

The Worried Executive's Guide: Preventing the Telephone Company's Disasters from Becoming Yours (Part 2 of 3)



By [Leo Wrobel](#)

Date: Jul 21, 2006

[Return to the article](#)

Leo Wrobel continues his series on preventing telephone system disasters from affecting you. Some sobering stories of real disasters at real phone companies ought to put you in the mood to take action.

War Stories from the Front

Last month I [began this series](#) with some inexpensive steps you could take right now to prevent the phone company disasters from becoming yours. This month I decided to try something a little different. We'll view the issue *from the perspective of the phone company*. In the process, I'll introduce some "war stories" from actual events that have befallen real phone companies. The names obviously have been deleted; however, the stories are true. We'll examine the disaster as presented virtually verbatim from the firsthand account of the person(s) involved. Then we'll consider what preventive steps could have been taken to stop the disaster from happening in the first place.

As you read, don't automatically assume that these suggestions are limited to phone companies. The same disasters could affect any organization, and the same precautions are probably just as applicable to any company in order to prevent such events.

Shake It Up, Baby

Let's begin with an account from an employee of a California-based telco, which experienced an earthquake.

"In the early 1990s I was working in Simi Valley for [this particular telco] and we experienced an earthquake affecting the data center there. There was minimal damage to the building, but the raised floor area equipment room sustained substantial destruction that resulted in knocking out the data center for several days. It was weeks before full function of the data center was restored. The principal reason that the outage was so protracted was that none of the equipment racks had been anchored to the concrete subfloor. As a result, the racks rocked with the quake and the contents were dumped out, and over, and spread about the floor. Surprisingly, some of the equipment survived and continued to function. In many other cases, however, equipment cables were severed, or power was disrupted. As you might imagine, lots of other physical damage was done.

The lesson in this case ought to be obvious. In earthquake zones, it's imperative to comply with building codes and other directives when installing any equipment. This isn't always an expensive proposition. The equipment required to brace and bolt down equipment racks is inexpensive, and available in any Home Depot.

On a personal note, I may have mentioned in other articles that my wife and I live in Tokyo, Japan for several years and as a result rode out a number of earthquakes. It's not like in the movies. We expected that when we experienced our first quake, it would be the up-and-down motion we all see in Hollywood pictures. This isn't necessarily the case. In the cases of the quakes we were experienced, the ground went back and forth. We also noted that the effect of even a small quake was much more noticeable when we moved to the seventh floor of tower apartment than when we lived at ground level. Many times, ground motion that would almost shake us out of bed on the seventh floor would barely be noticed by friends on the first or second floor of the same building. Distance from the earth should be a consideration if your data center is on the upper floors of a building. The building is probably designed to withstand a quake, and will most likely do fine. Everyone inside, however, might just feel like they're in an omelet pan.

Water, Water, Everywhere

Let's look at another account from the same telco this time, experiencing water damage:

"The same year in California, another of our data centers had an incident with a fire protection sprinkler system that had lapsed out of its maintenance window. The system was triggered accidentally and soaked many of the libraries of backup tapes. Not only were the tapes not properly stored, but the offsite rotation schedule for those tapes had been ignored. As a result, many backups were ruined and lost."

There are a couple of lessons to be learned here. First, pay close attention to the maintenance schedule of equipment such as sprinklers and other fire-protection systems. Doing so will keep you out of trouble with the fire and code-enforcement departments, and prevent obvious issues like the one just described. Second, note the compound nature of the disaster. The sprinkler issue was a major disruption, to be sure, but look at how the disaster was magnified and compounded by failure to rotate backup tapes offsite.

Don't Take the Word "Uninterruptible" Literally

Let's look at another firsthand account of what can happen if standards and procedures are not in place or are not strictly followed this time in Dallas, Texas:

"Our [telephone company] had an operations and monitoring center in Dallas with more than 100 seats. It supported numerous widely dispersed customers throughout the territory. This center sustained a serious power problem due to an overload on the uninterruptible power system (UPS). This condition occurred due to several factors.

1. Many noncritical pieces of equipment such as radios, heaters, and other nonessential machines were plugged into the special orange power outlets that were designated for UPS mission-critical equipment, including the PBX and ACD (Automatic Call Distribution unit). Many of the "butt-in-seat" folks comprised the call center staff had heard a rumor that "orange power" was somehow superior, so moved their desks to these outlets under their desks.
2. As the load on the UPS continued to climb to near its capacity, the heat in the room where the UPS resided also climbed. There was no temperature alarm in the UPS room.
3. In addition, since so many people used the room, there was inadequate space and airflow.
4. Another contributing factor was management of storage and boxes. It seems that where airflow might have been available was further blocked by someone using the UPS system room as storage for boxes, paper, and anything else that was in need of being tossed aside.

A rectifier board in the UPS finally failed due to thermal overload. The resulting disruption put the call center out of business for several days. There was no alternative power source for the PBX and the ACD, although some of the network tools came online after some juggling of power plugs by the technical staff. No single technologist, however, was assigned responsibility specifically to the UPS; therefore, no alternative power source was ever considered for the PBX/ACD. It stands to reason that this is also why nobody ever noticed the numerous other items that were running on the UPS erroneously. I became the HVAC/power/UPS person after that ordeal.

It was fortunate in this case that there was not a fire, particularly with the number of combustibles in the UPS room. In addition to blocking airflow, these materials easily could have ignited.

[We had] more than a few customers who were not on the happy side even before this incident. After the repairs were made and the center recovered, several of them left us for other alternatives with other companies, and the company lost business due to the disaster.

The lessons in the account above should be obvious:

- Follow manufacturers' specifications (including airflow instructions) for the environment that your equipment requires.
- Don't assume that because UPS systems hardly ever have trouble that they are invulnerable. They are not. I had firsthand contact with many customers who sustained UPS problems; believe me, that's the last place where you want to have issues.

- In this instance, nobody was responsible for the UPS. That's asking for trouble, cause general oversight and maintenance schedules go out the window. Every major piece of equipment should have a person designated as responsible for that equipment, even if that person is a vendor who comes in occasionally to inspect the equipment and perform preventive maintenance

Technician Does Not Necessarily Equal Data Center Man

Here's one more example, just to show that it's not always hardware that causes problems. Telephone equipment today is nothing more than big computers, and as such it demands the same protocol and procedures (such as change control) that have been in place in data centers for years. Sometimes, however, the telco forgets this rule:

"A group of technologists attempted to install a set of software operating system patches on an operational server in Sacramento. The trouble is that these individuals attempted to do so without first doing any regression testing. In the process, they corrupted the primary applications on the server, which resulted in a weeklong event to rebuild them. Other change-management procedures were also [ignored]. This led to many related difficulties, including network routing issues that left whole segments of the country unable to access these applications, even when they were resurrected later.

It's amazing how much telephone equipment today is dependent on servers. Just as servers lagged behind mainframes in operating and security standards in our data centers, telcos may lag behind other businesses in providing and following such standards. Servers don't require a specialized environment to operate, like most mainframes do. The server can sit right out on the floor, or in a closet, or in some other area that causes physical risk. Very often, issues related to change control also arise, as in this example. Because telephone technicians usually aren't data center managers, there's a learning curve. Consider what a technician's laptop can do to a DSLAM, for example. The *digital subscriber line access multiplexer* (DSLAM) is the equipment that the telco uses to provide your DSL lines. One wrong move could affect the voice and Internet services of hundreds of users; yet, in many cases, the same people responsible for providing dial tone are those primarily responsible for the DSLAM. Have these people had the proper training? It probably pays to check.

Reduce Vulnerability To Increase Survivability

Remember that even the smallest and least expensive steps you take can add immeasurably to the survivability of your company after a disaster, and to the well-being of your organization as a whole. I wish you the best in this regard.

I hope you've found this article useful. We'll conclude this series next month with a final article about avoiding vulnerability in the telco environment that I'm sure you'll find interesting.

My sincere thanks to everyone in the telco business who contributed to this article, particularly my longtime friend and industry expert John A. Lyons.
