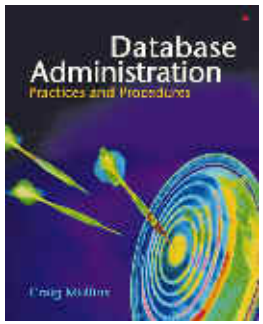
April 2005

DATABASE TRENDS AND APPLICATIONS

# The DBA Corner

*by Craig S. Mullins*




## Plan for Disasters and Test Regularly

A disaster recovery plan is like insurance – you're glad you have it, but you hope you don't need it. With automobile insurance, you pay a regular fee so that you are covered if you have an accident. A disaster recovery plan is similar because you pay to implement your disaster recovery plan by designating a disaster recovery site, shipping backup copies of the data off-site, preparing recovery jobs, and practicing the recovery procedures.

Disaster recovery planning, sometimes referred to as contingency planning, is the process of preparing your organization's assets and operations in case of a disaster. But what is a disaster? Sungard Recovery Services provides a good definition: any unplanned, extended loss of critical business applications due to lack of computer processing capabilities for more than a 48-hour period. Of

course, your definition may be more or less stringent with regard to the timeframe but that basic definition is a sound one.

Most of us have witnessed a disaster situation, at least on television. Floods, earthquakes, hurricanes, and fires are some examples of natural disasters. The recent (December 2004) tsunami in southeast Asia is a prime example of a disaster. Disasters can also be man-made, such as electric failure, bursting pipes, and war. Although most of us have never actually lived through a disaster like the ones you see on the news, many of us have had our basements flooded or been in an automobile accident. A disaster does not have to have global consequences in order for it to be considered a disaster to you.

You must recognize potential disaster situations and understand the consequences of each. How these disasters might impact your business is the purpose of disaster recovery planning. If your business is on a coast the likelihood of tornadoes, floods, and hurricanes increases. If your business is located in the North snow storms and severe cold weather will pose more of a risk. Californian businesses should be more apt to worry about earthquakes than businesses that are not located near a fault line.

Some disasters are not location-specific. Sabotage, computer viruses, vandalism, air conditioning or heating failures, and health hazards can happen anywhere on the planet. So every company should have a comprehensive and tested disaster plan that details how to resume business operations in the event of a disaster.

Even though disasters are unpredictable and unlikely, every organization should have a plan to cope with a disaster situation. Companies with a disaster plan will be able to service their customers again after a disaster much quicker than those companies without a disaster plan. Indeed, a company facing a disaster without a disaster recovery plan may never resume business.

Database disaster recovery must be an integral component of your overall business recovery plan. A disaster recovery plan must handle business issues such as alternate locations for conducting business, communication methods to inform employees of new locations and procedures, and publicity measures to inform customers how to transact business with the company post-disaster. A component of that plan must be the overall plan for resuming data processing and IT operations – and databases are a part of that. You will need to create a recovery plan for every DBMS platform for which you have databases implemented.

Once the disaster recovery plan is written be sure to schedule regular tests. It is a good practice to test your disaster recovery plan at the remote recovery site at least once a year. You should also consider testing the plan if your IT environment undergoes any significant change (such as an upgrade to a new DBMS version). Use a disaster recovery test to discover weaknesses and errors in the plan. After the test be sure to update the disaster recovery plan to address the problems. A valid disaster recovery test need not end in a successful recover – although that is the desired result. A disaster recovery test that unveils heretofore unknown weaknesses in the plan serves a useful purpose.

Another consideration for scheduling regular disaster recovery tests is to assure the readiness of your personnel. The best way to prepare for a disaster is to practice disaster recovery. The process of actually implementing the plan forces you to confront the many messy details that need to be addressed during the recovery process. Testing also helps you to become familiar with the tools and procedures you will use during an actual disaster recovery.

Actually, a scheduled disaster recovery plan is probably a poor idea. Instead of scheduling it so everybody can be ready, the disaster recovery test should work more like a pop quiz. One day your boss should came to work and announce that

the building was just destroyed. Such a scenario makes the test a lot more like an actual disaster. Who should be called? Is everyone available (vacation, illness, etc.)? How can you get the right people to the remote site for recovery? Can you get your hands on the disaster recovery plan?

The goals of recovery practice are to discover problems with the recovery plan, to provide on-the-job-training for key personnel to become familiar with the procedures and tools to be used for disaster recovery, and to raise awareness of the organization's actual level of readiness to confront an actual disaster.

Of course, you might decide that it is impractical to conduct disaster recovery testing without advanced warning. This is especially true if out of town travel is involved. But to keep the test as close to the real thing as possible do not use the advanced warning to cheat (perhaps by sending additional materials to the off-site location that would not be there in an actual disaster).

The disaster recovery testing should include all of the components of the written plan. This most likely will include setting up the operating systems, installing the DBMS, recovering applications and data, and testing the recovered environment for success or failure.

Additionally, you should periodically review the contents of your off-site tapes in between regular disaster recovery tests to ensure that they contain the correct backu data. At the same time you should review all of the additional materials sent off-site to assure that everything that is supposed to be there according to the plan actually is there.

Without a plan you will be unprepared in the event of the unthinkable. Without regular testing, your plan might be useless. Be sure not only to create a contingency plan, but to test it on an on-going basis.

From Database Trends and Applications, April 2005.



Home.