Backblaze

EBOOK

The Essential Guide to Disaster Recovery Planning

Table of Contents

About Backblaze

Backblaze is the cloud storage innovator delivering a modern alternative to traditional cloud providers. We offer high-performance, secure cloud object storage that customers use to develop applications, manage media, secure backups, build AI workflows, protect from ransomware, and more. Backblaze helps businesses break free from the walled gardens that traditional providers lock customers into, enabling them to use their data in open cloud workflows with the providers they prefer at a fraction of the cost. Headquartered in San Mateo, CA, Backblaze (NASDAQ: BLZE) was founded in 2007 and serves over 500,000 customers in 175 countries around the world. For more information, please go to www.backblaze.com

Introduction

Disaster recovery planning is not just for enterprise organizations. Every company faces the challenge of managing and protecting their data. Ransomware attacks, natural disasters, technical glitches, and all forms of data disasters can have a significant impact on a business's operations, finances, and reputation. We hear about attacks on well-known companies all the time, but small and medium sized businesses are not immune. Veeam's 2023 Data Protection Trends Report found that 85% of attacks targeted SMBs, and 75% of those businesses couldn't continue operating after an attack.

A well-crafted data protection and disaster recovery (DR) plan is essential for every size of business. By implementing a comprehensive DR strategy, organizations can ensure business continuity, faster and more efficient recovery, and clear communication for all stakeholders. This guide will help you understand the proactive steps you can start taking today to develop and test a robust DR plan that protects your critical data and ensures secure, affordable business continuity and resilience in the face of the unexpected.

The high price of data breaches

In 2023, a major cyberattack on MGM Resorts made the national news. MGM Resorts owns several well-known properties in Las Vegas, including the Bellagio, Mandalay Bay, and the Cosmopolitan. A ransomware gang breached MGM's systems, resulting in customers locked out of their hotel rooms, broken games in casinos, malfunctioning ATMs, and more. It's believed the bad actors were able to infiltrate the resort through a social engineering attack. The total cost of the attack is unknown, but the company did take a $100 million hit to their Q3 2023 results.

Source →

Top 10 Data and Disaster Recovery Mistakes

Here are 10 critical errors that can undermine your DR plan.

By avoiding these mistakes and implementing a comprehensive DR plan, businesses can ensure a rapid and efficient recovery from unforeseen disruptions.

1

Proximity paradox

A geographically close DR site offers limited protection. A natural disaster impacting your primary location could easily disable the nearby DR facility as well. And, if you don't have a DR site, this could still apply to your business if you keep your backups nearby, such as in a tape storage facility down the road.

2

Replication trap

Relying solely on replication for DR creates a single point of failure. If your primary site is compromised, the replicated data at the DR site might be compromised as well. Off-site full and incremental backups are essential.

3

Untested backups

Backups that haven't been restored and verified are unreliable. Regularly test your backups to ensure a smooth recovery process during a disaster.

4

Paper plan peril

A DR plan gathering dust on a shelf is useless. Conduct regular drills to simulate disaster scenarios and expose weaknesses in your plan.

5

Snapshot snafu

Snapshots are not comprehensive backups. Using snapshots for long-term storage and retention introduces both technical and compliance risks with how snapshots are managed. This affects both cloud and on-premises platforms.

6

SaaS surprises

Software as a service (SaaS) services like Microsoft 365 and Google Workspace focus on high availability, but have limited built-in protection and recovery options. You may not be managing servers, but you do need a comprehensive data protection plan including regular, incremental backups outside of the SaaS platform.

Object Lock

Object Lock is the feature in cloud platforms that enables immutability. With immutability, your data cannot be changed, deleted, or encrypted. This is the ultimate protection against ransomware.

Backblaze B2 Cloud Storage Object Lock can be configured in either governance or compliance mode, or with a legal hold. This extra layer of protection safeguards backups from ransomware attacks and can also be used to meet compliance requirements.

Be aware that some storage providers charge for PUT calls, so if you ever need to renew an Object Lock on a file (for instance, if your lock expires every 90 days), you may get charged for that call. Backblaze does not charge for PUT calls so you can renew your object locks as needed—without additional fees.

Learn More

7 Unforeseen force majeure

Disasters come in all shapes and sizes. Don't limit your DR plan to common IT disruptions. Consider scenarios like widespread power outages or communication breakdowns, and plan accordingly.

8 Backup infiltration

Bad actors are increasingly targeting backups to increase the chances of a payout. Utilize immutable backups, unchangeable after creation, for an extra layer of protection against ransomware attacks.

9 Cloud drive disasters

Storing data on Google Drive, Dropbox, OneDrive, etc. is incredibly common. But these platforms do not protect against ransomware and provide limited point-in-time recovery options. Cloud drives are not a sufficient backup of your data.

10 Overlooking compliance

Factor in compliance needs when building your data protection and DR strategy. Regulations like HIPAA, GDPR, and others may have security or archival requirements that should be considered in your plan.

Navigating Backup and Archive Infrastructure

Aging infrastructure, strained budgets, and exponential data growth create unique challenges for disaster recovery planning. While assessing your storage landscape, you must consider data governance or sovereignty requirements, compliance requirements, and the needs of your end users. Many legacy data storage systems can create gaps in an otherwise airtight DR plan.

On-premises legacy

Traditionally, businesses have relied heavily on on-premises backup solutions. Robust storage systems hold critical data, often backed up to secondary storage within the same physical location. While this approach offers a sense of control, it also presents vulnerabilities.

On-premises backups are at risk of localized events like loss of power, fire, flooding, or other natural disasters. A geographically separate DR site or other far off-site backup is essential for complete protection and compliance. Without this, the organization risks losing critical data in cases of a regional outage or loss of access.

The shift to public cloud and SaaS options opened the door to more secure and reliable data backup and disaster recovery solutions. By utilizing cloud-based storage and backup services, organizations can ensure that their data is protected in multiple locations, reducing the risk of data loss due to localized disasters. Additionally, cloud-based solutions offer scalability and flexibility, allowing organizations to easily expand their storage capacity as needed.

DR site limitations

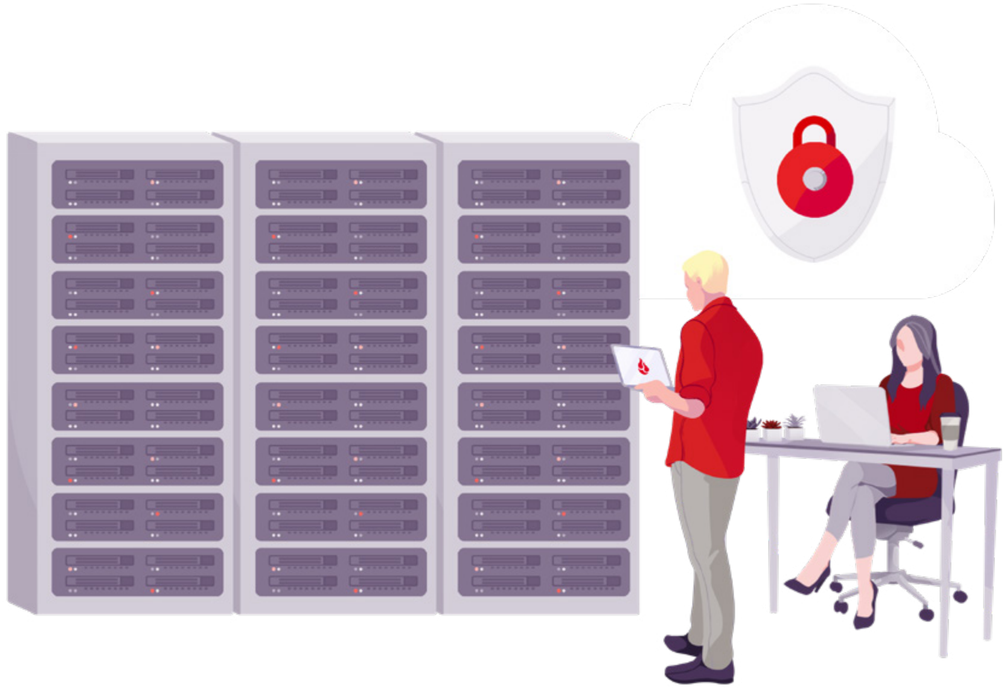
Many businesses have established alternate data centers as a secondary backup layer. However, since these sites frequently only use replication technology, a malware attack on the primary site could result in total data loss. This situation can result in a scenario known as the “replication trap.” There is a risk that data compromised by malware is replicated to the DR site, leading to potential data loss.

Off-site, immutable backups, independent of the primary site’s data, are a key component of a robust DR strategy. In cases of malware attacks or accidental data deletion by users, off-site immutable backups allow for data retrieval from a backup saved prior to the incident and reduce possible interruptions.

Despite being viewed as a legacy technology, tape backups continue to be used in some organizations due to their reliability and cost-effectiveness. It is common to store tapes in a separate location to diversify data storage geographically, which helps reduce the impact of local disasters on data access and enhances overall data resilience.

Off-site tape backups may increase recoverability but create challenges with recovery time objectives (RTO) because of the increased time it takes to retrieve data from a separate location and using tape technology. Hardware issues can happen often, and unexpectedly. Cloud-based data storage and archiving has gained popularity because of higher availability and cost savings over traditional tape backups.

The cost and time required to operate multiple data centers and recovery times should also be considered in the requirements for your production and DR infrastructure. Never underestimate the risk to a successful recovery when facing time-consuming tasks like physical site recovery and data restoration from tape.



CASE STUDY: ACENTEK

Telco Adopts Cloud for Resilience and Cyber Insurance Requirement

1
Cyber Insurance Policy Secured

300
Virtual Machines Backed Up

1 hr
Set Up Time

Learn More

> Adding Backblaze to our infrastructure allowed us to satisfy our insurance carrier's requirements. We could prove that we're maintaining immutable backups on third-party servers located across the country that comply with industry standards for data security.

Chris Hoiland, IT/Data Center Supervisor, AcenTek

Cloud services: A double-edged sword

Cloud-based collaboration and communication tools are commonly used by businesses and yet are often left vulnerable to data loss. Cloud services do not provide sufficient protection and recovery options that organizations likely need.

Many businesses leverage cloud services like Google Drive and Microsoft 365 for collaboration and document storage. However, businesses often find that the responsibility for backing up this data falls on their own IT, as these services typically don't offer comprehensive backup solutions.

To ensure a reliable DR plan that includes cloud services, you should:

- Evaluate granular recovery requirements for productivity platforms like Google Workspace and Microsoft 365.
- Evaluate adherence to your long-term backup retention policy keeping in mind the regulations that your business might be subject to.
- Determine if data stored in cloud platforms needs to be backed up with immutability due to cyber insurance requirements or other security policies.
- Examine best practices for comprehensive, secure data protection for shared cloud drive services and SaaS productivity tools to address the lack of built-in recovery features.
- Plan to store true backups of your SaaS data just as you would for any other data. It may seem redundant to back up cloud platforms to the public cloud, but doing so ensures that you have the right point-in-time backups you need and you can recover *on your timeline—not Google or Microsoft's*.

Cloud costs will need to factor into decisions for where to store your data. Cloud storage costs should be included as a non-functional requirement to make sure you can achieve your secure recovery goals without sacrificing affordability.

Cloud-based DR and backup

Many businesses have adopted cloud-based DR and backup solutions to augment their existing on-premises backups. Moving to cloud-based DR and backup options promises to be affordable, secure, and malware-resistant. A cloud-based strategy can also unlock scalability and more flexible location options.

Using cloud data storage for production, backups, and archive can lead to some price shock as your environment scales. Look for a cloud storage provider that provides the level of security you need at an affordable price. Using the same cloud service provider (CSP) for your backups as for your production data may not be necessary, as you don't need the same level of performance for backup data.

You need to weigh your cloud-based options to evaluate platform compatibility, ongoing costs, and whether your CSP locks you in or out of specific ecosystems due to high storage costs, data transfer costs, and proprietary features.

Many on-premises data protection tools also support cloud targets for backup storage. It's important to match the capabilities of your current backup vendors to your recovery requirements and cloud storage budgets.

Carefully read the fine print when considering cloud storage costs. Hidden fees, minimum retention requirements, and complicated pricing tiers make accurate forecasting difficult and could leave you paying for unused storage just to reach certain discount tiers.

Moving data to lower cost storage tiers or cold storage may achieve price reductions, but it often comes at the cost of recovery speed and added complexity. Look for a cloud storage provider with transparent pricing that makes it easier to plan your costs.

Better understand the three dimensions of cloud costs

Learn more about what to watch out for with regards to cloud storage pricing in this white paper, "The Cost of Cloud Storage."

Get White Paper

Hot, warm, and cold DR sites: Choosing the right strategy based on budget, risk tolerance, and recovery time objectives

Traditionally, DR for large-scale organizations would involve building a physical site to support RTO objectives. It's important to note that building or buying a dedicated DR site might not be the most cost-effective option for all backups. Instead, cloud storage offers a compelling solution specifically for backups. Cloud storage is generally more affordable and scalable than on-premises storage solutions, making it a great fit for this purpose.

Recovery sites are often referred to by temperature (hot, warm, cold) to describe the speed and importance of applications and data in those protected sites. The ideal DR site temperature (see table) depends on your organization's budget, risk tolerance, and RTOs. Businesses with critical systems requiring near-instantaneous recovery might opt for a hot site. Others might find a warm site or even a cold site a more cost-effective option for less time-sensitive systems.

Hot, warm, and cold: choosing the right DR site temperature

Hot site	Warm site	Cold site
A fully functional replica of your primary production resources, constantly maintained and ready for immediate failover in the cloud or to a secondary on-premises site.	A pre-configured cloud recovery site or hybrid recovery with hardware and software infrastructure. Requires some manual intervention (e.g., software installation) before becoming operational.	A basic physical facility with essential infrastructure (power, cooling, and network connectivity) requiring significant configuration and installation before use. May also include lower cost cloud storage.
Pros Fastest recovery times due to the site's constant readiness.	**Pros** A balance between cost and recovery time. Faster than cold sites, but slower than hot sites.	**Pros** Most cost-effective option, requiring minimal ongoing maintenance.
Cons This is the most expensive option due to the need for complete infrastructure replication.	**Cons** Still require some manual setup, potentially delaying recovery time.	**Cons** Longest recovery times due to the extensive configuration and installation needed.
Example RTO goal times		
RTO <15 minutes	RTO <24 hours	RTO >24 hours

Your DR Strategy: Building A Fortress for Your Data

DR planning is a collaborative effort, not a solo act for the IT department. A comprehensive DR strategy requires input and participation from various stakeholders across the organization. This section delves into the key components of a robust DR plan for businesses.

Stages of a DR strategy: From prevention to recovery

Comprehensive DR requires a multi-tiered approach. Your DR strategy should encompass four critical stages: prevention, preparation, mitigation, and recovery.

Prevention

This stage focuses on implementing proactive measures to fortify defenses against disasters. Examples include implementing robust security protocols, user awareness training, and regular vulnerability assessments.

Preparation

Preparation involves developing a detailed DR plan that outlines roles, responsibilities, and procedures for responding to various disaster scenarios. Regular testing and drills ensure the plan's effectiveness.

Mitigation

During a disaster, immediate and decisive mitigation efforts are necessary to swiftly limit the damage and prevent escalating disruptions. This might involve isolating the affected systems, activating backups, and communicating with stakeholders.

Recovery

The recovery stage focuses on restoring critical systems and data to normal functionality as quickly as possible. This involves implementing the pre-defined steps outlined in the DR plan and ensuring a smooth transition back to normal operations.

Are there best practices for DR?

Absolutely! These 12 key considerations will help IT teams when developing and reviewing a disaster recovery plan.

1 Leave no disaster unidentified

The first step in building a strong DR plan is to identify all potential threats, not just major disasters. Consider "minor" threats like human error or hardware failures that could disrupt security and operations.

2 Plan for the worst (and beyond)

While it's important to plan for likely threats like ransomware attacks, don't neglect worst-case scenarios. Develop a plan that can handle a catastrophic event like a natural disaster wiping out your primary site or a widespread communication outage.

3 Ransomware: Your uninvited guest

Ransomware attacks are a major threat. Dedicate a significant portion of your DR plan to addressing ransomware scenarios, including recovery procedures and strategies to minimize the impact of such attacks.

4 Beyond the walls: Cloud catastrophe

Extend your DR plan beyond on-premises threats to include potential disruptions associated with cloud services, such as outages or security breaches. Multi-cloud and hybrid disaster recovery options help reduce the risk of rare, but highly impactful outages. Cloud provider service level agreements (SLAs) define availability targets (e.g., 99.9% uptime) which can increase your overall data and application availability above on-premises capabilities.

5 Infrastructure independence

Always anticipate potential infrastructure unavailability during a disaster. Plan alternative methods for accessing critical data and systems, including leveraging cloud infrastructure as a service (IaaS) solutions as a backup.

6 Think beyond data recovery

A robust DR plan goes beyond just recovering data. It should outline procedures for rebuilding your entire IT environment, including applications, configurations, security, and user accounts.

Additionally, make sure to regularly test and update your DR plan to ensure it remains effective and up to date. By leveraging affordable, secure, cloud-based backup and archive as part of your overall disaster recovery strategy, you can better protect your critical data. The result will minimize downtime, risk, and unexpected costs in the face of unexpected events.

7 Plan variations

Develop different versions of your DR plan based on the severity of the incident. This allows for a more targeted response, depending on the specific nature of the disruption.

8 Run books: Your DR roadmap

Consider creating predefined "runbooks" that outline specific steps for various disaster scenarios. These detailed documents provide clear instructions for IT staff during a crisis.

9 Recovery is the finish line, not the starting point

Modern DR strategies prioritize planning for recovery from the beginning. Verify the usability of your backups and recovered data to ensure their effectiveness during a crisis. Test your restoration procedures regularly to avoid the pitfall of unusable backups during a disaster.

10 Securing resources in advance

Don't wait for disaster to strike before securing necessary resources. Budgetary approvals, software licenses, and hardware procurement should all be addressed in advance to avoid delays during a crisis.

11 Cyber insurance considerations

If your business has cyber insurance, familiarize yourself with the DR planning requirements outlined in the policy. Understanding the insurance company's expectations can help you tailor your DR strategy accordingly.

12 Backups are not the whole plan

As cybercriminals become more sophisticated, they often target backups as well. Backups—once a low-priority just-in-case item—are now mission critical. Backups are a critical foundation for your DR plan but they are not the entire plan.

CASE STUDY: LEMKEN

Global Manufacturer Adds Immutable Cloud Storage for Disaster Recovery

30
Global Locations

230
VMs Backed Up

440 TB
Protected

Learn More

> Backblaze made it very simple to go from proof of concept to the full solution. We didn't have to change the configuration or move to a production environment. They just gave us the storage, we moved our data, and that was it.

Ludger Demming, Head of IT Infrastructure, LEMKEN

DR storage destinations and services

Build vs. buy vs. cloud: Finding the right fit

Selecting a DR site is fundamental to your strategy. There are four main approaches to establishing a DR site: building your own, buying services from a co-location provider, buying public cloud storage, or leveraging a disaster recovery as a service (DRaaS) solution. Each approach offers distinct advantages and drawbacks.

Building an on-premises DR site

Pros

It provides complete control over the DR environment, offering greater customization and security.

Cons

Significant upfront investment in hardware, software, and facility infrastructure and management. Requires ongoing maintenance and staffing costs. Limited scalability to accommodate future growth.

Buying public cloud-based DR storage

Pros

Highly scalable and cost-effective. CSPs manage the physical infrastructure, reducing your IT team's workload. Features like Object Lock help address security concerns versus on-premises storage.

Cons

Retrieving large volumes of data may be slow due to bandwidth constraints.

Buying co-located DR storage

Pros

It offers a cost-effective alternative to building your own site. Co-location providers manage aspects of the physical infrastructure, reducing your IT team's workload.

Cons

Less control over the environment compared to an on-premises solution. May require additional investment for network connectivity and configuration. Potential vendor lock-in with specific co-location providers.

Buying disaster recovery as a service (DRaaS)

Pros

Highly scalable and cost-effective solution. Eliminates the need for upfront infrastructure investment. DRaaS providers manage the entire DR environment and provide technical support, freeing up your IT staff.

Cons

Reliance on a third-party provider for critical data and infrastructure. Potential concerns over network latency and vendor lock-in. Security considerations require a careful evaluation of the cloud provider's practices.

Why choose DRaaS?

DRaaS offers a compelling option for businesses seeking a cloud-based DR solution. DRaaS providers manage off-site backups, replication, and disaster recovery infrastructure, potentially reducing the burden on your internal IT team.

DRaaS pros include:

- **Cost-effectiveness**

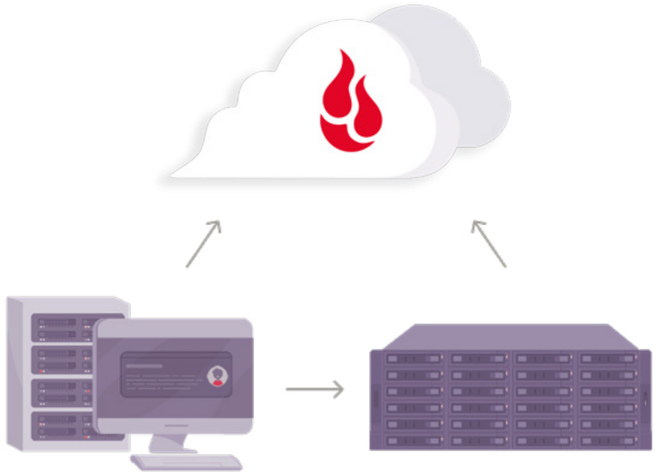
  DRaaS eliminates the upfront cost of purchasing and maintaining dedicated DR infrastructure.
- **Scalability**

  DRaaS solutions can easily scale up or down based on your organization's evolving needs.
- **Expertise**

  DRaaS providers offer the expertise and experience of managing disaster recovery infrastructure.
- **Improved RTOs**

  Geographically dispersed cloud backups can enable faster recovery times in the case of on-premises outages and primary site data loss.

It's important to carefully assess the specific needs and requirements of your organization before selecting a DRaaS provider. Consider factors such as data security, compliance regulations, target compatibility, and the level of support and assistance offered by the provider.



Replication vs. backups: Understanding the nuances

Data replication and data backup are terms that are often used interchangeably, but they are distinct concepts with fundamental differences in a DR context.

Data replication

Involves copying and synchronizing data between your primary site and the DR destination in real-time or near real-time.

Offers fast failover capabilities as the replicated data at the DR site is constantly updated.

However, if malware infects your primary site, it might also replicate to the DR site, rendering the backup compromised.

Data backups

Involves creating full and incremental copies of your data and storing them in a separate location, typically on a scheduled basis.

Incremental backups capture changes in data, thus offering a point-in-time recovery option.

Ideally, backups are immutable to protect against malware and ransomware by making files and images read-only for safe recovery.

Air-gapped and offline backups can further help resist malware and ransomware attacks by creating a virtual or physical separation from the production network.

Cloud-based backups are a great option for addressing these requirements while offering affordable scaling options as the environment grows.

Replicating backups

A hybrid approach involves replicating your backups to a secondary location, offering a balance between data protection and recovery time. This can be between on-premises and cloud environments, or across multiple cloud targets.

While replicating backups offers additional protection and accessibility for online recovery, the backup images are still subject to ransomware infection. Using immutable backups helps prevent the spread of the infection to recovery sites and backup repositories.

Data backups with replication can be an ideal pairing. Full and incremental backups with point-in-time snapshots can provide regular recovery points with replicated copies for remote recovery and additional protection.

Factors to consider when choosing the right approach based on specific needs and recovery requirements

The optimal approach to DR depends on your specific needs.

- For frequently accessed data requiring near-instantaneous recovery, consider a combination of hot site methodology and real-time data replication. This offers the fastest failover, but can come at a higher cost.
- For critical data with acceptable downtime, a warm site with replicated immutable backups at a secondary location (either on-premises or in the cloud) provides a good balance between cost and recovery time. While requiring some manual intervention, it offers protection against malware replicating to the DR site.
- For less critical data or archival purposes, cold storage with periodic backups is a cost-effective option. Backups offer a historical record and are less susceptible to malware infection compared to replicated data, particularly if Object Lock is enabled for immutability.

Data replication is important, but it should not be seen as a substitute for backups. Backups offer a required safety net, providing a point-in-time recovery option even if the replicated data is compromised.

Selecting the right DR strategy depends on a careful evaluation of your business' specific needs, budget, and risk tolerance.

By understanding the pros and cons of each option, you can make an informed decision that ensures optimal protection for your critical data in the face of unforeseen disruptions.

Common DR scenarios and major considerations

A robust DR plan anticipates various disaster scenarios. In this document, we will discuss two common threats: a ransomware attack and a cloud outage.

Scenario 1

Ransomware attack: The looming threat

Ransomware attacks are a major concern for businesses often topping the list of DR planning priorities. These malicious attacks encrypt critical data, making it inaccessible until a ransom is paid, posing a significant threat to operations. Here's what you need to consider in your DR plan for a ransomware attack:

Importance of backups

Backups are your primary defense against ransomware. A comprehensive backup strategy, incorporating frequent backups stored off-site and immutability (unchangeable backups, enabled by the Object Lock feature), helps ensure you have a clean, uninfected copy of your data to restore from.

Correct immutability configuration

Ensure your immutability settings and period are properly enabled. Know that there are different types of immutability, such as compliance mode and Legal Hold. Improperly configured immutability can put your entire backup at risk of corruption.

Rapid restoration

Time is of the essence during a ransomware attack. Your DR plan should outline procedures for swift restoration of critical systems and data from backups. Regularly testing your backup and restore processes is important for minimizing downtime.

User education

Educating employees about ransomware threats and best practices (e.g., not clicking suspicious links, reporting phishing attempts) can significantly reduce the risk of infection.

Network segmentation

Segmenting your network can help prevent ransomware from spreading across your entire IT infrastructure. This limits the damage if a single system becomes infected.

Incident response plan

Develop a well-defined incident response plan outlining steps to take upon the discovery of a ransomware attack.

Cyber insurance requirements

If you have a cyber insurance policy, be aware of your policy requirements for ransomware attacks. For instance, some policies will require you to have immutable backups—not just off-site backups—to better protect from ransomware.

Payout policy

It's never advisable to pay a bad actor; this just fuels the ransomware economy and doesn't ensure you'll get your clean data returned. Moreover, some cyber insurance policies may not allow for ransomware payments, or they may require you to use their own "ransomware negotiator." Check for these clauses in your policy. The best defense is to ensure your backups are recoverable within your necessary RTO so you're not against the wall to issue a payout.

Key focus: Restoring your full environment

The most common type of recovery in a ransomware scenario involves restoring your entire environment, including applications, configurations, and user accounts. This approach ensures a more comprehensive recovery, minimizing data loss and disruption to operations.

Scenario 2

The SaaS risk: When your productivity suite goes awry

SaaS applications like Microsoft 365 and Google Workspace are widely used in business. While these services offer some inherent redundancy, data loss and outages can still disrupt critical operations, largely because they operate on a shared responsibility model.

Backing up SaaS data: A must-have

Organizations should prioritize backing up their M365 and Google Workspace data. Although these platforms offer some built-in redundancy, it is built to protect their own infrastructure—not your data. Your data and applications are cloud-based for easy access, but do not include built-in granular backup and restore features, such as the ability to set retention periods or to choose the types of files being backed up.

A comprehensive backup and protection strategy should include periodic backups with granularity to be able to recover more than just entire mailboxes. Your backup should ideally be able to provide multiple recovery points while optimizing for storage and retention costs.

SaaS backups should also provide immutable recovery points to mitigate against ransomware and malware attacks. Mail and document repositories are popular targets for attackers because of widespread use. A comprehensive data protection and disaster recovery plan for SaaS needs to include planning for retention and managing data lifecycle. Your plan should include both recovery capabilities and the balancing of cost versus amount of copies retained.

Unexpected SaaS recovery challenges

If a widely used application experiences a significant outage, your DR plan should outline alternative communication and collaboration methods to minimize disruption. This might involve utilizing alternative cloud services or leveraging local resources like file servers for temporary document storage. (In this case, the need for endpoint backup becomes even more evident.)

The DR plan should also include procedures for monitoring service provider notifications and keeping the business informed about the outage and estimated restoration times.

By planning for these scenarios, organizations can ensure a faster and more efficient response to disruptions.

The mighty runbook: Your DR lifeline

- ☑ **Authoritative**
  Verified by IT and executive leadership through regular audits and approvals.
- ☑ **Accurate**
  Reflects current systems, procedures, and contact information.
- ☑ **Accessible**
  Easy to navigate, with clear instructions and visuals.
- ☑ **Absorbed**
  Regular training ensures familiarity with the runbook.
- ☑ **Adaptable**
  Can be easily updated to reflect changes in infrastructure or procedures.
- ☑ **Audited**
  Regularly reviewed and tested as part of your DR change control process.

Remember: Your runbook is a living document. Regularly review, update, and test your runbook to ensure its effectiveness in real-world disaster scenarios. This ongoing process is necessary for maintaining a robust and adaptable DR strategy.

Contents of the DR Runbook:

Executive summary

- Briefly outline the purpose of the DR runbook and its role in your disaster recovery strategy.
- Highlight the importance of the runbook in ensuring a swift and coordinated response to data disasters.

Vendor and contact information

- Include a comprehensive list of all relevant vendors and their contact information, categorized by service.
- This might include cloud providers, network providers, hardware vendors, and software support contacts.
- List your cyber insurance provider and their contact details, including any specific claims procedures.

Incident response team

- Provide a clear breakdown of the business' incident response team (IRT) structure.
- List key personnel in the IRT, including roles, responsibilities, and contact information (phone numbers and email addresses).
- Include escalation procedures for contacting additional personnel within the organization during a crisis.

Procedures

This is the heart of your runbook, outlining the step-by-step procedures for various disaster scenarios.

- Organize procedures by scenario. Categorize by ransomware attack, natural disaster, power outage, network outage, cloud outage, etc.
- Clearly define roles and responsibilities. Assign specific tasks to different team members within the IRT for each scenario.
- Outline detailed, step-by-step instructions. Provide clear and concise instructions for each action required during a disaster, including screenshots or visuals where appropriate.
- Set communication protocols. Create communication protocols for the IRT and how they will disseminate information to employees and executive leadership.

Establish key team members, roles, and hierarchy: The backbone of your DR response

A well-defined DR plan relies heavily on a well-coordinated team structure. This section outlines the key roles and reporting hierarchy needed for an effective DR response.

The importance of clear communication

A critical component of any DR plan is clear communication to employees and executives regarding their specific roles during a security incident. This ensures that the assigned team leader can coordinate a unified response. Remember to include guidelines about incident escalation, as well as agreed-upon methods of communication (e.g., email, direct messaging, video calls, etc.).

Executive sponsorship: Beyond awareness

Executive buy-in is paramount for a successful DR strategy. While awareness of the impact of ransomware attacks has grown over the years, contextualizing DR plans with historical financial impacts, downtime implications, and reputational risk associated with such attacks can help to communicate why DR is a top-line priority.

Educating executives: Framing the DR plan in terms of cost avoidance, user downtime minimization, and reputational risk mitigation can resonate better with executives. Quantify the potential financial losses from data breaches and system outages to garner executive support for DR initiatives.

Assembling your incident response team (IRT)

The IRT is the backbone of your DR response and is responsible for leading the recovery efforts during a disaster. Here's a breakdown of possible key IRT roles:

- **Incident commander**
  Oversees the entire incident response process, making critical decisions and delegating tasks to team members.
- **Technical lead**
  Provides technical expertise, directing recovery efforts for IT infrastructure and data restoration.
- **Communications lead**
  Handles external and internal communication, ensuring timely updates for stakeholders and mitigating potential reputational damage.
- **Documentation lead**
  Maintains the DR runbook, ensuring its accuracy and updating it with post-incident findings.
- **Legal counsel**
  Provides legal guidance and ensures compliance with relevant regulations during the response and recovery process.

Building redundancy

Building redundancy in your IRT allows you to account for team member absences. Assign backup personnel for critical roles within the team to ensure continuity in the event of unforeseen circumstances.

Establish a clear succession plan for leadership roles within the IRT. This ensures a smooth transition if the primary incident commander or other key personnel become unavailable during a disaster.

Establishing a reporting hierarchy

Clearly define a reporting hierarchy within the IRT, outlining who reports to whom and the escalation process for making critical decisions. A clear chain of command during a crisis prevents confusion and delays that could result in prolonged downtime and increased risks.

Beyond cell phones: Communication channels

Disasters can disrupt traditional communication methods like cell phone service. Develop alternative communication channels for the IRT, such as designated email threads, satellite phones, or pre-arranged conference call bridges. It is imperative to include this information and contact details in your DR runbook for immediate accessibility during crises.

By establishing a well-defined team structure with clear roles, communication protocols, and redundancy measures, organizations can ensure a coordinated and efficient response to data disasters.

Objectives, priorities, and KPIs: The compass of your DR strategy

A robust DR strategy starts with clearly defined objectives and priorities. These guide your approach and decision-making during a disaster recovery event.

Your strategy should prioritize rapid recovery of critical systems and applications to minimize operational downtime and resume normal functions swiftly.

Prioritization: Not all data (or systems) are created equal

Prioritizing your critical business applications depends on a deep understanding of your business. Collaborate with internal partners to identify critical business applications that are essential for ongoing operations.

Not all applications require immediate restoration. Prioritize systems based on their impact on core business functions.

Documentation is key

A popular mantra for DR specialists is **"Test the plan; don't plan the test."** Your DR plans must be clearly documented as working recipes for application and data recovery, including dependencies and prerequisites.

Document the recovery procedures for each critical application, outlining the steps required to bring them back online. This ensures your IT team can efficiently restore essential services during a disaster.

Primary DR objectives		
Minimize data loss	**Ensure business continuity**	**Optimize costs**
The primary objective is to minimize data loss through regular backups and secure storage practices.	The DR plan aims to rapidly recover operation of critical functions during a disaster, minimizing disruption to the business goals.	Application and data recovery needs to balance speed and costs to ensure recoverability without unnecessarily increasing IT spending.

Compliance considerations

Compliance regulations might influence your DR priorities. Understand any industry-specific regulations or data privacy laws that might dictate specific data protection and recovery timeframes.

Collaborative RTO and RPO setting

Working with internal partners to set RTOs and RPOs ensures alignment across the organization.

- RTO defines the acceptable timeframe for restoring critical applications to a functional state.
- The RPO defines the maximum tolerable amount of data loss acceptable in the event of a disaster.

Stakeholders need to understand the realistic trade-offs involved in setting RTOs and RPOs, balancing the need for quick recovery with resource and cost limitations. Achieving extremely short RTOs, such as recovery within minutes, might require substantial investments in advanced infrastructure, redundant systems, and skilled personnel.

Setting achievable RTOs and RPOs that effectively balance the need for swift recovery with the financial limitations of the organization requires open communication and collaboration.

Restore vs. recovery: Understanding the nuances

It's important to distinguish between data restoration and system recovery. Data restoration specifically involves retrieving data from backups. On the other hand, system recovery encompasses the comprehensive restoration of data, applications, configurations, and user accounts to fully restore system functionality.

Your RTOs should focus on the time it takes to bring an application to a usable state, not just the time to recover the data.

Setting expectations: Transparency is key

Employees might have unrealistic expectations regarding recovery times during a disaster. Educate the organization on the DR process and the inherent complexities involved.

Developing measurable KPIs: Tracking your progress

Key performance indicators (KPIs) are your guiding metric for measuring the effectiveness of your DR strategy. Here are some key DR-related KPIs to consider:

- **RTO achievement rate**
  Tracks the percentage of times critical applications are restored within the established RTO.
- **RPO achievement rate**
  Measures the percentage of data recovered that meets the defined RPO.
- **DR plan testing frequency**
  Monitors how often the DR plan is tested to ensure its effectiveness.
- **Mean time to recovery (MTTR)**
  Tracks the average time taken to recover critical applications after a disaster.
- **Data loss rate**
  Measures the amount of data lost during a disaster compared to the established RPO.

These KPIs provide valuable insights into your DR preparedness and help identify areas for improvement.

Your backup strategy

Let's explore the main components of a strong backup strategy for protecting your organization's critical data. These are essential to a comprehensive DR plan and assist in building the business case to align finances and teams on goals and objectives.

Understanding your data: Importance of location, age, and accessibility

The first step is to gain a comprehensive understanding of your data landscape. This includes documenting:

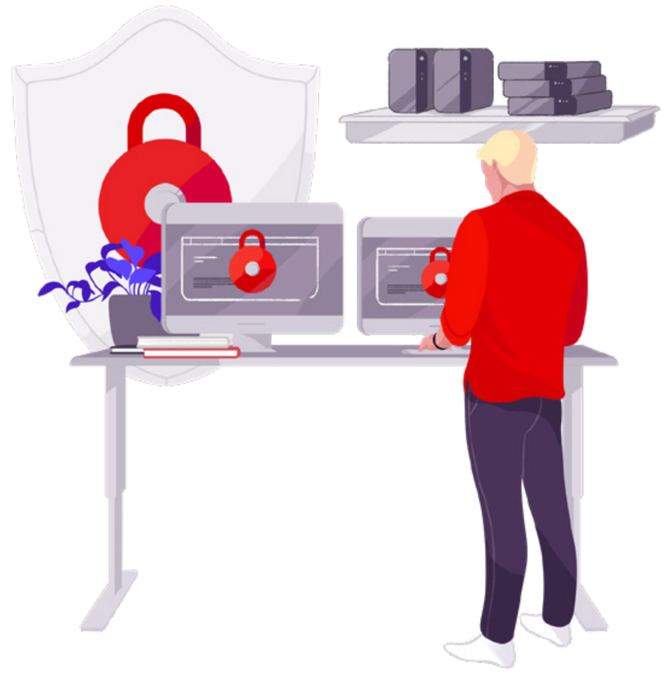
- **Data location**
  Identify where your data resides (e.g., on-premises servers, cloud storage platforms, and user devices).
- **Data age**
  Outline the frequency of your backups and the time period covered by existing backups.
  Note: Regular backups are key.
- **Data accessibility**
  Regularly test your restore processes to guarantee successful data recovery when needed.

For seamless backup strategy execution, your team needs comprehensive knowledge of requirements and backup limitations. This includes understanding the backup location, the access methods for efficient data retrieval and restoration, and the testing procedures to confirm backup integrity and ensure successful restoration in the event of a data loss scenario.

Looking beyond backups: Unveiling the complexity of data protection

It's important to understand that several commonly used data protection techniques are not true backups:

- **Snapshots**
  While snapshots offer a point-in-time view of your data, they are not true backups. While they can be useful for recovering from recent changes or errors, they don't provide historical backups or a comprehensive backup history. Backups, on the other hand, typically store multiple versions of data over time, allowing for recovery from a wider range of scenarios.
- **Replication**
  Data replication involves copying data to a secondary location for disaster recovery purposes. However, replication can also replicate malware, potentially compromising both your primary and secondary data. Backups offer a separate, uninfected copy of your data.
- **SaaS platforms (M365, Google Workspace)**
  Although platforms like M365 and Google Workspace offer storage, they do not promise adequate or complete backups. These platforms have their own backup and retention policies, which might not align with your specific data recovery needs, particularly if there are compliance standards you need to meet.



The 3-2-1 rule: A common standard in data protection

The 3-2-1 backup methodology is a widely accepted best practice for data protection. Cloud storage backup aligns to the 3-2-1 rule and unlocks geographic diversity without the need for physical recovery sites. For complex infrastructure, 3-2-1 is the *bare minimu*m. You should consider maintaining at least one immutable copy of your backup data, and having more than one off-site copy is also advisable.

3 Copies

Maintain at least three copies of your data. This redundancy minimizes the risk of data loss due to hardware failure, cloud site/service failures, or accidental deletion.

2 Media types

Store your backups on at least two different media types (e.g., off-site network attached storage [NAS], Backblaze B2 Cloud Storage, LTO tape, etc.). This offers protection against media-specific failures.

1 Off-site location

Keep at least one copy of your backups stored off-site in a geographically separate location or cloud region. This ensures data protection even in the event of a local disaster that impacts your primary site.

Immutability: Safeguarding against ransomware attacks

Immutable backups are unalterable copies of your data that cannot be modified or deleted.

How immutability mitigates ransomware

- **Ransomware renders primary data inaccessible**
  Ransomware encrypts your primary data, and often your backups as well, making it unusable until you pay a ransom.
- **Immutable backups remain untouched**
  Since immutable backups are unalterable, ransomware cannot encrypt or corrupt them.
- **Faster recovery**
  With readily available, uncorrupted backups, you can quickly restore your data, minimizing downtime and financial losses and avoiding the worst-case scenario—paying a ransom to regain access to your data.

Additional benefits of Immutable backups:

- **Enhanced data security**
  Immutability protects your data from accidental or malicious deletion, providing an extra layer of security.
- **Regulatory compliance**
  Many data security regulations may require organizations to maintain immutable backups for specific periods.

Integrating immutable backups into your DR plan is a powerful defense against ransomware attacks and ensures the integrity of your data in the face of cyber threats.

Enhanced protection for high-value data: Safeguarding critical information

Implement additional safeguards for your most critical data, such as:

- Schedule more frequent backups for systems storing sensitive information like personally identifiable information (PII) or high-profile research data.
- Geographically dispersed backups. Keeping an additional off-site copy in a different geographic location is important for all data—it's how you adhere to a true 3-2-1 strategy, but it's especially important for high-value data. Storing backups in geographically separate locations minimizes the risk of complete data loss from a single disaster event.

Version control: Enabling restoration to specific points in time

Backups should capture various versions of your data, allowing you to restore to a specific point in time if necessary. Document your version control procedures and schedule regular testing to ensure the restoration of previous data versions works seamlessly.

Hot storage for rapid recovery: Ensuring quick access to critical data

Store your backup data in readily accessible, hot storage. This minimizes retrieval times during a disaster, enabling faster recovery of critical applications and data.

By implementing a robust backup strategy that incorporates the 3-2-1 rule or greater, immutability, version control, and cloud storage, businesses can ensure the protection of their critical data against various threats.

Using snapshots, replication, or cloud storage alone limits your data protection strategy. Moreover, prioritizing additional protection for highly sensitive data further strengthens your institution's data security posture. By combining these tools in a thoughtful way, organizations can better protect their critical data.

Case Study: Texas A&M

Renowned University Protects Field Research With Easy Endpoint Backup

1 Day
Implementation

40 Years
Legacy Protected

$0
Cost Restores

Learn More

> I have full trust in Backblaze that, if something were to happen, I could easily retrieve what I need. Hopefully that never happens, but the benefit is having the peace of mind that our data is secure.

Mario Hernandez, IT Manager III, Caesar Kleberg Wildlife Research Institute, Texas A&M University–Kingsville

Testing and Refining Your Plan: From Paper to Practice

A well-crafted DR plan is only as effective as its implementation and ongoing refinement. This section explores effective strategies for testing and improving your DR plan.

Plan accessibility: Always available

Ensure your DR plan is readily accessible to your IRT members, even during a disaster. Consider storing it in a secure, cloud-based location accessible from various devices and internet connections. Ensure you can access your plan even if your primary environment is down.

The power of multiple perspectives: Encourage team review

Don't go it alone! Encourage key personnel from various departments (IT, legal, finance, etc.) to review your DR plan. You might discover potential oversights or areas for improvement that you may have missed with their diverse perspectives.

From text to action: Building a testing framework

Your DR plan should clearly define:

Testing frequency

Establish a regular testing schedule. The optimal frequency depends on your company's size and risk profile. A minimum of annual testing is recommended, with more frequent testing (every six months) beneficial for larger enterprises.

Testing types

Incorporate various testing methodologies into your plan. This might include:

- **Tabletop exercises**
  Simulate disaster scenarios through facilitated discussions, allowing your team to identify communication gaps and areas for improvement in the DR plan.
- **Walk-throughs**
  Step through specific recovery procedures outlined in the plan with your IRT, ensuring team members understand their roles and responsibilities.
- **Limited scope DR drills**
  Simulate a disaster scenario with a specific system or application outage, testing recovery procedures for that particular environment.
- **Full-scale DR drills**
  Conduct comprehensive tests that simulate a full-blown disaster, involving all critical systems, applications, and personnel.

Bringing it to life: Drills and exercises

Regularly conduct DR drills and exercises to put your plan into action.

Involve your team

These exercises should involve all members of your IRT, including IT specialists, communication experts, and management representatives, simulating real-world response scenarios and fostering teamwork within the team.

Learn from every test

The primary objective of testing is to identify weaknesses and improve your DR plan. After each test, conduct a thorough review session.

Use your DR exercises and drills to analyze successes and failures, identify areas for improvement in the DR plan and update your plan based on the lessons learned.

Leveraging cloud-based platforms

Consider cloud-based solutions for DR testing and recovery. This eliminates the need for ongoing infrastructure investment dedicated solely to testing purposes. Leveraging tools like cloud storage and virtualized infrastructure services provide flexible, affordable options.

Here are some key benefits of cloud-based DR testing:

- **Cost-effectiveness**

  Cloud platforms offer on-demand resources, eliminating the need for dedicated infrastructure and associated costs.

- **Scalability**

  Cloud resources can be easily scaled up or down to meet your specific testing needs.

- **Repeatability**

  Cloud environments allow for replicating test scenarios consistently, facilitating effective training and process improvement.

By implementing a robust testing and refinement plan, businesses can ensure their DR strategy remains current and effective. Regular testing helps identify weaknesses, promotes team coordination, and fosters continuous improvement, ultimately enhancing your company's ability to respond effectively to unforeseen disasters.

Embrace the power of retrospectives

Don't shy away from analyzing your performance during DR tests.

- Conduct post-mortems (also known as retrospectives) after drills and exercises to analyze performance and gather insights.
- Encourage open discussion and feedback from all participants, including the IRT and potentially impacted stakeholders.
- Identify areas where the plan fell short or where communication could be improved.
- Apply these insights to fortify your DR plan and improve your overall disaster preparedness.

Lessons learned during DR tests should inform the process and must be documented to augment and update your DR plan for future events.

APPENDIX A: DR Checklist

This checklist is designed to cover key aspects of DR planning and implementation to ensure that businesses are thoroughly prepared to handle unexpected disasters efficiently and effectively.

1. Risk assessment and planning

- ☑ Conduct a comprehensive risk assessment to identify potential threats and vulnerabilities.
- ☑ Develop a DR plan that addresses identified risks specific to your environment.
- ☑ Ensure DR plans align with business continuity, compliance, and cybersecurity insurance requirements.

2. Infrastructure and resources

- ☑ Assess and document the IT infrastructure, including hardware, software, and network configurations.
- ☑ Ensure sufficient backup facilities and procedures are in place and regularly tested.
- ☑ Evaluate the need for and implement cloud-based solutions for redundancy.

3. Data management

- ☑ Implement regular data backup procedures (daily, weekly, monthly).
- ☑ Test data restoration processes to ensure data integrity and availability.
- ☑ Classify data based on sensitivity and criticality, applying appropriate security measures.

4. Team roles and communication

- ☑ Define roles and responsibilities for disaster recovery within the IT team and broader staff.
- ☑ Establish and regularly test communication plans both internally and with external stakeholders.
- ☑ Train all team members on their roles in the DR plan.

5. Incident response

- ☑ Develop and document incident response procedures to address different types of disasters (e.g., cyberattacks, natural disasters).
- ☑ Set up an incident response team with clear roles and responsibilities.
- ☑ Keep an updated contact list of all team members and critical service providers.

6. Vendor management

- ☑ List critical vendors and service providers, along with contact details and service level agreements (SLAs).
- ☑ Establish protocols for coordination with vendors during and after a disaster.
- ☑ Regularly review and assess vendor performance and contingency capabilities.

7. Testing and drills

- ☑ Conduct regular DR testing to validate the effectiveness of the plan.
- ☑ Update DR procedures based on feedback and findings from tests and drills.

8. Documentation and compliance

- ☑ Ensure all DR procedures and policies are well-documented and easily accessible.
- ☑ Regularly review and update DR documentation to reflect new threats, technological changes, and regulatory updates.
- ☑ Conduct compliance audits to verify adherence to legal and regulatory requirements.

9. Awareness and training

- ☑ Implement a continuous education program on disaster recovery for IT staff and relevant stakeholders.
- ☑ Provide regular updates and training sessions on new threats and recovery techniques.
- ☑ Develop awareness programs for the organization's employees about their role in disaster preparedness.

10. Review and continuous improvement

- ☑ Schedule periodic reviews of the DR plan to ensure it remains relevant and effective.
- ☑ Solicit feedback from stakeholders to improve DR strategies.
- ☑ Keep abreast of technological advancements and incorporate appropriate innovations into the DR plan.
- ☑ In the event of a cyberattack, perform a retrospective with the goal of incorporating key learnings into your DR plan.