

# DATABASE

## TRENDS AND APPLICATIONS

Solutions for the Information Project Team • [www.dbta.com](http://www.dbta.com)

Volume 19, Number 12 • December 2005

## Managing "Under the Radar" Disruptions to Business Continuity

By Rick Weaver

When people think about "business continuity," there's a natural tendency to think about "disaster recovery." Given the number of recent natural disasters, this is only to be expected. My own recent travels have been impacted by an earthquake in Tokyo, a typhoon in Shanghai, a power failure in Los Angeles, and hurricanes in New Orleans and Houston. In all cases, there were businesses prepared with a disaster recovery plan that survived the disaster, and some businesses that were not prepared--and are still down.

When it is implemented and managed properly and consistently, disaster recovery works. But in the long run, a simple disaster recovery plan is not enough for ongoing business operations. Business continuity encompasses much more than just a good disaster recovery plan. There are many low-level events that can cause an interruption of business. And "business" is the key word here.

### Continuity and Process

This is why a discussion on business continuity should quickly escalate beyond the topic of disaster recovery. Site-wide disaster is only one of many events that can derail a business process. More often than not, disaster recovery planning isn't enough. For example, everyone is talking about "business service management" (BSM) these days. The underlying theme of BSM is that to be successful and competitive, a company must align its IT environment to its business processes. This alignment relies on application availability and performance. If the customer can't execute a sale because an application is down, the customer may well walk away and go to a competitor.

Business continuity requires that the IT

infrastructure support business processes, no matter what situations arise. But there are many things to consider in a business continuity plan. If you sit down and list all the data center components that have to work successfully for a business process to execute as required, you're going to come up with a list that includes hardware, software, communications, facilities, and operations. If any of these components fail or degrade, the service provided by them will impact the success of the business process.

Hardware glitches are one issue that needs to be examined in a business continuity strategy. Processors, storage devices, tape drives, network routers, and other technology components are very reliable, with increasingly improved mean-time-to-failure metrics. However, these components do occasionally fail, causing a business interruption. It is unlikely that the failure of a single processor or a storage array would cause a company to invoke their disaster recovery plan, which is typically based on a premise of total site failure due to catastrophic event such as a flood.

Software failures may also create disruptions to the business. In some cases, a software failure can cause widespread outage; for instance if the operating system fails, all DBMSs and applications running on that OS are unavailable. Migrating to a new version or performing maintenance on an existing version are frequent causes of an IT outage.

Communications failures may also inhibit business continuity. One of the biggest issues discovered during several recent disasters is that the customers and users of a business application couldn't access the data, even though it did survive the original disaster. Even though the data center was "available," the business

process was not, so there was no business continuity. That potential business was lost, probably forever.

Work areas also need to be included in business continuity planning. A natural disaster, for example, could displace a population. A broad power failure or transportation shutdown could immobilize employees. Thus, workers can't get to their posts to manage the applications and data. Alerts will go unheeded and business processes will begin to fail.

### Need for Data

At the heart of any business continuity effort is data, the core business asset of the IT infrastructure. The ability to capture customer information and execute a business transaction requires access to the data. Implementing a business service management strategy will help the IT group monitor and manage the components in the infrastructure, ensuring the linkage between the business process and the databases they need to successfully execute.

For example, a database may be about to use up its allotted space. A solid BSM solution would spot the database trending towards a space outage and automatically notify the appropriate personnel to resolve the problem before it causes a business service outage. An even better solution would automatically resolve the problem by performing an online space reclamation process to prevent the problem from causing an outage.

Business continuity is mission-critical. Good IT infrastructure support is a competitive advantage for the company that ensures business continuity.

*Rick Weaver is product manager for mainframe database recovery at BMC Software, Inc.*