

With 100% Uptime, Do I Need a Business Continuity Plan?

October 2006

In our article entitled [All About Continuous Processing Architectures](#), we pointed out that active/active application networks are capable of incredible availabilities – uptimes measured in centuries. One might well question the need for a Business Continuity Plan if the system is never going to go down.

No assumption could be more fallacious. Extreme availability does not mean an absolute 100% uptime. Even if our calculated uptime is in the thousands of centuries, that means that on the average there will a system failure during that interminable time. And as random events go, that failure could be tomorrow. We might not expect another one for 10,000 years, but we had better be able to deal with tomorrow's failure. That is why we always need a good Business Continuity Plan. How is the business going to survive tomorrow's failure?

It is true that an active/active application network will protect us from a myriad of faults. Hardware faults, software faults, operator errors, environmental problems – these generally will only affect one node. The same is true for most natural and man-made disasters. Should a node go down, users quickly can be switched to other nodes. That is what active/active is all about.

However, there is a wide range of faults that, though highly unlikely, could take down your entire application network. This is why a good Business Continuity Plan is a must. What is the probability that a second node could fail before the first failed node is repaired, thus leaving the system with not enough capacity to maintain the business? No matter how small the probability that you calculate, you may have two nodes down simultaneously someday. And that someday might be soon.

Does your system have network-wide commands that could cause wide-spread damage if used improperly by your operators? Hopefully, you have put in safeguards to prevent this; but have you really covered all of your bases?

Are your nodes and database copies distributed widely enough so that the equivalent of the 2004 Northeast blackout in North America will not take down all nodes? What is the chance that a massive network failure could disconnect all users from their nodes? Can a software bug propagate through the network? (Do you remember the software bug that propagated through the ATT network in 1990 and took down the entire network, thus denying telephone service to subscribers for hours? A decade earlier, a similar bug collapsed the ARPAnet.)

What about a health crisis like the recent SARS and Avian flu scares? Fortunately, they didn't become an epidemic, though it was within the last century (1918 to 1919) that the Spanish flu killed 20 million to 40 million people worldwide. This could decimate your operations staff. What if your buildings housing your systems were quarantined by a similar epidemic and could not be entered?

Is your operations staff unionized? What happens in the event of a strike? Can your supervisory staff and others less trained in the operations carry on service?

And, of course, there is always the present danger of attacks by viruses, worms, hackers, and denial-of-service attacks. No matter how smart you are at protecting your site from such outside dangers, there is always a hacker who is smarter. Furthermore, don't forget the easiest way for your system to become infected – one of your people innocently bringing in his or her infected notebook and logging onto your system.,

Consequently, there must be in place a plan directing the efforts of all concerned so that your business can recover from such disastrous occurrences. Simply having an extremely available system is not good enough. One must plan how to recover from a highly unlikely, but not impossible, total system outage.

This plan is, of course, the Business Continuity Plan; and it is the subject of much literature today. Though proper business continuity planning is beyond the scope of the Availability Digest, there is much in the way of good literature concerning these plans (just Google Business Continuity Planning or see our review of [Business Continuity Planning: IT Examination Handbook](#)). Also, there are many significant consulting services being offered to help you write your plan (offered by, among others, IBM and HP). Without a good Business Continuity Plan, one cannot say that one has approached 100% uptime because otherwise, that one-time failure of the system could have disastrous consequences.

Of course, any Business Continuity Plan must be kept up-to-date and practiced periodically. A Business Continuity Plan that does not reflect the current business or IT environment, or a plan that is unfamiliar to the people who must implement it, is no more valuable than the dust that covers it.

Though needed for an active/active system, Business Continuity Plans are generally associated with "highly available" systems such as clusters in which occasional outages are expected. This leads to an important distinction between these plans and Continuous Processing Architectures. *A Business Continuity Plan is used to recover from the effects of an outage. A Continuous Processing Architecture is used to avoid the effects of an outage.*