

STORAGE SWITZERLAND REPORT

RESTORING CONFIDENCE - BACKUP SYSTEMS SHOULD RESTORE MORE THAN JUST DATA



Eric Slack, Senior Analyst

Organizations need more than a backup system they know is working, they need a data protection system they can have confidence in. This confidence comes from being able to verify that critical business processes, not just the data, can be restored within an appropriate timeframe. Most have implemented a backup application and simply assumed that running it would provide the data protection they needed. But by default these systems don't always protect the most critical data efficiently or provide adequate verification of the process.

In essence, we've assumed that if we complete backup tasks that adequate protection for all data, including the most critical business assets, will follow. This explains why the bulk of data protection management tools and applications focus on keeping track of backup jobs and telling you when they've been done, or when they fail. They don't take a step back and help you determine which job failures have the most impact on the business or how certain failures can impact service level agreements and create customer satisfaction issues. Given the amount of data that most backup systems handle, the 'welfare' of critical subsets of data can be difficult to maintain and difficult to verify. In short, you can't take steps to protect the enterprise's most important data (ie: that which must

be restored first, the most difficult, or impossible, to recreate, etc) when focused on the *entire* data set that's running through the backup system.

In an attempt to resolve this lack of verification issue, people typically add more 'protection' for critical data sets. This often results in that critical subset being protected by a number of different processes in addition to the backup application (snapshots, application dumps, etc.) compounding the challenge of ensuring verification of protection and subsequent recovery of the data. Ironically, this 'belt and suspenders' approach can complicate the entire process further and render the existing system *less* effective.

Fixation with Backup Windows

Similar to this 'focus on everything' mentality that's common with backup applications and the way most monitoring tools work is a preoccupation with the backup window. When having data protection means simply that backups are complete, and it's assumed that *all* backup jobs must be completed, then the timeframe in which this process runs becomes all important.

But when the focus, instead, shifts to only a critical subset of an enterprise's data, and the system's ability to restore it in support of required application service levels, then the backup window is less important. What becomes more important than having backups of *all data* completed is having *the right* data backed up and the confidence that comes from knowing it's protected.

The "right data" refers to data which impacts the business. Rather than asking "did the backup window complete?", IT should be asking "did the jobs *that matter* complete?". IT needs intelligence about the data protection system and how its supporting SLAs to determine which jobs really matter. A Data Protection Services Management (DPSM) system like [Bocada's Prism](#) can help provide this intelligence to assure that the data protection system in place is effective - and to provide regular verification that its in force. In short, instead of the backup window, IT should be preoccupied with its SLAs and having the right policies and procedures in place to support those service levels.

An Effective Data Protection Process

The first step is to collect data on the process itself and establish a functional baseline for the existing data protection system. These data points include not only 'snapshot' conditions, like backup successes and failures, but also histories and longer term trending. These give a more complete 'moving picture' across multiple business and backup cycles to illuminate weaknesses in protection. In addition, this baseline should also look at 'over-protection'.

This refers to backup jobs that run on data that's no longer important or backups taken too frequently, 'just to be sure'. While this may increase confidence, it can actually reduce overall effectiveness of the system. Resources wasted on inappropriate backup jobs are resources that aren't available for those that *are* appropriate. This 'opportunity cost' can mean storage capacity, admin time, network bandwidth or application windows are unavailable when really needed by the system to handle critical tasks.

After the current system functionality is known, service levels should be confirmed effective to meet business needs. This may require engaging outside consultants to modify or create SLAs, but these parameters are fundamental to assuring business continuity and establishing a framework with which to measure success of the data protection system. It follows then, that they need to be in place before the data protection process can be made effective. Then backup system policies can be reviewed against these SLAs and modified as needed. Ideally the DPSM system would be able to partition or subdivide clients and data sets within the environment such that standards of protection can be applied, based on application, geographic location, users, business units, etc. These standards can be created to support specific SLAs for each of these 'zones' and monitored to assure continued compliance.

Verify and Manage Data Protection

After its deemed effective at protecting the organization's data and providing the availability needed to restore operations, the data protection system should be verified on a regular basis. Confidence comes from the knowledge that protection is in place and is in force. Ongoing management of the system includes continuous monitoring of critical task completion, but also management of the policies, the standards and the changes that occur in a dynamic environment. This verification could even be made available for business unit 'customers' and management, directly if desired, so confidence that the business is protected can be shared throughout the organization.

Confidence in a data protection system comes from the knowledge that its processes are effective and its operationally up to date. Traditionally organizations have relied on the backup system to do this and assumed that simply completing its tasks meant that data was protected. Unfortunately this is not accurate. Instead comprehensive SLAs and a DPSM process are needed to confirm that the system is effective and current, to provide regular verification, and to deliver the confidence that the business is protected.

About Storage Switzerland

Storage Switzerland is an analyst firm focused on the virtualization and storage marketplaces. For more information please visit our web site: <http://www.storage-switzerland.com>.