

STORAGE SWITZERLAND REPORT

DOING MORE WITH LESS RISK



Eric Slack, Senior Analyst

IT is being squeezed to be more productive and get more done with fewer resources. This can mean expanding infrastructure without buying storage capacity, without consuming more power or adding to administration workload. There are a number of ways to increase productivity, but trying to do more with less involves change and change brings risk. In IT, a process that increases productivity but also increases risk isn't usually an appealing solution. The trick is to get solutions that provide the needed increases (getting more done), within budget (with less), while keeping risk under control.

Risk can be defined as "the probability of a negative outcome". In IT this outcome is usually a system failure, or degradation, sometimes including data loss. Management of this risk requires monitoring systems, like [Tek-Tools' Profiler](#), which confirm the control processes that are working, identify those which aren't and provide tools to correct them. These systems also help to proactively keep the control processes updated and effective in response to potential failure conditions or in response to pending system changes.

Backup

If the risk is failed backup jobs, then risk reduction systems need to report jobs that ran successfully and

allow the focus to shift to potential problems. Jobs that didn't complete must be brought to the forefront and displayed with appropriate information to support troubleshooting and remediation.

The risk of inadequate backups - incomplete or slow to complete - must also be eliminated. Data about client hardware, networks, backup storage and server performance must be examined, as a start. If backups are going to tape, the state of all media in the environment must be provided, including reports on media usage, availability and location. Backup tuning is a fact of life with traditional backup systems, especially if tape is included. Performance and configuration information must be correlated across platforms to uncover potential bottlenecks and failure points before a problem occurs.

Historical information on completion of backup jobs can also be presented for trending and predictive analysis. The objective is to identify which clients and backup jobs are "at risk" for failure in the future. Information on backup software policies can also be provided to help maintain the integrity of the backup process - keeping configurations pertinent and clients accounted for.

Virtual Machines

In the virtual environment, the risk typically faced is running out of resources - storage, CPU and memory. In order to manage this risk, you need information on VM use of these critical resources, presented together, to confirm that current VMs are adequately provisioned. Also needed is visibility into the physical environment, like storage capacity by resource (SAN, NAS or DAS) and CPU utilization by ESX hosts. Thresholds for system resources must be established and monitored to prevent out-of-capacity conditions. Finally, an historical representation of these data and usage modeling scenarios can be used for trending and predictive analysis to forecast growth rates and efficiently plan for expansion. Risk management requires the use of standards for VM provisioning in order to assure process integrity, something also enabled by advanced monitoring systems.

Compliance

As resource utilization is expanded, so must visibility over those resources. IT needs to know how storage is being used, who's using it, and that policies are being observed. Applications that are over their allocation and users that are saving restricted file types (MP3, PST) can point to a pending capacity issue. There's also the risk of external compliance with privacy and legal discovery regulations, which IT needs adequate monitoring and reporting tools to manage.

Infrastructure Management

There's also a risk related to IT job performance, perhaps called 'the risk of bad decisions'. These could be making the wrong purchase - buying an ineffective solution for the problem at hand or choosing the wrong vendor. It could

also be paying too much for the right solution. It's likely that more scrutiny will also follow these decisions. In this climate of more IT activity without more resources, you need more information faster, in order to make and support quality decisions.

Not only must IT maintain systems health and uptime in a cost-efficient manner, it must also be done in a controlled fashion. 'Fire drills' and close calls don't indicate good management. You need the ability to predict resource requirements ahead of demand and have the data to back up these projections. Here too, the right monitoring and process control information can reduce the risk associated with making poor decisions in the pursuit of getting more done.

Conclusion

In this climate of doing more with less, IT finds itself facing more risk as a result. These can be the risk of failed backups or inadequate data protection or the risk of resource exhaustion in virtual server environments. It can also be the risk of compliance with internal data policies or external regulations. Trading increased productivity for increased risk is not acceptable. IT needs comprehensive, effective monitoring tools to manage the risk out of this environment.

Managing risk requires important information be made available and separated from the impertinent data. IT systems produce more information than is needed for effective control. Ironically, the sheer volume of the data available can quickly obscure the critical information needed to make quality decisions. IT must have systems that can cull these critical pieces of data from the rest and present it in a way that supports sound decisions and enables more productivity with less risk.

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>.