

The Worried Executive's Guide: Preventing the Telephone Company's Disasters from Becoming Yours (Part 3 of 3)



By [Leo Wrobel](#)

Date: Sep 15, 2006

[Return to the article](#)

Leo Wrobel concludes his series on preventing telephone system disasters from affecting you, designating 26 major (or seemingly minor, but nonetheless important) areas you need to check before considering your organization "ready for anything."

Think of this article as "Telecommunications Disaster Recovery Considerations, AOZ There are 26 specific items for your consideration. Some items center on how to develop a telecommunications recovery plan; some address how to test one. Many items deal with the important issue of maintaining command and control. Use this as a handy checklist of items that you may not have considered with regard to your telecommunications disaster recovery plan of like the fast-food equivalent for recovery planning

Let's dive right in

A: Where Will You Meet After a Disaster?

Issue: One major role of telecommunications in a disaster is command and control. You need to set up the eyes and ears of your organization in a place from which recovery can be coordinated. If your original building is totally inaccessible or lacks the required telecommunications, water, or sanitary facilities, it will be necessary to set up a staging area in a nearby location conducive to your type of business.

Action: Identify a prearranged staging area for recovery operations, such as in a nearby hotel. After the location has been identified, it will need to be capable of handling communications. That responsibility lies in the telecommunications recovery plan.

B: Make Your Phone Numbers Follow You

Issue: It's important to be sure that phone numbers critical to command and control do not change, since users will be confused enough after a disaster.

Action: Identify predetermined telephone numbers for recovery. For example, will the network control center or Help Desk numbers be diverted to the recovery center or staging area?

C: Recognize the Benefits and Pitfalls of Wireless Phones

Issue: Wireless phones can be invaluable for maintaining command and control after a disaster. Be aware, however, that if the disaster covers a wide area such as an earthquake, tornado, hurricane, etc., there will be intense competition for wireless frequencies. Other companies will also be in trouble, and due to limited capacity on the wireless network, there could be many blocked calls.

Action: Address the possible inadequacies of wireless phones in a disaster by providing other options, such as two-way radios (covered in the next section).

D: Consider Two-Way Radios

Issue: In addition to wireless phones, consider adding other backup systems to maintain critical command-and-control communications. Two-way radios are especially useful in situations where there may be competition for wireless frequencies, or simply as an additional way of keeping in touch. They are cheap and have up to a 12-mile range these days, so they are great for campus environments. In addition to being expensive, two-way radios require no licensing.

Action: Acquire, maintain, and practice working with a sufficient number of two-way radios for use in an emergency.

E: Carry Pagers

Issue: Pagers can also play a role in the disaster recovery process, especially when coupled with voicemail or another medium. For example, an employee could be paged at home after hours if it's difficult to reach him by other means; after finding a working phone, the employee can call in and listen to his voicemail for directions you provide.

Action: Set up appropriate employees with paging systems. Make sure that the employees maintain and understand how to use their pagers. Develop a notification plan for emergencies. Who will call whom, and how? Where will instructions or messages be left? If such systems require passwords, make sure that more than one person has the password.

F: Large Campus? Consider a Low-Power AM Broadcast Station

Issue: Another option for receiving and disseminating information and instructions is a broadcast station. The typical telecommunications department does not have one, so you might be surprised to learn that a low-power radio station (similar to the kind that supplies traffic or airport information) need not be cost prohibitive. They run around \$15,000 (including the broadcast license). A low-power station broadcasts on a standard AM radio and can be heard for 50 (100) miles. This arrangement can be particularly valuable in campus locations, or as a means of getting emergency instructions out to many employees simultaneously. In non-disaster mode, you can use the station to broadcast general items of interest, such as changes in benefit plans or the company's stock price. This approach will encourage employees to listen regularly. When the time comes to tune in for a disaster, they will know where the station is on their dial.

Action: If appropriate, investigate setting up a low-power radio station for your organization. If you go this route, remember that you will need staff who know how to run it and have that responsibility assigned in case of emergency.

G: Who Will Clean Up the Mess?

Issue: A professional cleanup company could save you a ton of money in not having to scrape damaged equipment after a disaster. These companies employ a freeze-dry process to save valuable data stored on magnetic media. They have similar processes for saturated paper or smoke-damaged equipment. These companies should be notified immediately after any disaster, since much of the magic they work on equipment, tapes, and paper must happen within the first 48 hours. After that, it's too late.

Action: Develop an arrangement with a professional cleanup company. Make sure that your plan includes details on how to notify the cleanup company, how they will get access to your facilities, which of your employee(s) is in charge of the operation, and so on.

H: Who Rewires the Building?

Issue: Which department is responsible for rewiring the building? The telecommunications department probably is only one of five or more groups or individuals in your organization that claim ownership of your wiring. Others might include the facilities department, the computer center manager, the LAN administrator, and so on.

Action: Be sure that the responsible people are predefined in advance, to avoid overlap, wasted efforts, and squabbles during the recovery.

I: Consult a Commercial Disaster-Recovery Center

Issue: Many companies use offsite disaster-recovery facilities from a variety of commercial sources such as Sungard or IBM. While these companies are especially well-adapted to this purpose, they still cannot single-handedly recover everything for an organization. This fact creates unique challenges for the telecommunications department from an internal communications perspective as well as in terms of command-and-control communications.

Action: Address all of the factors involved with moving into someone else's data center telecommunications hub temporarily. Items JON in the following sections cover some of the issues

J: Are Your People Willing to Leave Town in a Disaster?

Issue: Especially in cases of widespread disasters, many employees will go home before reporting to work, to ensure that their homes and families are okay. During Hurricane Katrina, for example, 256 New Orleans police officers bailed out on the job and went home. If the telecom department for your company did not show up for work or did not go to the recovery center, it could very well be dead in the water.

Action: Identify the people who are responsible for showing up regardless of their home situations. Make sure that they understand the importance of this function and get their assurance that you can count on their being responsible (And have backup personnel lined up, just in case).

K: What If Some People Don't Show Up?

Issue: How would your recovery plan work in the absence of your key personnel? Worse, what if there were injuries or even fatalities?

Action: For a very effective test, "bump off" a few key personnel temporarily to simulate this situation, and see how the others compensate. The best person to bump off is your key technical guru. Since this person is doing such a good job, he or she would probably enjoy an afternoon golfing game, while the rest of the team tests the plan. It will also give you a good idea of how others respond without this key individual, and a good indication of how well they work under stress.

L: Does Everyone Know How to Get to the Recovery Center?

Issue: A recovery center does not do you much good if everyone is wandering around looking for it, rather than being inside working.

Action: Arrange in advance to obtain maps from your recovery service vendor. Have detailed directions documented and placed in a vital part of the recovery plan. Then make sure your people have them.

M: Test Your Recovery Center

Issue: Most commercial recovery centers do an excellent job of staffing with onsite employees. These centers make extensive use of matrix switching for telecommunications, however, which can be complicated to figure out without a helping hand. And remember, the recovery center is not yours alone. Others will have been there since the last time you were, and they probably have changed configurations of various common components.

Action: When testing a plan, or during an actual activation in an emergency, document the condition and usability of the recovery center. After all, your organization is paying a lot of money for permission to use it. Was the necessary equipment in a usable configuration? Were diagrams available to technical personnel to assist in setup of the equipment? Were recovery center personnel available and knowledgeable? If not, you need to solve these problems before the next disaster.

N: Do You Know How to Use the Recovery Center Phones?

Issue: Many feature-rich phones are very complicated. Almost everyone has had the experience of having to ask how to use unfamiliar telephones, and the recovery center may have some very high-end equipment. Are you snickering? Transfer a call on your own office phone right now without dropping the call. Many people cannot

Action: Take a look at what type of phone system is in place at your recovery center. Is easy to use? The preference is for regular touch-tone, analog telephone sets. If these are unavailable, get some documentation information and train your personnel in advance, to avoid unnecessary delay

O: Who's in Charge of the Recovery?

Issue: Even a dominant telecommunications department is going to play "supporting cast" to higher management in a disaster. Are these higher-ups identified in your telecommunications recovery plan? Many organizations use the concept of an Executive Management Team (EMT). The EMT is the group of people who meet at temporary facilities or staging areas (residence, hotel, branch office, or some other location) to coordinate the overall recovery

Action: As part of your disaster-recovery coordination, plan for the EMT to have ready access to phones, fax, email, high-speed Internet, and other telecommunications technologies essential to command and control. While we're on this subject, remember that your staff may be split three ways after a disaster. Some people will be going to the recovery center, some will stay to coordinate the cleanup, and some will staff the EMT.

P: Keeping the EMT Apprised

Issue: An effective EMT must know what's going on among the various recovery teams to be in true control of the recovery process. Business resumption is a lot more than just telecommunications. People will be fetching tapes and equipment, coordinating with local authorities, making statements to the media, rushing through purchase orders.. and, yes, setting up emergency telecommunications

Action: In your plan, include specific details of telecommunications responsibilities for supporting the EMT. For example, include statements like this: "Within 90 minutes of disaster notification the EMT should receive a faxed written, or verbal report from each team, both onsite and at the recovery center

Q: Who Will Retrieve Data Stored Offsite?

Issue: Most companies have procedures for the offsite storage of mainframe data and have regular pickup schedules for the tapes. This isn't always the case for telecommunications equipment.

Action: Make sure that your data is part of the daily collection and offsite archival process. Keep in mind that with any type of offsite storage facility, mobility could be a problem. If you happen to be on the West Coast, for example, it will be difficult to get anywhere after an earthquake if bridges are down, traffic light don't work, and there's eight feet of glass in the street! Introduce these types of complications into your planning and your testing procedures.

R: Consider Online Vaulting

Issue: With more and more bandwidth available these days, the telecommunications department may be able to provide an *online vaulting* solution to address the archival/retrieval problem noted in item Q above. Also known as "*point in time*" recovery, a properly engineered vaulting system can record the very last stock trade or credit card transaction immediately up to a catastrophic failure. The other end of the online vaulting connection may in fact be your organization's recovery center. While expensive, tele-vaulting earns you the peace of mind of knowing that all of your data is safely vaulted at the recovery center and that you won't have to go and get it.

Action: If appropriate, investigate setting up a tele-vaulting system for your organization. If you choose to implement such a system, your emergency plan should designate the contact persons in your organization and at the service provider, and how the system will be handled in a disaster situation

S: Where Is Your Voice Mail System?

Issue: Voice mail can be indispensable for command and control in a disaster. However, if your voice mail system resides onsite, chances are that it could be toast in a building-wide disaster

Action: Develop fallback procedures that use a commercial voice mail vendor. If you can advocate outside voice mail quickly, your normal telephone numbers can be call-forwarded there, as described in [part 1 of this series](#). Remember,

by keeping these changes transparent to end users, you give yourself every advantage for command and control!

T: Look Carefully at Automated Call Distribution Units

Issue: Automated Call Distribution units (ACDs) are highly customized and heavily software-dependent pieces of equipment. Therefore, their restoration in a disaster could be slow due to long lead times for replacement equipment. What's more, they often represent the cash register for organizations, since they manage large volumes of inbound calls.

Action: If you cannot afford to do without your ACDs, make sure that you don't have to. Include your disaster planning or restoring or replacing this essential equipment as a top-level requirement.

U: Don't Expect Anything to Work the First Time After a Disaster

Issue: Anyone who's been involved in any type of a recovery center test knows that getting replacement software up and running is a very common problem. Small subtleties in operating systems, or even minute differences in components such as tape drives, can create lasting and severe headaches for people attempting to uninstall software from one system and reinstall it on another.

Action: Expect problems with the installation or restoration of your software. Get your technical team together and plot strategies for solving at least the most common installation problems that are likely to come up. Your plan should list who needs what software immediately and where the original software media are located. (Offsite in a secure location? Good!) You should also have sources for purchasing replacement software if some is destroyed. Note that forcing replacement software on users may mean unintentionally upgrading to the last version (with unwanted attendant usage problems), loss of customizations that are essential to the workflow, etc. All of these potential problems should be addressed in your plan.

V: Where Will You Get Telecommunications Test Equipment?

Issue: We've all had the experience of working on some project and suddenly not having the proper tool to finish the job. It's just as frustrating (and probably more expensive) with the recovery process.

Action: Be sure that your people have the proper tools to do what they're there to do. It will be difficult if the same fire that got your data center consumed all of your test equipment, and you haven't made provisions to find replacements.

W: For Want of a Nail

Issue: Will small items such as hand tools be available and adequate when needed at your recovery center? What will your recovery process be like if your staff cannot find a pair of pliers, screwdriver, soldering iron, crimping tool, notepad, or other seemingly insignificant items? Wal-Mart and Home Depot may not be open immediately after a hurricane.

Action: Make note of any small tools that are not available during a test, so that they be available for the next test, or for an actual disaster.

X: Seen Any Good Books Lately?

Issue: Have you considered where to get equipment manuals or other documents for equipment after a disaster?

Action: Many of your people will be out at a recovery center, installing a system that originally took years to create and are probably expected to have it operational overnight. Give them every advantage: At least make sure that they have the manuals.

Y: Could You Work at the Recovery Center for a Long Time?

Issue: With the rash of mega-disasters in 2005, hundreds of organizations activated recovery plans. Many are still working in their recovery centers today. If you utilize a recovery center, is the overall environment there reasonably conducive to your organization's work environment? In other words, could you get your done job there if recovery stretched into many months?

Action: Consider factors such as workspace, distance from home, and other possible discomforts. Another issue to consider: Could your staff work from home for many months? That might be necessary if Avian flu or some other epidemic strikes. Ensure that your plan prepares for supporting legions of telecommuters, if applicable.

Z: What Did You Learn From Your Last Test?

Issue: Even the most advanced organizations learn something new every time they test their recovery plan. In fact, if your organization consistently produces flawless results on its recovery tests, it's probably time to tighten the standards.

Action: After each test, document what you learned from the activation and the items you would change for the next test, in order to allow for a more graceful outcome.

Summary: What Did You Learn from This Series?

Telecommunications disasters encompass such a broad spectrum that I am sure I will have to write a few more articles on this topic in the future—perhaps even another three-part series. Although this series has barely scratched the surface, I hope you've gained some valuable insight that may not have been immediately apparent otherwise. These suggestions should prove to be helpful when your company activates its recovery plan, or in a test.

Just remember that, no matter how small a step or how insignificant a refinement you make to your preparations and plans, you have incrementally increased your company's resistance to a disaster. The process, you're safeguarding your job as well.

It's been fun writing for you in this series, and I wish you the best in your pursuits. Feel free to [email me](#) if you have any questions, comments on this series, or suggestions for other articles. See you again next month with a new disaster-recovery topic!
