **MIS** — in this context, the computer room and mainframe
- **Distributed Processing** — the LAN recovery plan
- **Telecommunications** — both voice (for command and control) as well as data (for LAN interconnection, etc.)
- **Field Services** — broad responsibilities here; these are people who are deployed to a recovery center or rebuild the existing facility, or go out to remote users to help establish emergency configurations. Your staff could literally be split three ways.

Think that's enough? You aren't even close yet!

- *Are you a union shop?* You will need to get representatives of organized labor involved.
- *Need pens, pencils, paper and a place to sit?* Better plan on some procurement people.
- *Are you ready to look into the television cameras?* If not, better factor in a media relations person.
- *Are you ready to counsel Jim's wife?* If not, better plan on a professional grief counselor.
- *Are you ready to go to Jim's house to search for the backup tape for your LAN?* If not, better plan on some formal off-site storage today, and a media retrieval person to go after it when a disaster is declared.
- *Think you will need any money for this little project?* Better get finance involved at the team level as well.
- *Will you need to move people or equipment? Catch a plane? Rent a truck?* Looks like the corporate transportation department will have to flesh out a team for you too.

I could probably exhaust the alphabet with this line of thought, but I think you get the point. Responsible individuals or "teams" need to be defined in advance. Equally important is how one team interacts with another. For example, the data center may think it owns the building by virtue of the fact that it owns the data center. The facilities people, however, think they are the rightful owners. And then there is that security guard who will probably be inclined to declare "martial law" and keep the other two groups out. See what I mean? "Turf wars" can waste valuable time when disaster strikes.

MAKING YOUR PLAN "MESH"

How well does your departmental plan "mesh" with the corporate plan? If you and the other teams "export" too many of the details of your plan to the corporate plan, the corporate plan quickly becomes a 1,000 page monster. But what if, for example, each departmental plan (MIS, LAN, Telecom, Facilities) had a special "yellow pages" section? The yellow pages would be the first 10 pages of each department's plan. It would contain the most critical information and the basic game plan. This yellow pages section would be the only part of each plan "exported" to the corporate plan. That does two things:

1. It keeps the corporate plan a manageable size. If 10 teams export 10 pages rather than 100, your corporate plan is 100 pages long rather than 1,000.
2. It reduces the temptation for "micro-management" of the recovery process. If you are the telecom manager, the last thing you need is a phone call from a senior vice president asking, "Are the DLCIs and PVCs re-established on the frame relay network yet? After all, it is 10:20 and that's what your plan says you will be doing right now." Anyone who has been though an exercise of this type knows it goes a lot smoother without someone looking over your shoulder. Additionally, some tasks designed to take four hours take eight, and some designed to take eight take six. The important thing is that everyone is ready to join hands at a predetermined time. In other words, we go live in 18 hours. Between now and then we have the latitude to do it as we see fit.

We have used this "yellow pages" concept (we make ours blue by the way) in recovery plans for years for this very reason.

OTHER WEAK SPOTS

What other kinds of weak spots exist in recovery plans? For many, one near the top of the list is what the military refers to as "CCC" — Command, Control, Communications. Ever wonder why in the opening minutes of a war the first thing knocked out are the command centers and communications hubs? (This was not a reassuring notion to me years ago as an Air Force communications technician!) It's because you can't respond to anything when you are suddenly blinded. The same holds true with recovery plans.

We worked with one company who had a state-of-the-art data center and had spared absolutely no expense to be sure it stayed online. One day, however, they experienced a major power disruption. In this case the data center stayed up, but the communications were dead in the water.

In actuality, the picture was a bit more convoluted. The company was a huge call center as well as a mainframe user. As such, it had crossed the invisible boundary between being just a large user and being a telephone company in and of itself. Telephone companies have backup batteries. Since this company had passed the boundary almost imperceptibly, it didn't know the exposure existed until disaster actually struck. Since that time they have invested in backup batteries for their switches and are opting for a "telephone company level" of protection on other systems.

Has your company passed any of these invisible boundaries? It's more common than you think and not only in voice communications. How prevalent is the Internet in your organization? What was simply a flirtation a couple of years ago has now become a mission-critical revenue-impacting

system in many organizations. PC home banking, PC-based home shopping networks, and PC-based securities and portfolio trading are just a few examples. Is you Internet platform up to par? Just as the company mentioned previously neglected backup power, this can also be a factor for web servers. Other things to look at include redundant common logic boards, hot-swappable parts, inventory of spare parts, redundant T1 access, etc. In short, many of the same systems we have employed on other systems for years need to be considered.

Last, but certainly not least, under the CCC category are cellular and PCS phones. These contribute enormously to coordination after a disaster, especially when primary communications systems could be down. Do you have a comprehensive listing of who owns these devices? Do you publish them in the corporate directory? Do you issue spare batteries? Remember, most of these phones have only eight hours or less of "talk time" and they will be in almost constant use in a disaster situation.

In summary, watch your environment for those "invisible boundaries" as systems that were previously benign suddenly cross into new territory and become mission-critical. Evaluate your teams to make sure you have what you need before disaster strikes. Make sure your teams work out turf issues in advance. Script your recovery callout procedures. Make sure your CCC procedures are up to par. I realize this article only scratches the surface of what could be weak points in your recovery plan, but maybe you spotted a few new items worthy of further consideration in your organization. Remember, business resumption planning insurance is also job preservation insurance. Good luck, and happy planning! ts

NaSPA member Leo A. Wrobel is an active author, lecturer and technical futurist. He has published 10 books and more than 200 trade articles on a variety of technical subjects. Wrobel is president and CEO of Dallas-based Premiere Network Services Inc., a 12-year-old management consultancy and now a Texas PUC-certified local telephone company. For more information, contact their web site at www.dallas.net/~premiere or call 1-888-REWIRE-IT.