



## THREE PRINCIPLES OF BUSINESS CONTINUITY

This ARTICLE IS REPRINTED BY PERMISSION OF THE AUTHOR AND ENTERPRISE STRATEGIES, A WEEKLY E-NEWSLETTER FROM ENTERPRISE SYSTEMS (ESJ.COM).

COPYRIGHT 2008, 1105MEDIA LLC

## Three Principles of Business Continuity

By

Jon Toigo

In the previous column, we talked about some of the challenges facing planners who are seeking to deliver a business continuity capability to their firms. Three big ones consisted of coping with disk drive failures that can compromise RAID schemes, building an effective tape backup program, and herding cats in the form of the multiple, proprietary data replication schemes that just about every hardware and software vendor are building into their wares these days.

Without saying so, the message of the column was that data is key to recovery. Next to personnel, data is your most irreplaceable asset. Without people or data, you can restore all of the systems and networks that you want in the wake of a disaster without realizing the continuity of operations that the Front Office is seeking.

This concept, while easily grasped, is just as easily forgotten as we go about the business of disaster recovery planning. It is easy to lose sight of the primacy of data protection when you become immersed in the vetting of strategies for recovering this system or that one, not to mention the allure of marketing pitches from various vendors regarding the blessings of server or storage virtualization, failover clustering, or other panjandrums.

Protecting your data is one of the three fundamental principles of business continuity. It is one with some far reaching ramifications in terms of how planning should be undertaken and who should run the plan development process.

Breaking this down, there are some views of business continuity planning floating around that need some adjustment. The first of these is that continuity planning should be undertaken by a non-technical type. If some technical understanding is required to build a strategy that protects a given mission critical system, the non-technical planner can simply ask for the assistance of knowledgeable IT folk to define a solution. While such a view has the potential merit of enlisting a non-technical person with considerable “people skills” into the leadership role – someone who can interface with business stakeholders in the company to define mission critical business processes and their underlying IT support structures – it also imposes a practical limitation on planning efficacy.

Truth be told, business continuity planning cannot be undertaken successfully by a non-technical administrator. Planning does not begin at the moment that management funds the project and investigatory activities commence into the operational

processes of business units. Continuity planning needs to become part of other processes.

When hardware platforms are evaluated for use by the company, procurement needs to be advised regarding continuity aspects of their choice. Selection criteria, specifically keyed to equipment manageability and recoverability, need to be put forward so that the right gear is selected, purchased and deployed. You can't protect what you can't see, so manageability via a common management platform preferred by the company, should be just as much of a vetting criterion as, say, performance and cost. Also, a lot of hardware vendors offer redundancies in key components such as power supplies, controllers, etc. that can make the difference between a failure that results in a minor inconvenience and one that results in a cataclysmic disruption. Unfortunately, these features are often offered as add-ons to the base product and are overlooked by procurement officers unless they are directed to buy them.

The continuity planner needs to be able to advise procurement in order to build in continuity to infrastructure hardware components. This presumes a certain degree of technical acumen.

Technological savvy is also required of the planner if he or she is to impact the recoverability of applications themselves. In shops that build their own client/server applications, the planner must be able to sit down at a table across from application developers and make suggestions that will improve the resiliency of their wares. For example, using message oriented middleware, rather than remote procedure calls or other approaches that require hardwired connections between application components, can be a boon when it comes time to build a recovery environment. The former technique enables apps to be re-hosted on the fly and on different hardware platforms than are used in production settings; the latter requires the maintenance of two environments in which every configuration change must be mirrored exactly within the shadow infrastructure – a daunting and expensive proposition even with the aid of “infrastructure wrapping” and “geo-clustering” products discussed last week from CA and others.

Even when off the shelf software strategies are in play, whether shrink wrapped ERP or server virtualization wares, the planner's ability to advise the CIO or CTO about the continuity ramifications of his or her choices is key. Too often, the reason why applications and their hosting environments have not been constructed for recovery is because nobody ever made it a priority – or mentioned continuity at all.

Bottom line: the continuity planner does need to bring technical acumen to the job. It is all that stands between building in continuity or needing to bolt it on, which is always the more costly and painful undertaking.

But even with an infrastructure and application set that are designed for resiliency and recovery, there is the central problem of data. To IT folks, it has been correctly ob-



served, data is just an anonymous set of ones and zeros. They focus on data protection in its most banal form: replicating ones and zeros across media to protect the data. The three approaches are tape backup, disk mirroring, and copy on write.

Tape backup is well understood yet much maligned. Make a copy of data to removable media, move the copies out of harm's way (usually to an offsite storage company), then grab the tapes and take them to a recovery center if a disaster interrupts normal operations. There, you read the contents of the tape back onto disk and continue normal operations. It works and works well, despite what you read in analyst funny papers, if you observe some simple guidelines about tape management, handling, storage and retrieval.

Tape restore takes time, of course, that certain business processes (though definitely not all) can not tolerate. When this is the case, support "always on" applications with more expensive near-real-time data copy in the form of either disk to disk mirroring over distance or copy on write over distance.

Disk mirroring is expensive (very much so compared with tape) and falls prey to vendor-specific lock-in techniques that require only vendor A's gear to be used at both ends of the replication process. However, for the companies that use it, a risk assessment has determined that the cost is offset by the business value of failover-based continuity.

Going forward, the real time data replication process will inevitably become less vendor proprietary. Companies like Zetera in Irvine, CA are showing the way. The company sports a storage interconnect based on UDP and IP networking. Using UDP rather than TCP (both are part of the Internet Engineering Task Force's vaunted IP Protocol Suite), the target of a data write can be defined as a set of disks that are local to the application as well as a set of disks that are remotely located. That means that when an application writes some data to disk, it is in fact writing it to two different locations at once.

Another approach that is hardware agnostic for data replication is proffered by Moonwalk, a data management software company in Australia that has become a darling of several prominent storage ware makers. Moonwalk facilitates a true "file area network" by providing a lightweight Java agent-based approach for managing the movement, copying and migration of data around infrastructure. You can set up some simple rules, designate target destinations and replicate and manage data on an ongoing basis.

Data must be managed via Moonwalk or some other mechanism if it is ultimately to be protected. You need to understand what data pertains to which application and which application supports which business process in order to ascertain the business value of data itself. Only in this way can you provide appropriate protection services to the data and ensure the availability of that subset of data that will be needed in a hurry if an

interruption occurs. Implementing a data management scheme is a priority list item for a continuity planner, even if some consider data management to be outside of the scope of disaster recovery planning – which is unfortunately too often the prevailing view.

Without data management, it is almost impossible to do the heavy lifting of continuity planning. Without data management, everything must be backed up because we don't know what will be required to support a specific process we have designated to be business critical. This, in turn, stresses tape backup to the breaking point: in addition to backing up critical data, we are backing up umpteen petabytes of duplicate and contraband data – because we don't know which is which. If mirroring or copy on write are being used for data protection, we run into substantial problems of cost for redundant hardware or extra bandwidth to handle the replication of our total storage junk drawer.

Protecting data is one of the three principles of solid continuity planning. The other two are protecting people and keeping business value in mind at every stage of the planning process. Clearly, you need some good evacuation planning and contact lists to facilitate the health and needs of employees, so we won't dwell on this point here. However, business savvy is the ultimate practical determinant of effective continuity planning.

Management must authorize planners to do their work. They must give planning activity high visibility to ensure the cooperation of business unit managers. And, they must fund not only the development of the continuity strategy but also its maintenance and testing over time.

The latter is especially important, since the continuity planning impetus appears to spike in the wake of a highly publicized disaster, then wane rather quickly in many companies. Part of the reason is cost: it is anathema to management to spend money on a capability that may never need to be used. To keep management interested and engaged, it is important to present the full business value case of planning and to demonstrate smarts when it comes to how you are spending hard to come by cash.

Emphasize minimum equipment configuration. This means simply that the infrastructure at the recovery site does not need to be everything you have on the floor at the production center. Chances are good that in the hours or days following a disaster, you only need to have a subset of the most critical systems up and running and that workload will be far less than what you have in normal business operations. Let management know that you are making intelligent and cost effective decisions about what will be restored and at what price.

Secondly, emphasize dual use value of the elements of your plan. Data management not only serves to identify data that must be protected, but also helps define appropriate data hosting approaches in day-to-day operations. The capacity wastage that is all



too common in enterprise storage environments is illuminated by data management, so your data management strategy can help optimize infrastructure and reduce cost in addition to affording better continuity services. This same concept applies to other plan elements, such as redundant user work areas. A dual use value of such a facility might be its re-purposing as a user training center, call center or customer meeting site when it is not being used for disaster recovery.

Finally, in everything you do, show management that you have an eye on the bottom line. Identify options for replication and explain your rationale for selecting the approach you have chosen, emphasizing not only efficacy, but also cost efficiency. The Hummer H2 uses exactly the same chassis as the Chevy Tahoe, but costs \$40,000 more. Given the skeleton crew that will be operating your recovered systems, reduced workload, and smaller application and data sets, you might be able to get buy with SATA rather than FC storage and iSCSI or UDP rather than an FC fabric at your recovery site. In fact, your recovery center might have dual use value as a location to try out alternative technologies that can then be introduced into the production environment reducing CAPEX and OPEX costs.

Successful continuity planning comes down to protecting data, protecting personnel and demonstrating some fiduciary common sense. The planner needs to know a lot about business, technology and especially data. Your comments are welcome: [jtoi-go@toigopartners.com](mailto:jtoi-go@toigopartners.com).



Moonwalk Universal specializes in large-scale data management solutions. With a support base that spans Europe, the USA, Australia and Asia, Moonwalk Universal solutions encompass best of breed technologies, created by some of the world's leading IT innovators.

**Contact us**

For more information about Moonwalk Universal please visit us on the web at:  
[www.moonwalkinc.com](http://www.moonwalkinc.com)

Moonwalk Universal Pty Ltd  
Milton, Qld, Australia  
T: +61 7 3247 1080  
F: +61 7 3247 1084  
E: [info@moonwalkinc.com](mailto:info@moonwalkinc.com)  
W: [www.moonwalkinc.com](http://www.moonwalkinc.com)