

Are Private-Sector Organizations Responsible for Failing to Plan for Natural Disasters? (Part 1 of 3)



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

Date: Mar 16, 2009

[Return to the article](#)

In this three-part series, Leo A. Wrobel and Sharon M. Wrobel address an interesting question: If you're the company's disaster-recovery planner, and you're caught unprepared for a natural disaster (hurricane, earthquake, wildfire, etc.), are you at fault?

It's no secret that commercial and/or private-sector organizations can be held accountable for all kinds of negligence. This is the fundamental reason that organizations have disaster recovery plans. Most of the readers of this series know this to be true and are probably actively involved in the recovery-planning efforts for a critical computer center, call center, or other business function within their own organizations. Indeed, the hazards to any organization are a myriad, including fire, flood, sabotage, computer viruses, disgruntled employees, and so on. We have covered quite a lot of them over the years in this venue. We now pose a totally new question: Is time for the serious contingency planner to add active and proactive planning efforts geared toward dealing with natural disasters? We believe it is, and we present our rationale in this three-part series.

A Not-So-Rhetorical Question

Can contingency planners in commercial and private-sector organizations be held accountable for failing to plan for natural disasters? As a speaker at a recent Homeland Security Summit, I posed this question to an audience. While it's not by any means a scientific methodology, noting the instant responses and reactions of such a group (comprising security and disaster-recovery professionals) to such a question can be considered a barometer of things to come.

To spur some discussion, I offered several choices to the audience as suggested responses:

1. No. That's why I pay taxes as a business owner. It's someone else's responsibility.
2. No. What can I do as a businessperson to prevent a tsunami or steer away a typhoon?
3. Yes. Sources exist for predicting the possibility of damage caused by natural disasters: hurricane risk, geophysical data, elevational information, infrastructure vulnerability. These sources should be considered by commercial planners when deciding such matters as where to locate production facilities, and when crafting recovery plans.

Much to my surprise, the audience in this non-scientific straw poll vacillated between blank stares (no opinion, or never really considered this question previously) and the strong opinion that planners are responsible, at least in part, for planning against natural disasters. No one expressed a strong opinion that planners are not responsible.

This unexpected response resulted in some additional discussion about the history of contingency planning in general. Stated briefly, the focus of the contingency planner changes over time. Technology and business processes change. Whether someone adds a mainframe, begins to use a call center, adopts just-in-time delivery, or introduces something entirely new to the business process, such changes alter the planning paradigm and introduce new complexity to the recovery plan.

Technology Changes Your Job, and Vice Versa

Later in this series, we'll discuss some of these topics in more detail, but first we'll briefly summarize the basic principle at work: Any change in business processes and/or technology leads to a common series of events. For example:

1. Changes in technology almost invariably outpace the ability to back up that technology.
2. Recovery resources and technology eventually catch up; as a result, new standards and practices are adopted for dealing with the new technology
3. Commercial enterprises generally adopt these standards and practices as they become widely available and affordable.
4. The new standards and practices then become the responsibility of the corporate or private-sector contingency planner

Let's consider how this system works in practice

Consider "first alert" systems circa 1979 in use by the United States military. These systems utilized multimillion-dollar AUTOVON switches, satellite communications, and various types of radio backup systems such as tropospheric scatter systems.

Since the purpose of these systems was to detect missile attacks and other threats against the United States, they were mission-critical to the lives and livelihoods of hundreds of millions of Americans and their allies. Therefore, they were funded by the government, but certainly not required by commercial organizations; the cost was simply out of reach. The switches were superb for maintaining what the military calls "4C" (command, control, communications, computers, and intelligence). They could get word to policymakers in seconds in any situation, whether it was a possible missile launch or a call from the President. The switches also contained features whereby high-priority calls could preempt low-priority calls to ensure that the most important instructions always got through. But they were extraordinarily expensive to deploy, well into the tens of millions of dollars.

Now fast-forward to the present. Today, the capabilities of what used to be a \$50 million AUTOVON switch fit in a \$1,000 server. Moreover, things like satellite communications are available commercially, affordably, and practically anywhere. Even the public switched telephone network (PSTN) is extraordinarily diverse, compared with the network of 30 years ago. Services that were prohibitively expensive in days past are available everywhere today, in the form of wireless networks, Voice over IP (VoIP) services, and other technologies. Even the multi-level preemption feature enjoyed by the military 30 years ago is available (after a fashion) under IP Version 6 or alternatively under programs like the Government Emergency Telecommunications Service (GETS) for landlines and Wireless Priority Service (WPS) for mobile phones. These government priority services allow for priority in a disaster, and while such government-sponsored priority schemes must be arranged in advance, they're certainly affordable.

When a technology becomes more affordable, there's less reason not to adopt and use it. For the planner who opts not to use such technology even after the reduction in cost, the exposure for possible negligence increases. Stated another way, a planner could not be found negligent for failure to acquire and use a switch costing \$50 million. But saying no to a \$1,000 server that could have averted disaster? That's a different story.

Overview of Past Paradigm Shifts in Disaster Recovery

As a preface for the next two articles in this series, consider the history discussed in Table 1, in which business processes advanced, new technologies were introduced, and recovery standards for backing up that technology changed. After you have an understanding of this evolution, we'll postulate our arguments in the second article of this series. Part 2 will expound on why we believe that the paradigm has shifted, and what today's serious recovery planners should be taking an active role in planning for natural disasters. Assuming that we get you to buy into our arguments, part 3 provides some affordable tips and resources for improving your planning to include addressing natural disasters

Table 1 High-Level Evolution of Private-Sector Disaster Recovery in the U.S.: Motivations, Causes, and Effects

Date(s)	Event(s)
---------	----------

1948O1968	Military development of the concept of command, control, and communications (C3,
1968O1978	Continued refinement of C3, but the Cold War standoff demands that decisions be made more quickly than humans can achieve. This calls for the addition of computers to the concept of C3, resulting in the concept of 4C.
1978O1981	First commercial computer (mainframe) recovery centers, as the private sector begin to demand backup, restoration, and recovery technologies
1981O1986	First best practices (a.k.a. operating and security standards) for mainframe computers used in the private sector.
1981O1991	First intensive and widespread use of commercial telecommunications to link mission-critical mainframe applications. Initially, these were private-line circuits; later came packet technologies such as frame relay and switched multi-megabit data services (SMDS
1990	Publication of Disaster Recovery Planning for Telecommunications by Leo A. Wrobel (Artech), which was one of the first books to document disaster-recovery standards for telecoms, applicable to the non-military private sector
1993O1998	Intensive and widespread use of client/server topology to link mission-critical applications. Auditors go mad as mission-critical applications leave the relative security of the mainframe computer and spread directly to end-user desktops and servers
1993	Publication of Writing Disaster Recovery Plans for Telecommunications Networks and LANs by Leo A. Wrobel (Artech), which documents disaster-recovery standards for local area networks (LANs).
1996O2001	U.S. Telecom Reform Act of 1996 gives users the opportunity to buy piece parts of telecom services such as <u>dark fiber</u> . Price of telecom services drops dramatically. "Native LAN" speed circuits (100/100 Mbs) replace T1/T3 in U.S., E1/E3 in Europe. Technology such as <u>optical televaulting</u> becomes cost-effective, first utilized in the financial services sector. Publication of Understanding Emerging Network Services, Pricing, and Regulation by Leo A. Wrobel and Eddie M. Pope (Artech), which discusses these concepts
September 11, 2001	World Trade Center attacks. Largest mass activation of computer recovery centers in history. Not everyone makes it into a recovery center; some businesses never recover. New legislation results in the establishment of numerous new agencies, such as the <u>U.S. Department of Homeland Security</u> and the <u>Transportation Security Administration</u> .

2001 to date	Continued focus on terrorism but also natural disasters. Rising awareness of global warming issues. Hurricanes Rita, Katrina, Gustav, Ike. Indian Ocean tsunami causes unprecedented destruction. Earthquakes in Chile, China, and elsewhere. Private sector realizes the need for a military level of 4Ci to activate complex recovery plans when the unthinkable happens. Prices for enabling technology (from VoIP to server hardware to telecommunications services) drop. Wireless access capability proliferates. Local number portability comes into being with the potential capability to relocate entire area codes. Satellite communications become portable and affordable. Commercial companies specializing in 4Ci come into being for both command and control communications as well as backing up complex call centers and other operations.
2009	Disaster Recovery Planning for Communications and Critical Infrastructure to be published by Artech House Books, the first operating and security standards and best practices for 4Ci. This book first suggests that the private sector bears some responsibility for natural disaster prevention.
