Cubbit

Backup in 2024:
7 best practices for MSPs/IT managers

Table of contents

Introduction

Unstructured data will be facing massive growth in the years to come. In today's digital landscape, data has emerged as a basis of organisational operations, with its production far from reducing.

This underscores the urgency for robust backup solutions and emphasises challenges in data storage management. Organisations across the world are then confronting a rocketing number of data-related challenges: cyber threats, compliance understanding, data sovereignty complications, and more.

This rapid proliferation of data brings inherent risks, as evidenced by numerous significant incidents in recent years. From high-profile disruptions such as the Amazon cloud glitch impacting access to sites like McDonald's and Delta Airlines (Washington Post), to the global ransomware attacks of early 2023 rendering thousands of web pages inaccessible (TechCrunch), the vulnerabilities are stark.

Cyberthreats' landscape never stops evolving and growing in complexity. Ransomware now targets every kind of infrastructure, whether client-side or server-side, understanding any vulnerability and attacking with unequalled smartness and precision. On the one hand, ransomwares appear to be the most feared and worst type of cyber attack for companies. On the other hand, regional disasters provoked by natural hazards and physical calamities like fires in data centres are growing in numbers.

Many efforts are being put by cloud providers to comply with European digital regulations (GDPR, NIS2, ISO 27001) in order to adapt to a complex and evolving landscape. Data sovereignty is at the forefront of cybersecurity concerns, the location of data being a major question as jurisdictions differ from one region or country to another.

Whether aimed at mitigating data loss, ensuring operational continuity, or complying with regulatory directives, a robust backup plan is indispensable. Like an insurance policy, it must function as a safety net in times of system failures, providing resilience against a series of threats such as ransomware attacks, natural catastrophes, and human errors.

Our guide aims to address the above-mentioned challenges, providing a comprehensive overview of best practices and strategies to empower informed decision-making in the realm of backup strategy.

Is the 3-2-1 backup rule still valid?

1. The 3-2-1 backup rule in a nutshell

The 3-2-1 backup rule was coined by US photographer Peter Krogh and largely recommended by storage industry leaders. Today, it remains an essential rule to ensure reasonable protection against any type of data disaster, especially localised disasters.

Here is how it works precisely:

1. Make 3 copies of your data.
2. Keep them on at least 2 different media.
3. Finally, save 1 copy off-site.

Essentially, the 3-2-1 backup rule ensures data safety by avoiding single points of failure and enhancing data availability. Yet, modern trends and considerations prompt a more sophisticated approach to adapt to the complexity of the cyber threats environment.

In the context of ransomware protection, having at least one offline, air-gapped, or immutable copy of data is vital. Also, regular recovery testing guarantees error-free backups, ensuring data readiness for restoration when needed. The 3-2-1-1-0 backup rule we'll discuss in the next section considers these two elements crucial.

While the 3-2-1 Backup Rule remains a fundamental framework, its application has evolved to meet the demands of modern technology and data protection needs. By embracing these advancements, organisations can ensure that their data remains secure, resilient, and readily recoverable in the face of disruption.

Veeam has updated this excellent rule of thumb by suggesting the 3-2-1-1-0 backup rule, detailed in the next section.

Let's now consider two updated versions of the 3-2-1 backup rule.

2. The 3-2-1 backup rule updated: 2 key strategies to consider

Backup rules are constantly evolving and growing more robust due to fearsome and dangerous cyberattacks and regional disasters leading to downtime and sometimes business closure.

a. 3-2-1-1-0 Backup Strategy

Ideated by Veeam, the 3-2-1-1-0 backup rule is an upgrade to the 3-2-1 backup rule.

The goal is double: on the one hand, tackling the ransomware attacks by having an air-gapped, immutable, or offline copy of the data. On the other hand, it stresses the importance of validating backups and recovery procedures. The additional 1 and 0 stand for:

1: Store the off-site copy offline, air-gapped or on immutable storage.
0: Backups and recovery should be checked daily, so that we count 0 errors.

Here is the detailed procedure:

- Maintain at least three copies of data.
- Store data on at least two different types of storage media.
- Keep one copy of the backups in an off-site location.
- Keep one copy offline, air-gapped or on immutable storage.
- Check and test backups and recovery on a daily level to fix errors quickly.

Implementing an offline (or air-gapped) copy using methods like tape backups stored off-site or cloud backups with immutability and object lock strengthens data security by protecting sensitive information from ransomware threats.

To maintain the integrity of these backups, rigorous practices such as continuous monitoring, error correction, and regular restoration tests are essential. Zero-error storage is even more important. Despite a highly secure backup, any business can potentially be a ransomware's target or victim of natural disasters. A test procedure is necessary to avoid the loss of confidential and fundamental data.

b. 4-3-2 Backup Strategy

The 4-3-2 backup plan offers a robust approach to data protection and recovery. Creating multiple copies stored across diverse locations and mediums shields against threats like cyber attacks and hardware failures. This strategy emphasises regular backups and verification, ensuring data integrity and readiness for any contingency. In an ever-changing digital landscape, the 4-3-2 backup plan provides a vital safeguard for organisational resilience and continuity.

Here is the method procedure:

- Maintain four copies of your data.
- Store your data in multiple locations.
- Two copies are stored off-site, on separate networks.

By maintaining multiple copies of data and distributing backups geographically, redundancy and protection against disasters are ensured. However, depending on the business's needs in terms of backup and considering the importance of data, the number of locations should vary. **The question of costs** then becomes at the heart of the process of choosing the right backup plan and service — indeed, with traditional services you pay for the storage occupied by every single copy of data.

Considering the digital threats ecosystem, today's most performant backup strategies focus on redundancy and off-site storage laying stress on geographic distribution and network isolation to enhance data security.

In the next section, we will put forward the most trusted and considered practices that emerged from conversations with various IT professionals.

7 backup best practices for MSPs/IT managers

In today's ever-evolving digital landscape, safeguarding data is paramount. From selecting the optimal storage repository to minimising attackable surfaces, we'll explore seven key strategies to ensure your backup infrastructure is resilient, efficient, and ready to face any challenge. Let's delve into the core principles that will help you fortify your data protection strategy and mitigate risks effectively.

#1 Find the right S3 storage repository for your needs

Start by selecting the appropriate storage solution that meets your specific requirements depending on the industry you're operating in and business needs.

Several key points are then to be considered to assure an adequate storage environment for an ultimate backup plan and adapt to an evolving cyber threat and disasters landscape:

- **Disaster recovery capabilities:** when it comes to second or third-line backups, resilience and reliability carry more weight than performance. You're investing in an insurance policy for your data here.

- **Durability and availability:** stick to some crucial metrics (11 nines for durability and 99.95% for availability, at least). Consider also the presence of some useful APIs such as object lock and versioning for ransomware protection and thoughtfully consider services that demand bucket replication fees.

- **Digital sovereignty and compliance:** any company, from ICT to manufacturing, is subject to legal scrutiny as it is increasingly necessary to adopt solutions that comply with the major data management regulations and standards, such as GDPR, ISO 27001, and ACN (formerly AgID). In case of non compliance, hefty fines are imposed, often leading to the company's closure. Adopting a solution that allows for data localisation and geo-fencing within the nation boundaries ensures compliance with regional regulations and data control.

- **Interoperability via S3 compatibility** emerges as crucial for seamless integration across multiple cloud and on-prem storage platforms, facilitating intuitive compatibility with the clients and tools you're already using. It is essential that the storage solution you choose adopts the S3 standard, thus avoiding manual operations that require a significant investment of time and attention and are prone to high error rates.

- **Reactive and native-lang customer support:** from various reports by IT professionals, it is increasingly clear how crucial it is to have a team with expertise in the field, capable of dedicating time to listening and responding quickly and in the customer's language.

- **Upload performance:** it's crucial to be able to upload critical data within a reasonable timeframe, even with fibre constraints.

- **Cost voices:** ensure a predictable budget and ROI by avoiding services that charge egress, deletion, and bucket replication fees.

#2 Check bandwidth availability by putting the system under stress during testing

Following conversations with hundreds of European IT managers and MSPs, it emerges that ransomware is not the only challenge. Indeed, it's also very important to recover data within a reasonable timeframe, even with fibre constraints.

Companies need to back up and restore data in a reasonable amount of time (upload performance). Suppose, for example, that the available bandwidth is 100 MB (e.g., your company's headquarters is in an area not covered by fibre). During the day, the company already saturates it at about 50%. If, on the other hand, we use 100% of our bandwidth at night for backups, antitheft and other systems will be unavailable due to internet saturation. That is why, in addition to regularly performing backup tests, it is critical to know in advance what is the maximum bandwidth you can use for recovery and how long it takes to restore business continuity after a disaster.

This problem can be solved with a little-used (but extremely efficient) Veeam capability: the **Veeam forever forward incremental backup**. This strategy has two advantages:
1. It reduces file sizes through deduplication technology.
2. It only patches/updates the full backup you performed in the first phase.

This way, when it comes time to recover ransomware data, you will only have to restore the initial backup (instead of hundreds of incremental backups), which you can do in a reasonable time.

Check out the demo to learn how you can set up a secure, high-performance cloud backup with Veeam and Cubbit.

#3 Backup cost predictability for budget and ROI

Review the cost structure of your chosen storage solution to ensure that backup costs are predictable and align with your budgetary constraints.

Budget predictability is paramount for the stability and longevity of businesses, as well as for the effective operation of public sector entities. In an increasingly digital world, where the threat of cyberattacks looms large, organisations must allocate sufficient resources to safeguard their data and systems.

This predictability extends to the realm of cloud storage services, where Managed Service Providers (MSPs) rely on stable pricing structures to effectively resell storage solutions to their clients and easily predict their ROI. Moreover, in the public sector, access to public funds often hinges on clear budget forecasts, making predictability not just desirable but essential for efficient data management.

Ultimately, by avoiding surprises on the invoice and maintaining a steady financial trajectory, businesses and public entities can safeguard their operations and ensure long-term viability.

a. Key factors in S3 storage cost consideration

When evaluating S3 storage costs, several crucial factors come into play, impacting budget predictability and overall expenditure. Understanding these cost voices is essential for effective financial planning and decision-making in cloud storage utilisation.

1. **S3 basic storage cost:** Cloud providers offer storage tiers with varying cost, performance, and availability levels. Some pricing structures require careful assessment to optimise cost and performance based on specific storage needs.

2. **Egress Fees:** One significant cost consideration is egress fees, which apply every time data is downloaded. Some hyperscalers impose extra fees which poses challenges for budget predictability, especially in case of disasters and subsequent expenses related to recovery processes.

3. **Deletion Fees:** Managed Service Providers (MSPs) encounter challenges in offering free trials due to deletion fees. For example, some cloud providers charge MSPs a 'penalty' for file deletions. This unpredictability hampers budget planning and poses obstacles to offering predictable free trials, since if MSP’s prospects don’t convert into customers, the MSP will have to pay a penalty for every deleted file.

4. **Bucket replication fees:** replication fees are part of hidden costs that can obstruct budget predictability. Indeed, most of the major cloud storage providers offer ‘basic redundancy’ within a few centralised data centres, yet if you want to store data in multiple places (e.g., across more than one city), you have to multiply the costs — just to ensure the market standard for durability levels.

5. **API calls:** These are among the most hidden costs on the list of hidden fees. All the major clients open a lot of API calls to check that the system is working well, but it may happen that one backup client might check every single object you’ve uploaded to the system to ensure that they are correctly listed or protected by object lock. The cost is minimal, but the number of these operations is in the order of thousands, which might result in large fees asked by the cloud storage provider you might use.

#4 Review and update storage policies

Regularly review and update your storage policies to ensure that they reflect your organisation's evolving needs and compliance requirements.

As ransomware continues to evolve and grow in sophistication, it has become capable of not only encrypting data but also deleting and exfiltrating critical backups, both client-side and server-side. This highlights the growing importance of closely monitoring backup policies. One crucial measure is implementing a policy based on immutability. Leveraging the object lock feature, immutable storage empowers users to safeguard selected data by setting an expiration date. During this period, neither cyber attackers, ransomware, nor the service provider can delete, encrypt, or modify the protected data. On the other hand, geographical resilience is also important to avoid critical damages in case of server attacks.

But ransomware is not the only challenge. In an evolving threat landscape, we are witnessing an uptick in regional and natural disasters (data centre fires, earthquakes, etc.), affecting service continuity.

Here are 8 best practices your company should follow:

1. Verify and test your backups daily.
2. Ensure endpoint protection on backups and servers.
3. Always verify that you are using a versioned backup.
4. Maintain multiple recovery points with backup copy jobs.
5. Use immutable storage as a solution for ransomware resilience.
6. Adopt a WORM (“write once, read many”) strategy.
7. Apply Veeam’s 3-2-1-1-0 backup rule with more than one immutable storage.
8. Ensure that your data is protected by strong client-side encryption.

#5 Apply Veeam’s 3-2-1-1-0 backup rule

In the previous section, we presented in detail Veeam’s 3-2-1-0-0 backup rule and why it is a very recommended backup strategy standard.

There are several fundamental elements to take into consideration when implementing a backup plan — among them having an immutable copy and proceeding to daily backup and recovery checks.

First of all, maintaining at least three copies of data is absolutely essential to minimise the risk of losing it entirely by saving them in different places. The storage of data should then be done at least on two different types of storage media: one copy of the backups in an off-site location and one copy offline, on an air-gapped or immutable storage. Finally, daily checks of backup and recovery is a very recommended practice to follow, as it allows us to find errors in advance and fix them as quickly as possible. You never know when the next disaster or ransomware will occur.

#6 Adopt an incident response plan

To deal with potential disasters of all kinds without stress, it is essential for organisations to have a proven ransomware incident response plan ready. Below are the key checklist points that IT managers, CTOs, and developers should consider when creating a ransomware incident response plan:

a. Before the incident
Make sure you have done everything you can to prevent the attack. Follow digital hygiene practices, such as software updates, employee training, and the principle of least privilege. In addition, it is critical to test and verify your full backup (and disaster recovery plan).

To facilitate impact analysis, you can develop a risk assessment framework that considers the likelihood and potential impact of ransomware attacks on your organisation (e.g., downtime, data loss, reputational damage, regulatory fines).

After following the ransomware prevention checklist, you should prepare a ransomware incident response plan. The steps for doing so are outlined below.

First, it is essential to know what to do during a ransomware attack. Then, you need to create a table of roles and responsibilities: from IT to legal communications and crisis management teams. In addition, you need to know who to notify about the breach (e.g., internal teams, external stakeholders, and law enforcement).

Establishing advanced regulatory, insurance, and business policies is critical. Make sure your company's insurance policies cover ransomware incidents and that the terms and conditions of the policy are clear.

Finally, label and protect critical data. This last step helps you define the resources you will need to prioritise for recovery in order to maintain business continuity. In addition, you can mark sensitive resources that need advanced encryption to prevent exfiltration.

b. During the incident
Ransomware is not a matter of "if" but "when." Sometimes the worst happens even though we have followed all the best prevention practices. If your company is under attack or you notice something wrong, you need to act immediately.

First of all: wait to restore your backup! (Otherwise, the attackers will encrypt it again). Instead, you must identify the type of attack, analyse its scope and impact, and isolate it from your devices and network. We have explained all the steps to follow in a dedicated article.

Please note: Make sure that there is always a secure environment and that you can restore systems to bare metal. If this is not possible, consider moving applications to the production environment.

c. After the incident

Even if you have removed the ransomware and restored all critical systems, you need to understand what worked and what didn't. Also, consider implementing tools that allow you to granularly identify the causes of a data breach within minutes. Then, update your disaster recovery plan accordingly.

In conclusion, ransomware attacks are becoming increasingly sophisticated and widespread. Therefore, organisations must be proactive and prepared to handle such incidents. By following the checklist above, you can create an effective ransomware incident response plan that ensures business continuity during a ransomware attack.

#7 Follow digital hygiene best practices

Within a data storage system, attackable surfaces are multiple. Threat actors mainly target backups and servers and often attack weak points along the ‘hierarchy’ like laptops, desktops, tablets, and smartphones. Also, as mentioned previously, human error is part of the origin of cyber attacks. This is why it is essential to stick to fundamental data processing hygiene practices:

1. Train your employees regularly.
2. Minimise the attackable surface by adopting the principle of least privilege, IAM policies, and more.
3. Patch software vulnerabilities.
4. Use layered security.
5. Adopt unique passwords and enable multi-factor authentication.

Conclusion

In the realm of modern business, safeguarding data is paramount. As companies navigate the complexities of digital operations, adopting a robust backup strategy becomes indispensable. By adhering to a comprehensive approach, organisations can fortify their defences against potential threats and maintain uninterrupted operations.

Start by selecting a storage solution tailored to your organisation's needs. This choice should be complemented by sufficient bandwidth to support seamless backup and recovery operations. Ensuring predictability in backup costs and regularly reviewing storage policies are critical steps to maintain financial stability and compliance.

Implementing Veeam’s 3-2-1-1-0 backup rule offers a framework for creating redundant copies of data and diversifying storage locations, ensuring resilience against disasters. Simultaneously, measures to minimise the attackable surface, such as network segmentation and access control, bolster security defences.

Moreover, developing a robust incident response plan is vital. This plan should outline clear procedures for initiating backups and restoring operations swiftly in the event of a security incident or data breach.

By integrating these practices into their backup strategy, businesses can safeguard their valuable data assets and maintain operational continuity, even amidst unforeseen challenges. In doing so, they fortify their resilience and ensure readiness to navigate the evolving landscape of digital threats and opportunities.

In this context, Cubbit emerges as Europe’s 1st geo-distributed cloud storage provider, offering hyper-resilient and sovereign solutions in line with GDPR, NIS2, and ISO 27001 certifications. Cubbit's commitment to data security, encryption, and compliance positions it as a strategic ally for organisations intending to safeguard their data assets in the digital era.

Cubbit

About Cubbit

Cubbit is Europe's 1st geo-distributed cloud storage: hyper-resilient, sovereign, 100% S3 compatible — with no costs for egress, deletion, and redundancy.

Unlike traditional cloud storage, where data is stored in a few centralised data centres, every data saved on Cubbit is encrypted, fragmented, and replicated across multiple geographic locations within a single country or geographic perimeter — safe from ransomware and localised disasters.

The service is compliant with GDPR and **certified ISO 9001** and **ISO/IEC 27001**, **ISO/IEC 2017**, and **ISO/IEC 27018**.

Cubbit supports object lock, versioning, IAM policy, and lifecycle configuration features.

Thanks to its compatibility with S3, Cubbit can be integrated in a few clicks with any S3 compatible stack such as Veeam, Nakivo, and Synology, enabling **immutable** and highly secure **backup** lines.

To date, over 5,000 clients in 70+ countries rely on Cubbit, including partners, institutions, and world-renowned companies like Exclusive Networks (a European leader and cybersecurity distributor listed on the Paris Stock Exchange with $5.45B in revenue) and Leonardo (a global leader in defence and security with $14B in revenue).

If you want to learn more and discover how Cubbit can help protect your company's data and backups, you can activate a free trial with no credit card required. And if you need custom support or consulting on storage and cybersecurity topics, you can book a free 15-minute consultation.

Disclaimer

Please note that the information contained in this guide is provided by Cubbit S.r.l. for general information purposes only and should not be construed as professional advice or opinion. We cannot guarantee that the information is up to date or that it reflects the latest regulatory and cybersecurity developments.
For specific information relating to your business situation, we recommend that you seek professional advice.

Registered Office: Via della Zecca 1 - 40121 - Bologna (BO) - Italy
Shipping & Meeting address: Via Altabella 17 - 40125 - Bologna (BO) - Italy

business@cubbit.io

www.cubbit.io