ConversationalGeek

10 Azure Backup Practical Tips

By Brien M. Posey, Microsoft MVP

#1 Make Sure that You Are *Backing Up Your Data*

Even if your data is in the cloud it still needs to be backed up. Microsoft uses a shared responsibility model for its Azure cloud, in which subscribers are responsible for protecting their own data.

10% of Companies found in a 2020 study, are not backing up their data.
https://www.helpnetsecurity.com/2020/04/03/back-up-data

42% of organizations in the same 2020 study, reported a data loss event that resulted in down time within the past year.

60% of companies that lose their data will shut down within 6 months of the disaster
https://www.bostoncomputing.net/consultation/databackup/statistics/

#2 Use the *Right Tool* for the Job

Legacy backup software designed for on-premises use is often ill equipped to backup Microsoft Azure data. While such tools may be able to protect some Azure data, they may leave gaps in coverage, especially if you use managed (serverless) services in Azure.

33% A third (33%) of organizations used cloud-based backup solutions last year, with the percentage expected to grow up to 50% by 2023.
https://www.itproportal.com/news/backup-failures-are-putting-businesses-at-significant-risk-of-data-loss/

40% IT organizations surveyed don't use third-party backup tools to protect Office 365 data.
https://www.darkreading.com/threat-intelligence/40--of-organizations-not-doing-enough-to-protect-office-365-data/d/d-id/1334283

#3 Use Automation to *Work Smarter*, Not Harder

Automation is the best option for making sure that your Azure data is being regularly backed up. Automation is also an important tool for reducing the chances that human error will result in problems with your backups.

50% of all data loss events are a result of Human error, which is the number one cause of data loss.
https://hostingtribunal.com/blog/data-loss-statistics/#gref

#4 Be Aware of *Cloud Costs*

When planning your Azure backups, it is important to be mindful of the cost. Not only is there the cost per gigabyte of cloud storage to consider, but backing up Azure data to on-premises storage or to another cloud can incur hefty data egress fees. Ideally, a backup application should provide native cost calculation and data management tools to help with these issues.

As many as 95% of business and IT leaders say that cloud billing is the most confusing part of public cloud adoption.
https://www.hostdime.com/blog/data-egress-fees-cloud

A 2021 report by HostDime found that Amazon, Microsoft, and Google would each charge over $2000 in cloud egress fees to transfer 25 TB of data.

#5 Use *Storage Tiers* Effectively

Azure Block Blob Storage is divided into various storage tiers. These tiers vary in terms of cost, availability, and performance. Your tier selection can dramatically impact your backup storage cost.

Amazon AWS offers six different tiers of S3 storage
https://aws.amazon.com/s3/storage-classes

Microsoft offers four tiers for Azure Block Blob Storage
https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-storage-tiers

#6 *Isolate* Your Backup Data

Modern ransomware is increasingly targeting backup systems. Ransomware authors hope that by disabling an organization's backups they will only be able to recover from a ransomware attack by paying the ransom. That's why it is so important to maintain isolated backups that are well out of a ransomware infection's reach.

1. The UK's National Cyber Security Centre recommends "only connecting the backup to live systems when absolutely necessary" and "never having all backups connected (or 'hot') at the same time".
https://www.ncsc.gov.uk/blog-post/offline-backups-in-an-online-world

2. According to Check Point Research, the average number of daily ransomware attacks increased by 50% in the third quarter of 2020.
https://blog.checkpoint.com/2020/10/06/study-global-rise-in-ransomware-attacks

3. According to Microsoft, using Multifactor Authentication can block over 99.9% of account compromise attacks.
https://www.microsoft.com/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks

#7 Consider the Importance of *Data Mobility*

Most organizations have their eyes on some form of hybrid/multi-cloud strategy. Your backup strategy should mirror this, placing an emphasis on backup solution flexibility that supports moving from on-prem to the cloud, cloud-to-cloud, or even from cloud back to on-prem.

92% **82%** A 2021 Flexera study found that **92%** of enterprises have a multi-cloud strategy and **82%** have a hybrid cloud strategy.

#8 Use a *Single* Backup Solution

Standardizing around a single backup solution rather than relying on a collection of various backup products can help to break down data silos and eliminate any gaps in coverage that might exist.

37% 37% of SMBs have lost cloud data due to ransomware, accidental overwrites, and other data loss events
https://invenioit.com/continuity/disaster-recovery-statistics

#9 *Avoid Complexity* Where You Can

A simple backup solution is more likely to work when it is needed. Rather than choosing one of the many overly complex backup products on the market, it is better to choose a product that has been designed to promote simplicity of operations. A simplified user interface helps to reduce the chances of human error. Likewise, simplicity can sometimes reduce the chances of a failed backup. This is especially true when it comes to using agents. Look for a solution that can scale across an environment of any size without the need for an admin to manually deploy agents for each new workload or to spend time writing automation scripts.

According to TechTarget, agentless backups can simplify licensing while also eliminating the need to maintain the agent software that is installed on hosts.
https://searchdatabackup.techtarget.com/answer/What-are-some-agentless-backup-benefits

#10 Having the Ability to *Restore* Matters

Backup testing is critically important, but time consuming. Some backup tools allow admins to perform automated backup testing, which helps to ensure that backups can be restored if needed.

60% **50%** A recent study found that **60%** of backups are incomplete and **50%** of restores fail.
https://ontech.com/data-backup-statistics

34% **77%** **34%** of companies do not test their tape backups, and **77%** of those who do have found tape back-up failures.
https://www.bostoncomputing.net/consultation/databackup/statistics