

Business Continuity – 5 Critical Points

When designing a Business Continuity Plan the first thing you should consider is Disaster Recovery. According to Wikipedia, Disaster Recovery is the process, policies and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organization after a natural or human-induced disaster. Disaster recovery is a subset of business continuity. Also, Business Continuity is the activity performed by an organization to ensure that critical business functions will be available to customers, suppliers, regulators, and other entities that must have access to those functions. These activities include many daily chores such as project management, system backups, change control, help desk and many others based on the type of business. Business continuity is not something implemented at the time of a disaster; Business Continuity refers to those activities performed daily to maintain service, consistency, and recoverability.

While business continuity involves planning for keeping all aspects of a business functioning in the midst of disruptive events, disaster recovery focuses on the IT or technology systems that support business functions. When looking at business continuity testing and disaster recovery testing, probably the last thing you think about is performance. The system's performance is good or at least adequate in your main office, so why will it be any different in a backup or disaster recovery site? Most organizations that have a business continuity plan, test it in some way, but do they test that not only can their systems run on the equipment at the disaster site but that they can run successfully, i.e. accurately and with the required performance?

The systems in your primary site have been tuned to provide the necessary performance. Running your systems on a different site could produce completely different performance, even if you think the specification of the equipment is the same. Different makes of machine, even if quoted as being the same power can produce different results depending on other internal factors such as chipset, type and speed of memory and numerous other parts which can differ between machines.



Intelligent Business Solutions Ltd

- 1. Central machines/servers:** When looking at central machines it does not necessarily mean that the backup machine should be the same specification as the original primary machine. You should carry out the proper sizing in order to determine the appropriate specifications for the backup machine, in order to handle the workload at the given time. According to the Disaster Recovery strategy you have to define and prioritize the criticality of your applications.
- 2. Network:** At the disaster site it is assumed there is a network. It is assumed that according to the criticality of your business and the necessity of an internet connection you will have a standard internet connection and a backup connection. You have to make sure through the proper procedures that the network at the recovery site is frequently tested and maintained. As well as either replication of data is running smoothly and the backup and restore procedures are indeed tested and working. There is no point in having a disaster recovery site, if when you need it, it will not work.
- 3. Desktop:** A business continuity plan considers that your existing offices in case of a disaster will no longer be usable, therefore the business side of your organization has to relocate, what desktop machines will be available and where? Almost all of the time are companies acquire new and more powerful desktop, they relocate the older ones to the disaster recovery site; this create an issue that the older pcs' at the recovery site will eventually be so outdated that will not be able to run the new applications currently being used at the primary site. You have to consider both the hardware and software specification of the desktop machines at the secondary site.
- 4. Testing all systems:** As previously mentioned we need to setup procedures that will define: WHEN, WHAT, and HOW will we test. Can the machines in the recover site run the necessary applications in the desired time-frame? It is common to simulate a disaster and document the results during the recovery, having in mind 3 key factors: a) procedure b) task assignment c) timing.
- 5. Automated testing:** Your production environment is very dynamic, continually being updated and upgraded. Most organizations are testing the updates in the production



Intelligent Business Solutions Ltd

environment. It is important when carrying out application testing at the primary site to also test at the recovery site. Many organizations use automated test tools that give you the ability to test and record as well as monitor systems at both sites.

In summary, all business continuity and disaster recovery plans require proper procedure placing and thorough, repetitive testing, as well as performance testing. The faster recovery times, the better the chances of the business surviving.

IBSAC Intelligent Business Solutions Ltd

George Agathangelou
Professional Services Director

MCTS, MCSA, CCSE, CITM, DCUCSS, RSA CCE
HP-ASE, HP-APS, HP-ASP, STS, VSP, VTSP

14 Spetson Street
Limassol 4000, Cyprus
Phone : +357 70088022
Fax : +357 25754550
Email: info@ibs.com.cy
Web: <http://www.ibs.com.cy>