

Backup myths vs. reality

11 things every business must know



Introduction

Do you know how important your data truly is? If you have harbored misconceptions and myths about backups, this World Backup Day is the perfect time to bust those myths. Many assume that backup strategies are only necessary for large enterprises or that data loss is a problem that is less likely to impact their organization.

According to a survey conducted by [TrueList](#), data loss can affect businesses of all sizes, whether from hardware failures, cyberattacks, human error, or unforeseen disasters, with up to 94% of businesses failing to recover from severe data loss and only 50% testing their disaster recovery plans annually.

In this e-book, we will debunk a few common backup myths and reveal the key principles of a robust data protection strategy.

1. MYTH

Backups are only necessary for large businesses



REALITY

Organizations of all sizes face data loss, and small businesses are at a greater risk due to their limited financial and technical resources. According to [TrueList](#), "almost 70% of small businesses close within a year of a large data loss." Implementing consistent backups is crucial for all organizations to safeguard data and meet regulatory requirements.

2. MYTH

The probability of data loss is low, and I'm statistically unlikely to experience it.



REALITY

Data loss is more common than many assume. Even if the odds seem low, factors like hardware failure, software glitches, cyberattacks, natural disasters, or human error make data loss a constant risk.

3. MYTH

Having one backup copy is enough.



REALITY

Relying on a single backup copy can be unreliable in the event of a single point of failure. The 3-2-1 backup rule suggests having three copies of your data, two local copies in different storage locations, and one offsite backup.

4. MYTH

Backup solutions are too expensive.



REALITY

The notion that backup solutions are expensive is a fallacy, as many affordable options exist. Many backup solutions offer exceptional backup and recovery capabilities with flexible pricing models that allow businesses to customize their plans to fit any budget.

5. MYTH

Daily full backups are the only reliable way to ensure complete data protection.



REALITY

Modern backup solutions save time and storage by using incremental backups and continuous data protection to capture only changes, while adjusting backup frequency based on data importance, ensuring fast recovery and an optimized recovery time objective.

6. MYTH

External hard drives are a foolproof backup solution.

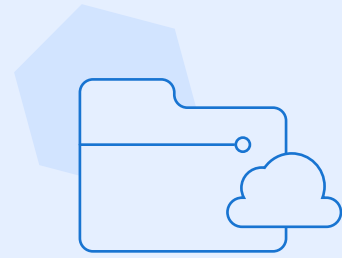


REALITY

Hard drives can fail, can get lost or be stolen, and should not be the sole backup method. According to [Secure Data Recovery](#), hard drives can fail in under three years, often accumulating over 1,500 bad sectors before crashing. Hard drives should be part of a larger backup strategy that includes offsite or cloud backups with automatic scheduling to backup critical data at regular intervals.

7. MYTH

My data is in the cloud;
it is automatically backed
up and protected.



REALITY

Cloud storage can be affected by outages, ransomware attacks, or even account compromise. [Expel's Annual Threat Report 2025](#) found a 72% rise in cloud infrastructure incidents. Having a local backup adds an extra layer of protection against data loss.

8. MYTH

Once a backup system
is set up, it doesn't
require monitoring.

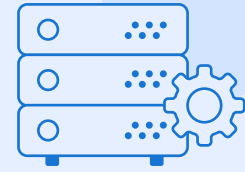


REALITY

Backups require constant monitoring, not just an initial setup. Failures, data changes, and security threats necessitate ongoing checks for successful backup and recovery strategies to align with recovery point objective and recovery time objective values. However, research from [Avasant](#) reveals only 25% of businesses test their disaster recovery plans annually.

9. MYTH

Backup is the same as disaster recovery.

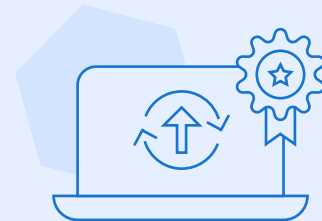


REALITY

Taking a backup is the process of making a copy of your data, while disaster recovery involves a comprehensive plan to back up and restore data to have the lowest possible recovery time objective and ensure business continuity.

10. MYTH

Free backup solutions are as reliable as premium solutions.

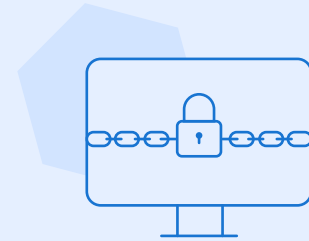


REALITY

While free backup solutions may seem sufficient, they often lack advanced features like incremental backups, granular recovery, automation, and encryption, making data restoration slower and less flexible.

11. MYTH

Backups are safe from ransomware attacks



REALITY

Ransomware can encrypt all organization data, including backups, making recovery impossible. Storing backups in immutable repositories ensures backups stay secure and unaltered.

Don't fall for common backup myths—invest in a diversified and reliable backup and recovery solution like RecoveryManager Plus to ensure your resilience against any disaster. This web-based platform delivers a unified console for managing a wide range of applications like Active Directory, Entra ID, Microsoft 365, Exchange, Google Workspace, or Zoho WorkDrive environments. RecoveryManager Plus provides comprehensive backup capabilities, granular recovery options, minimal administrative overhead, and multiple storage options, ensuring comprehensive data protection.



ManageEngine RecoveryManager Plus

Our Products

AD360 | Log360 | ADManager Plus | ADAudit Plus

ADSelfService Plus | M365 Manager Plus

About RecoveryManager Plus

ManageEngine RecoveryManager Plus is a comprehensive backup and recovery solution for Active Directory, Entra ID, Microsoft 365, Google Workspace, on-premises Exchange and Zoho WorkDrive environments. With its incremental backups, flexible retention policies, backup immutability and multiple modes of restoration—such as domain controller recovery and object-, item- and attribute-level restoration—RecoveryManager Plus delivers a holistic solution for ensuring seamless business continuity by backing up all enterprise application data.

For more information, visit www.manageengine.com/ad-recovery-manager.

\$ Get Quote

⬇ Download

