ISG™ imagine your future®

DEFINING THE RIGHT DATA PROTECTION STRATEGY

The Nuances of Backup and Recovery Solutions

Cindy LaChapelle, Principal Consultant, ISG

ISG WHITE PAPER © 2012 Information Services Group, Inc. All Rights Reserved

INTRODUCTION

Most organizations have traditionally believed that having data backed up and stored off-site is sufficient to ensure data recovery and maintenance of business operations. In this environment, well-defined disaster recovery plans and regular testing have not typically been priorities. In recent years, events such as the 9/11 attacks and the tsunami in Japan have caused many organizations to reassess their overall data protection strategies for data backup and recovery, disaster recovery and business continuity as well as long-term retention and security of their data.

However, most business downtime is caused not by catastrophic events or major natural disasters, but by hardware failures, data loss, power outages or UPS failures, network outages, security breaches, human error and application failures. These factors can do just as much damage to the organization's long-term performance and reputation.

As data volumes and retention requirements grow in response to business demands and regulatory mandates, data protection strategies must ensure that critical business data can be accessed and recovered in a timely fashion.

Many IT organizations still employ data protection strategies from 5 or even 10 years ago.

Server and storage virtualization, data center consolidation, explosive data growth and new compliance requirements are major change drivers within the data center, but many IT organizations still employ data protection strategies from 5 or even 10 years ago. In a rapidly changing environment, determining the "right" data protection solution is no longer a black and white issue, but rather a grey area that involves myriad considerations that impact complexity, effectiveness, and cost.

This ISG white paper is designed to help IT organizations navigate the nuances of data backup and recovery and select an appropriate data protection solution that addresses business needs.

 © 2012 Information Services Group, Inc. All Rights Reserved

GREY IS THE NEW BLACK FOR DATA PROTECTION

The right data protection strategy must ensure that the backup and recovery solution goes beyond basic recovery of the occasional lost or mistakenly deleted file. It must also be leveraged to provide the right level of disaster recovery and business continuity capability.

At the same time, given the reality of flat or decreasing IT budgets, the data protection solution must effectively balance cost and risk factors.

Traditional "black and white" backup and recovery solutions were typically implemented over a shared IP network with data being backed up to physical tape media in an automated library. Incremental backups occurred daily while full enterprise data backups were conducted every week or two, normally during weekends. Occasionally, backup pools were established with different retention parameters for different data types or file systems but many organizations simply backed up all of their data with a plan to keep it "forever."

If asked, they could legally, and honestly, state that they had the data - and then pray that nobody demanded it be restored.

Backup was used to recover lost user files and as a basic strategy to provide some guarantee of business continuity in the event of a major event or disaster. Full recovery of a critical environment from backups was rarely tested. Many organizations maintained older legacy tape media formats without any reliable means to recover the data that resided on them. The attitude was that, if asked, they could legally, and honestly, state that they had the data – and then pray that nobody actually demanded it be restored.

As compliance regulations grew and e-discovery requests became more common, businesses recognized that the policy of retaining data forever could come back to haunt them. For one thing, attempts to migrate older legacy data were often largely unsuccessful as well as extremely costly. Standard backup strategies lacked processes to migrate relevant data as tape technologies were retired. To further compound the problem, many backup tapes with a "forever" retention mixed irrelevant data together with data that legally had to be kept for compliance reasons.

Additional factors affecting backup and data protection strategies include the following:

1. Shorter or nonexistent available windows during which backups can run.
2. Backup complexity associated with virtual server environments and multiple backup technologies.
3. Legal time limits to recover data in e-discovery requests.
4. Changing compliance requirements for retention.
5. The need to delete data once it is no longer required.

 © 2012 Information Services Group, Inc. All Rights Reserved

6. Exponential growth in primary data that translates into unmanageable growth in backup data sets.

7. Backup complexity due to requirements for more frequent backups of some key business-critical data sets, different retentions, etc.

In this changing environment, organizations require complex business-focused backup and recovery solutions and implementations. Each "shade of grey" solution requires considerations of cost, complexity, risk implications, recovery time and recovery point objectives, technology options, alignment of retention to changing business and legal needs, etc.

Recovery point objectives (RPO) associated with daily backups may not satisfy targets defined in the disaster recovery (DR) plan, particularly for some business-critical applications and data stores. In the latter instance, alternate data protection strategies may be needed in conjunction with backups as part of the overall DR strategy. In a DR plan, the RPO and the RTO (recovery time objectives) need to be defined based on business need and criticality. The plan should also define what systems need to be in place (and where they should be located) to get the key business applications up and running again. Often, critical system and application RTOs are shorter than the typical 24-hour interval associated with daily backups, so other data protection technologies and strategies (such as remote replication or mirroring, snapshots or point-in-time copies, or continuous data protection technologies) may be required.

The cost of disaster recovery needs to be carefully balanced against the business risk and cost of downtime.

The cost of DR solutions needs to be carefully balanced against the business risk and cost of downtime. To address this challenge, many businesses are reviewing cloud-based backup and storage options for disaster recovery.

OPTIMIZING DATA PROTECTION

A business case for an enhanced data protection strategy must address all relevant costs and risks to ensure alignment to business requirements for data backup and recovery. Design the backup and recovery solution to be flexible. As business requirements evolve, modify the data protection strategy to integrate new and emerging technologies which add necessary functionality and/or greater responsiveness to the overall backup and recovery solution.

Leverage multiple storage technologies to provide the right level of flexibility and responsiveness while balancing cost and complexity. Virtual tape libraries (VTL) and disk-based backup solutions leverage online disk storage to provide faster backups and faster recovery times for key systems and applications and frequently-used data. To control costs, while still addressing responsiveness and compliance requirements, migrate disk backups to lower-cost tape storage as they age. Disk and VTL solutions also offer deduplication capability, which can significantly reduce the overall storage required by limiting backup to data changes.

ISG WHITE PAPER © 2012 Information Services Group, Inc. All Rights Reserved

An all-disk backup solution that eliminates tape completely can become very expensive and introduce different challenges for data with long-term retention requirements that exceed the lifespan of the disk technology. New advances in tape technologies, such as linear tape file system (LTFS), may provide reasonable alternate approaches to disk-based technologies for both faster access to backup data and for lower performance storage tiers for archive solutions. LTFS is a self-describing file system that makes files on tape directly host-readable, enabling tape to be used in the same fashion as a USB drive.

The backup and recovery solution therefore must be flexible and frequently reviewed and updated to reflect the evolution of the business and supporting technologies.

To select the right mix of automated tape, virtual tape and disk-based technologies, consider business requirements for backup and recovery performance, data access and retention (both short and long term), reliability, ease of management and cost. However, the right mix of disk and tape today does not necessarily guarantee that future business needs will be met. The backup and recovery solution therefore must be flexible and frequently reviewed and updated to reflect the evolution of the business and supporting technologies.

Alternatively, some organizations enhance their existing backup solution with cloud-based backup and storage services. When choosing this option, verify that SLAs are aligned to the business RPOs and RTOs for data recovery for the applications and data sets being backed up to the cloud. In addition, make sure that all internal business requirements for data security are being met and that cloud service capabilities are reviewed on a regular basis, as compliance and regulatory requirements can change with time.

With virtual server environments that share the same data store, backups must be fully integrated with the overall backup solution to avoid backing up the same data stores multiple times. Leverage technologies like deduplication to avoid redundant backups. Be sure to back up physical as well as virtual servers.

A recent study by Kroll Ontrack ("Data Loss in a Virtual Environment – An Emerging Problem", 2011) noted that, "if deployed or managed carelessly, virtualization can itself create business disruptions or data disasters." This study reported that human error (vs. machine error) accounted for 26 percent of systems failures in traditional non-virtualized systems, but 65 percent in virtualized environments.

When adding new servers (virtual or physical), establish a check list to ensure that backups are mapped to the appropriate backup pools, based on business requirements.

1. Map incremental and full backup schedules and frequency to application and server RPOs.

2. Map data retention and deletion schedules to legal and compliance regulations.

 © 2012 Information Services Group, Inc. All Rights Reserved

3. Choose the backup solution storage architecture and software (disk, virtual tape, physical tape, disk migrating to tape, etc.) that meet data and application objectives for available backup windows and restore-time objectives.

4. Leverage alternate, or additional, data protection solutions such as continuous data protection (CDP) technologies, snapshots, or local or remote replication or mirroring for servers and applications with high availability requirements.

5. Ensure RPOs are met by confirming backup processes are in place to:
   - Redo or restart failed or missed backups.
   - Guarantee new servers are configured for backup during the server build.

Backup solution bottlenecks change over time depending on where throughput is limited within the data path. Define a regular annual review process for the backup solution to identify bottlenecks, or potential bottlenecks, and redesign the solution to eliminate or minimize the impact on backup windows and backup success. Bottlenecks within an end-to-end backup solution may occur in any of the following points in the data path:

1. Network Bottlenecks – (IP or fiber channel).

2. Back-end Bottlenecks – (tape libraries and tape drives, disk for backups, etc.).

3. Front-end Bottlenecks – (client servers and backup servers).

Monitor all of these systems to ensure data throughputs are not being restricted.

Monitor and report backup capacity and performance and leverage this information to perform proactive backup capacity and performance planning.

Establish a regular program for testing and validating backups by performing random restores of files and data sets. Integrate this testing with DR planning and testing to ensure that data can be recovered from backups within the required time frames. The worst time to discover that backups are failing or are unrecoverable due to media failures or other corruptions is in the middle of a disaster.

Whenever possible, store backups at an alternate location or secondary data center, or create copies of key backup data as insurance in the event of a major failure or disaster. If tapes are transported off-site encrypt the data during backup to ensure security.

As backup technologies age and refresh, migrate backups to newer backup platforms and media to ensure that legacy backups with long-term retentions are recoverable. Migrate existing backups on legacy formats where possible and, once migrated, retire legacy backup

hardware and software. If a lack of compatible legacy hardware or software precludes migration, delete or destroy backup tapes rather than store them if there is no chance for a successful restore. Make sure the backup data retention schedules align to the business lifecycle, recovery access and availability of the data being backed up.

SUMMARY

Backups are pointless if data recovery fails or is insufficient to meet business requirements and objectives. Don't over- or under-configure the backup solution; rather, right-size the solution and leverage a mix of backup technologies and platforms to ensure a data protection strategy that delivers the right balance between risk and cost.

Backup solutions should not be considered static and expected to run unmodified forever.

Revisit and redesign the backup and recovery solution as the business evolves and requirements change. Once implemented, backup solutions should not be considered static and expected to run unmodified forever. Factors such as exponential growth of structured and unstructured data, new and changing regulatory and compliance requirements, and a greater need for faster and more effective disaster readiness are driving IT organizations to embrace more complex and adaptable backup solutions to address business needs.

Make sure that the backup and recovery solution is flexible and responsive by reviewing and reconfiguring backups as technologies and business needs change. The days of a simple "black and white" backup and recovery solution are over – today's challenge is developing the right "shade of grey" backup and recovery solution that fits your organization's business needs.

 © 2012 Information Services Group, Inc. All Rights Reserved

ABOUT THE AUTHOR

DEFINING THE RIGH DATA PROTECTION STRATEGY
The Nuances of Backup and Recovery Solutions

Published August 22, 2012

CINDY LACHAPELLE
Principal Consultant, ISG

For more than 30 years, Cindy has built expertise in technical strategy, project management, IT outsourcing and data center performance assessments and transformations. She helps clients with data backup and protection strategies, disaster recovery planning and analysis to enable cost-effective technology solutions. She has worked with global clients across many industries in the U.S., Canada, Europe and the Asia-Pacific. Cindy has a BSc degree in honors chemistry from McGill University and a doctorate in planetary astronomy from the University of Arizona. She is a published thought leader on a wide range of business and technology topics and is ITL V3 certified.

ISG™
imagine your future®

ISG WHITE PAPER © 2012 Information Services Group, Inc. All Rights Reserved

ABOUT ISG

ISG (Information Services Group) (NASDAQ: III) is a leading global technology research and advisory firm. A trusted business partner to more than 700 clients, including 75 of the top 100 enterprises in the world, ISG is committed to helping corporations, public sector organizations, and service and technology providers achieve operational excellence and faster growth. The firm specializes in digital transformation services, including automation, cloud and data analytics; sourcing advisory; managed governance and risk services; network carrier services; technology strategy and operations design; change management; market intelligence and technology research and analysis. Founded in 2006, and based in Stamford, Conn., ISG employs more than 1,300 professionals operating in more than 20 countries—a global team known for its innovative thinking, market influence, deep industry and technology expertise, and world-class research and analytical capabilities based on the industry's most comprehensive marketplace data. For more information, visit www.isg-one.com.

Let's connect NOW...

ISG™

imagine your future®

 © 2012 Information Services Group, Inc. All Rights Reserved