

When Disaster Strikes

By Rebecca A. Morgan
Inc.com • 2004

Disasters, whether natural or man-made, can be expected, yet many businesses are unprepared.

While the towers still smoldered, organizations began to scramble. The personal toll was overwhelming. Efforts to limit the economic impact had to begin immediately.

A T1 line, critical to The Bureau of Labor Statistics (BLS), ran under the WTC. BLS computers were not maintained in the WTC but vital systems housed nearby could not be reached. The BLS collects data and calculates and reports major economic indices that are used in many ways by various parts of the economy. The process follows a very specific and tight schedule. Excessive delays could impact financial markets negatively, beyond what the attacks themselves had done.

It took a few days for the BLS to gain access to those hard drives and the information they contained. A lesson was learned. The BLS now has, through its continuity of operations plan, a replicate system that would maintain data access despite a major interruption affecting any of its key facilities.

The towers fell in New York. Hurricanes swept through Florida, one after the other. Fires roared across the West. Tornadoes hit the Midwest. Disasters, whether natural or man-made, can be expected, yet many businesses are unprepared. Whether it is a West Coast dock lockout, a labor strike, an anthrax scare, a fire at a building down the street, or a flood that swamps your business, you can expect a major interruption to occur at some time. You don't know which type, where, or when, but you can prepare nonetheless. Without a response plan in place, the impact of an interruption can be even more devastating.

Disaster preparedness efforts in most companies have been led by IT historically but are equally important in other arenas of the business. Where will your employees report to work if your building is gone or access denied? How will you contact them? How will you communicate with customers and suppliers? What are your most critical supplier back-up plans, should a key one shut down unexpectedly? How can you support and retain a significant customer whose building caught fire? While you may receive empathy for a disaster, you can also lose your entire business. To minimize the impact, the time to prepare is now.

Let's start by taking a look at what the folks in IT do to prepare for disaster recovery. There are lessons to be learned there.

"Start by knowing what you have," says Ned Sherry, Director of Information Technology for Kinetico Inc. "Document your network with enough detail that you can use it as a shopping list if you have to start from scratch, and as a blueprint for rebuilding your architecture." Next, review and test both your backup and your restore procedures. Verify that you are backing up what you need, that you follow the tape rotation system, and that access to the backups is available 24/7/365 despite a crisis. A plan that looks good on paper may contain big holes. Test, and then test again -- at least annually. Make sure the backup can really be used to restore files. Make sure your system diagrams are kept accurate.

Software is equally important. Product key-codes are required for reinstalling software. "Keep the software and the key-codes in a safe place, again accessible despite the emergency," reminds Sherry. Service patches downloaded over the Internet must be tracked, for both operating systems and business software. Failure to reinstall them may cause other problems.

Identify the threats to your company's information. Viruses and hackers are well-documented menaces, but there are many others. Determine the risks, prioritize them on both likelihood and impact, and then define your plans to recover from them quickly and successfully. Mission critical systems are high priority, but within that you may still have precedence decisions to make. Business leaders should work with IT leaders to define those priorities.

Continued on back



Contact Rebecca A. Morgan at:
Fulcrum ConsultingWorks, Inc.
voice: 216-486-9570
fax: 216-486-9922
cell: 216-210-9109
morgan@fulcrumcwi.com
www.fulcrumcwi.com
© 2007 Fulcrum ConsultingWorks, Inc.

When your plans are in place, make sure they are documented. And make sure a copy of that documentation is in a safe but accessible offsite location. Documentation does little good if it was burned in the fire or you can't get to your building where it is stored.

Some of the basic lessons the rest of the business can learn from IT include:

- List and prioritize disaster threats; plan accordingly

- Document key "rebuild" information --
 - * Employee, supplier, and customer contact data
 - * Replacement physical location(s) and equipment
 - * Outstanding commitments, both supplier and customer
 - * Supplier alternatives
 - * Key customer support plans
- Test

Fairly simple lessons, but invaluable when disaster strikes.



Contact Rebecca A. Morgan at:
Fulcrum ConsultingWorks, Inc.
voice: 216-486-9570
fax: 216-486-9922
cell: 216-210-9109
morgan@fulcrumcwi.com
www.fulcrumcwi.com
© 2007 Fulcrum ConsultingWorks, Inc.