Structured: Cloud Backup
A Modern Guide to Optimizing Data Backup and Recovery

What to Consider in an Enterprise IT Environment
A Modern Guide to Optimizing Data Backup and Recovery

Data is the lifeblood of any organization, but many companies are drowning in it. Enterprise data continues to grow in volume and complexity and it is no longer confined to a defined set of local repositories. In the modern enterprise environment, data is stored and accessed on multiple devices and endpoints, including laptops, tablets and smartphones. Corporate data now spans LANs, WANs and geographic locations such as branch or remote offices, creating formidable challenges for managing it and safeguarding it, often with limited resources, budgets and personnel.

The high risks of inadequate data protection

Corporate users have high expectations for data and applications—both need to be available and responsive so they can do their jobs effectively. Data loss can dramatically limit the productivity of workers and affect the company’s bottom line, while a catastrophic data loss event can threaten the very existence of an organization by irreparably damaging the reputation of a business and its brand by rendering it incapable of serving customers.

Most IT professionals understand that protecting data through regular and verified backups is a standard best practice, and nearly all enterprises have backup and recovery systems in place. However, IT organizations face many competing demands
Evaluating the options

Enterprises that proactively seek to establish data backup infrastructure as part of an overall disaster recovery strategy must contend with a plethora of technology options and deployment models, from solutions that are implemented within a company's firewall to engaging a fully outsourced managed service provider that specializes in offering cloud backup services. Evaluating what is right for your organization can be a complex process.

Implementing a comprehensive data backup and recovery plan is an essential role of any IT organization. A properly structured plan not only dramatically reduces risks to the organization, but it can also achieve more effective resource allocation, freeing up IT personnel to be deployed to more strategic initiatives.

This guide will take you through several important considerations for optimizing your backup and recovery systems, including the importance of distributed and remote data, managing physical and virtual environments, resource allocation and data lifecycles. It will also address how to get better insights into what data resides where in your organization, how it is being used, and most importantly, how to ensure that data can be recovered promptly in the event of data loss. Throughout the guide, the roles that cloud backup, recovery and restore (BURR) technologies and services can play will be examined in the context of enterprise IT environments.

Planning for Change

As an organization changes and grows, so does its IT infrastructure. Backup and recovery systems must follow suit to ensure continuous data protection, and a variety of pressures borne out of shifts in both business and technology requires IT organizations to revisit how they protect corporate data.

IT professionals face several significant trends that affect backup and recovery:

- **MORE PEOPLE, MORE DATA**: Whether it's through organic growth or corporate acquisitions, more employees mean more endpoints generating more data.
- **NEW INFRASTRUCTURE AND APPLICATIONS**: The addition of new applications, operating systems, hardware and additional facilities often has a domino effect on your data protection planning and the BURR systems you use for backup and recovery.
- **MORE MOBILE DATA**: The trend toward Bring your own device (or BYOD) means employees increasingly access corporate data and applications on their own laptops, smartphones and tablets. This requires IT organizations to change how they track where data resides, especially because mobile devices are more easily lost, stolen or damaged. In addition, mobile workers who rarely or never come into the office to connect to the company network must also have their data protected.
• **COMPLIANCE PRESSURES:** Depending on your industry, you likely face a gamut of government regulations or professional standards that you must adhere to when handling certain kinds of data.

• **INTRODUCTION OF NEW TECHNOLOGIES:** Some or all of your data protection strategy may still rely on systems such as tape or disk-to-disk, while other aspects of the organization push toward the adoption of cloud. Integrating new forms of technology can present challenges for maintaining the integrity of BURR systems.

• **ADOPTION OF CLOUD-BASED APPLICATIONS AND PLATFORMS:** As enterprises increasingly adopt Software-as-a-Service (SaaS) and Platform-as-a-Service (PaaS) models, more data and applications are residing offsite with third-party service providers. These services may or may not provide sufficient redundancy. Although you are not directly in custody of the data and your custom applications, it is vital that you make provisions for backing them up in the event your SaaS or PaaS service provider fails. A Service Level Agreement (SLA) with the service provider may include backup and recovery but the responsibility ultimately lies with your organization to ensure adequate protection of your data.

• **NEW MANAGEMENT:** Leadership changes such as a CIO may prompt a review and refresh of your entire IT infrastructure or key portions of it, which can raise issues for backup and recovery.

Any of these common scenarios may compel an organization to re-evaluate its data backup and recovery strategy and supporting platforms, especially if a legacy system has technological limitations that prevent it from easily adapting.

**High Risk, Low Reward**

IT organizations are under constant pressure to become more efficient and to do more with less. Even if your company operates in an especially data-intensive industry, the backup and recovery of data is not your core business. However, it is a mission-critical function that requires infrastructure and professional resources.

As much as organizations would like backup to be a set-it-and-forget-it system, the fact is all solutions need some oversight, management and occasional updates. Highly automated “low touch” in-house backup and recovery systems still require regular monitoring and verification to ensure that they are achieving performance benchmarks and adhering to policies for data retention and acceptable recovery windows.

For IT organizations, this is a high-risk, low-reward situation: the value of their efforts may never be recognized until a significant data loss event occurs, but most IT teams are expected to dedicate their focus to more strategic projects.

**Striking the right balance**

Relegating backup and recovery to the backburner is a risky proposition. When managing this function for the business, IT organizations need to strike the correct balance between risk, cost and shifting requirements.

Many enterprises view their IT environments and compliance issues as too complex to simply outsource everything to a managed service provider. But external providers can offer important expertise and the right technology platform can enable a balanced approach to align the value of data with the total costs of protecting it.
In order to optimize how backup and recovery works within the enterprise—and the supporting role IT personnel play—organizations must have a comprehensive understanding of its data and the requirements for restoring it when something goes wrong.

Not all data is created equal

Data is a ridiculously broad and oversimplified term. It is not just a single file created by the CEO or summer marketing intern; it could be a data set, a database, an application or entire operating system, or a snapshot of all live data within an organization at any given time.

To some degree, all data is important, but clearly not all data has the same value to the corporation.

What is your data really worth?

The challenge most organizations face is in assigning the right value to data in terms of how it is backed up. They no longer have the luxury of treating all data equally; they now face a torrent of data from different sources, in different formats and structures. Even with the cost of storage what it is, backing up all of it on the same medium is too costly. IT organizations often struggle to make informed accurate decisions about what data needs to be kept, for how long, and under what circumstances.

One major pitfall that organizations should avoid is choosing to not backup some data at all. Although this can reduce the costs related to storage and data management, it introduces risks that important information will somehow not be preserved. Of course, some organizations may not even realize that some data is not protected, because, it is stored on mobile devices such as laptops, tablets and/or smartphones.

Different data has different demands

A one-size-fits-all approach to data protection is no longer feasible, so backup and recovery strategies must be strategically aligned to business needs in order to balance availability and cost.

A well-designed data backup and recovery strategy should define how to safeguard mission-critical data using a different standard than for lower priority data, such as emails, that still must be retained for compliance or competitive objectives. Depending on your industry and business operations, your data will require a unique range of recovery time objectives (RTO) and recovery point objectives (RPO).

Ultimately, a mix of backup and recovery models might be used; with some data stored on-premise in a central data center while a service provider might store other, less sensitive information in the cloud. Ideally, even this kind of hybrid model could be knitted together by a common software platform that makes it easier to manage and adjust.

Getting a complete picture

Before you can start determining how different types of data are backed up, you need to have a comprehensive view of all data that is in the enterprise IT environment, and how it is currently protected.

Undertaking a recoverability assessment can reveal important information such as:

- The reliability of backup and recovery systems already in place, including its ability to meet recovery time and point objectives (RTO and RPO)
- Whether there are some types or locations of data in the enterprise, such as on laptops, smartphones or tablets, that are not adequately protected
- How existing data storage infrastructure could be optimized to backup data more cost effectively based on its value
- Evidence of duplicate data
- Evidence of out-of-date archived data

External experts in backup and recovery can play a valuable role in completing a comprehensive and independent review of your IT infrastructure and backup systems while assessing organizational risk and exposure. This assessment can be shared with all stakeholders and help make the business case for moving to new models including cloud services.

This recoverability assessment should also be performed within the context of a larger disaster recovery plan to account for all contingencies.

Addressing the data glut

There are two key strategies that enterprises can use to more
efficiently manage growing volumes of data:

DEDUPLICATION—identifying duplicate data that is queued for backup and rationalizing what is stored. Some systems compare all data based on its content so it does not matter if the files are on different servers or have different names.

COMPRESSION—in combination with deduplication, data compression further reduces the amount of data that must be transmitted and stored. The compression ratio that can be achieved depends on the data type, with higher ratios for databases than for image or audio files.

Managing the backup lifecycle

In order to properly align the cost of backup with the value of data, enterprises should ensure that less important information gets relegated to lower cost, lower performance devices. Managing information based on how important it is to a business can save money when it comes to storage and backup, whether it employs a private cloud model or offsite cloud storage.

Backup Lifecycle Management (BLM) is a comprehensive approach developed by Asigra that categorizes backup data into two different types:

YOUNG BACKUP DATA—information that a business needs to stay operational, and is critical to run an efficient business

OLD BACKUP DATA—information that no longer is needed to keep the business up and going. With new low-cost technologies for archiving data, including cloud storage, enterprises no longer need to be concerned about being unable to retrieve information from tapes or microfilm

As information moves from being “young” to “old”, it can be shifted within a tiered backup system, where young and/or high priority data is backed up on a high-performance solution. While older and/or less critical data is relegated to lower-cost and lower-performance backup systems.
Preparing for the worst
At some point, all organizations are inevitably faced with data loss, although it’s rarely catastrophic. The value of your backup and recovery systems and data protection strategy should be judged on your ability to recover and restore data quickly and easily to avoid interruptions in the operation of your business.

Validating backup data
No solution is flawless but some measures can be taken to dramatically reduce common faults in backup and recovery.

For example, enterprise data protection platforms should perform backup file validation to ensure that all the data components have arrived and have been collected in the correct sequence before storing it in a private cloud or off-site location.

Some software platforms are also able to scan the entire storage to ensure data integrity. Leading enterprise data protection platforms feature a process that checks links between the data blocks and compares digital signatures between different encrypted components for inconsistencies. When corrupted data is uncovered, it is marked as corrupted and a notification triggers the data that was marked corrupted to be re-sent. This ensures that the data is always recoverable in case of a disaster.

Other specific tools that a backup and recovery platform should provide include:
• Ability to run regular auditable recovery tests and simulations to ensure RPO and RTO can be exceeded
• Tiered recovery of most critical data first
• Ability to perform automatic switchover to redundant data center with replicated data

Managing backup and recovery operations
Selecting the right technology platform is a critical step toward optimizing backup and recovery operations, but it’s also essential to anticipate what kind of personnel resources will be required to properly manage it and be responsible for restorability when a data loss occurs. Automated processes can provide a lot of efficiency and alleviate some of the burdens of ensuring data is backed up correctly, but enterprises need to have backup systems monitored and promptly address any issues that arise.

For compliance or security reasons, some enterprises mandate that these functions remain in-house. External service providers can still provide critical expertise in designing an optimal backup and recovery architecture as well as manage some aspects of non-critical backup and recovery operations.

Working with a Cloud Service Provider
There is a range of approaches an enterprise can use to incorporate a cloud service provider into its data protection strategy that enables it to strike the right balance between cost and data availability.

PRIVATE CLOUD—controlled behind an enterprise firewall, this backup architecture is owned and operated on-premise by company personnel. This architecture provides flexibility, scalability, provisioning, automation and monitoring with all of the benefits of a cloud architecture without giving up the control of maintaining your own data center.

MANAGED PRIVATE CLOUD—an external service provider actively monitors and manages the private cloud architecture either remotely or on-site.

PUBLIC CLOUD—fully outsourcing data backup and recovery requirements to an external cloud provider with secure offsite data storage requires a lot of due diligence in the service provider and the technology platform it employs. However it frees up resources and personnel to focus on strategic projects.

HYBRID CLOUD—two or more private and public clouds that work together to enable data and application portability. This allows an enterprise to maintain control of an internally managed private cloud while relying on a secure public cloud as needed using the software platform’s cloud architecture to bind the two separate cloud environments together. A hybrid approach provides the greatest amount of flexibility, leveraging a mix of local backup and also offsite protection. It also allows enterprises to architect backup and recovery solutions for specific types of data, such as those from mobile devices or remote company offices.
Regardless of your approach to data backup, you’ve likely encountered the following:

1. Damaged target media, including tape and disk, which requires a costly and time-consuming data recovery service
2. Corrupted backup data
3. Human error in proper formatting of the backup medium or overwriting backup data
4. Delayed recovery process due to backup tapes or disks being stored offsite
5. Accidental deletion of a file or software bug replicated to backup due to remote mirroring
6. Unavailability of IT staff required for recovery and/or restoration
7. Impaired connectivity hampering recovery of a file from the cloud
8. Self-service interface and process for file recovery from a cloud service was too complex for most users
9. Granular file recovery was unavailable—multiple files and applications or an entire snapshot had to be restored for to recover a small number of critical files
10. RTO or RPO could not be achieved

Each of these all-too-common challenges need to be proactively addressed by a backup system, whether it is deployed internally or in conjunction with an external service provider. Consistently reliable and cost-effective data backup must be paired with rapid recovery and restoration at a granular level without complex administration processes or requiring technical know-how.