

Are Private-Sector Organizations Responsible for Failing to Plan for Natural Disasters? (Part 2 of 3)



By [Leo Wrobel](#), [Sharon Wrobel](#)

Date: Mar 23, 2009

[Return to the article](#)

In part 1 of this series, Leo A. Wrobel and Sharon M. Wrobel pointed out that, as business needs change and technologies arise to fill those needs, contingency planners must adopt those new technologies - or be held responsible for failure to do so. In part 2, they consider how these issues affect your role in emergency planning for your organization

[Part 1 of this series](#) asked whether the commercial contingency planner must take a proactive role in planning for the possibility of a natural disaster. We proffered the observation that when a technology for backup and recovery of a given business system becomes accepted, ubiquitous, and affordable, it's the responsibility of the serious contingency planner to adopt it

Let's return now to the central question: Are private sector planners responsible for planning against natural disasters? When set in this context, we believe that the answer is an unequivocal yes. For example, commercial organizations determine where to locate their facilities. If the chosen location is on a seismic fault, oceanfront floodplain, or other risky area, recovery plans must address this fact:

The Contingency Planner's Job: Get Ready for Anything

Today, the technology for predicting the frequency and intensity of virtually any kind of threat to critical infrastructure is both available and affordable. You just have to know where to look for it and how to interpret it. Critical infrastructure (loosely defined as electrical power, water supplies, fuel distribution, and so on) affects any commercial enterprise. Therefore, the responsibility for having a recovery plan for loss of any of these components rests, at least in part, with the contingency planner

Consider the possible effects of natural disasters on communications:

- During Hurricane Katrina, some 34 central telephone offices in southern Louisiana were under water
- If your U.S.-based or UK-based organization has call centers in India, you are not only highly dependent on undersea telephone cables. These cables are vulnerable to seismic events, acts of war, or deliberate sabotage.

Many companies already consider how to react to seismic events. For example, we know of a significant number of banks and financial services companies in the San Francisco and Los Angeles areas that sit on geologically active real estate. These companies have invested heavily in technologies such as point-in-time recovery systems that back up all data in real-time to other remote locations. Such systems will soon become more the norm than the exception and will become more affordable as the cost of telecom and storage technologies continues to fall. However, some resources allow for predictive analysis of these events in order to make your company even better prepared. We'll discuss those resources later in this article and in part 3 of this series

In a historical context, large-scale point-in-time data recovery (a.k.a. online vaulting or televaulting) was totally cost-prohibitive from both a telecom capacity and storage technology standpoint for many years after the need for such technologies was identified. Today, they have become so ubiquitous and affordable that an organization in California that doesn't use such technologies might be considered negligent for its failure to do so. The same can be said for technologies that predict natural disasters, which today are becoming mature and affordable.

Understanding the Issues and Bridging the Vulnerability Gap

Even elite and leading-edge commercial organizations may not have taken the next logical step: performing a formal vulnerability analysis of threats by natural disasters to critical infrastructure. We submit that the technology and resources are mature enough now for performing essential vulnerability analysis on the effects of natural disasters on an enterprise. Much of this technology is affordable, and the new emphasis on natural disasters and terrorism mandates its consideration. The time is now for the serious contingency planner to evaluate what can be done to reduce the organization's exposure to natural disasters.

As history shows, every time a new technology or business process is introduced, the paradigm shift inevitably creates a "vulnerability gap." This vulnerability gap is the period of time from the introduction of the new technology until an affordable solution is devised to back it up. Remember Table 1 in [part 1 of this series](#)? Let's put the concepts described in that table in terms that most commercial organizations should remember and understand:

- **1980.** Most commercial organizations are using large mainframe computers and are just beginning to realize that they've outgrown the ability to fall back to paper in the event that the mainframe fails. Organizations realize that a fire in the computer room would be very bad, and they adopt standards for fire-suppression systems and management of combustibles in a computer room. Companies realize that a catastrophic failure of recording media would be disastrous; therefore, standards are adopted and written for backup of data, etc.

Resulting technologies: Mainframe computer recovery centers, offsite data storage companies

- **1986.** Most commercial organizations have begun to connect the mainframe to branch offices. Service bureaus such as Electronic Data Systems spring up. Suddenly, dependence on the public telephone network has become acute. In fact, the reaction of the corporate contingency planner of the early 1980s to recovery planning for the phone company was very much like the reaction often received today to the notion of planning for natural disasters. Many planners considered such an effort to be beyond their scope of responsibility. After all, they paid big phone bills, so why shouldn't the telecom carrier handle its own recovery plan? But the phone company might be more concerned with restoring payphones (access by the public to 911 service) than in restoring the T3 line or frame relay network that supported your entire online network of multiple branches. Therefore, much of the 1980s and well into the 1990s was spent writing operating and security standards for telecommunications. Case in point, Leo's 1990 book, *Disaster Recovery Planning for Telecommunications*.

Resulting technologies: Telecom companies introduced technologies such as command routing, remote call forwarding, diverse cable routing, synchronous optical networking (SONET), on-demand T1 services, and so on.

- **1995.** Mission-critical applications moved out of the relative safety of the mainframe and computer center to distributed local area networks. The industry responded with operating and security standards for LANs. Leo played a role in the transition by publishing *Writing Disaster Recovery Plans for Telecommunications Networks and LANs*.

Resulting technologies: Computer recovery companies, rooted in mainframes, added client/server systems and technology with more space for people

- **September 11, 2001.** No need to elaborate on this date

Resulting technologies: Creation of the U.S. Department of Homeland Security and other federal emergency-management agencies.

- **2001 to date.** Hurricanes Katrina, Rita, Gustav, and Ike. Indian Ocean tsunami, other megastorms

Resulting technologies: Proactive planning efforts geared at natural disasters, including data validation, storm modeling, and advanced predictive analysis

What Does This Mean Today?

We believe that the specter of terrorism since 9/11, combined with the increasing frequency of natural disasters, must fundamentally change the mindset of the corporate contingency planner. Planning for natural disasters is now arguably in the province of the private-sector planner, much as telecommunications entered the planner's scope of responsibility in the 1980s and 1990s. Just as demand from the private sector, particularly the financial services community, drove innovative new telecommunications solutions and dramatically reded telecom networks, those

same forces will drive and refine responses to natural disasters. New operating and security standards and best practices will be developed, but this time for mitigation against natural disaster and terrorism.

Although disaster recovery planning as a science and a profession continues to evolve, we can draw parallels with the past. We are literally starting from scratch in many respects with regard to natural disasters. For example, we have sought out a few brain trusts for inclusion in this series that may be unfamiliar to the typical corporate contingency planner. One noteworthy contributor mentioned in past articles is the [Pacific Disaster Center](#) (PDC). Formed after Hurricane Iniki devastated the Hawaiian Island of Kauai in 1992, the PDC has evolved into "information central" with regard to information on disasters, which span the spectrum from earthquakes and seismic events to hurricanes, typhoons, and tsunamis.

If information about disasters were the only requirement, the job would be easy. We could all just sit on the web and mine it for free. But there would be no way to validate which information was truly accurate and useful. Even if we could prove validity, the question of how to use the information would still present difficulty. Those of us who have immersed ourselves in web-based research know that when it comes to information, it's not how much you have but how you use it. When projecting how natural disasters might affect your organization, it's important to focus on the kinds of things you can control with preplanning, and on preparations you can reasonably afford.

We hope you are now convinced that commercial organizations must consider the issue of natural disasters and terrorism in crafting recovery plans. In the conclusion of this series, we'll look at some sobering evidence of the urgency of this need.
