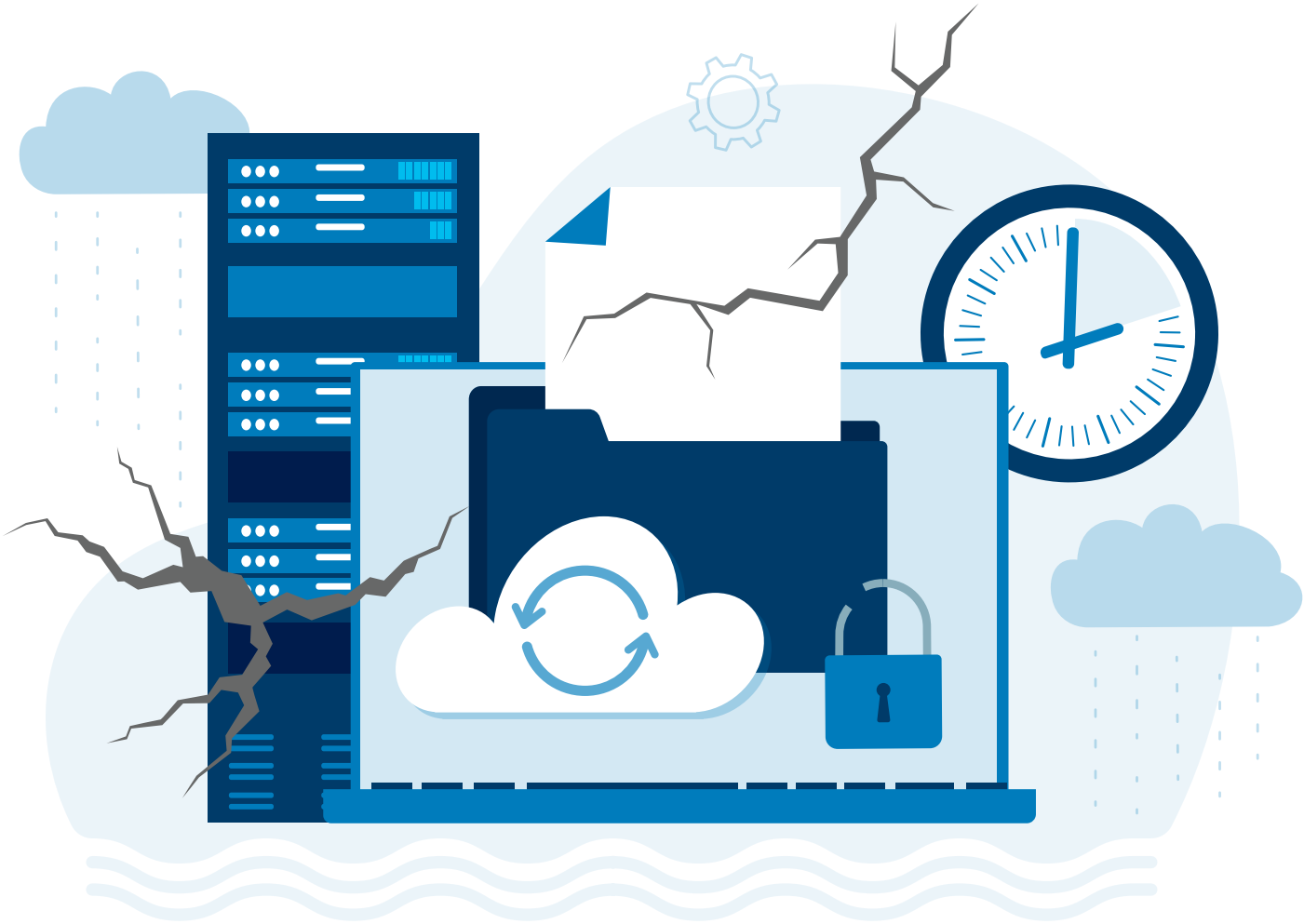
Macrium Software

Disaster Recovery Guide for IT Pros

www.macrium.com

THE COMPLETE GUIDE TO DISASTER RECOVERY



A cyber attack, an earthquake, a power outage, or a flood can damage an organization's technology infrastructure and prevent it from conducting business. And for any business, downtime costs money. Although these scenarios seem extreme, these situations are not uncommon. From 2019 to 2022, one in five organizations reported experiencing outages that resulted in serious financial losses and damage to their reputations.

While it is impossible to protect your business from every threat out there, one thing you can do is establish a robust disaster recovery plan to get your systems back up and running as quickly as possible.

This guide details the critical nature of disaster recovery and its implications, the steps to creating a disaster recovery plan, how to evaluate disaster recovery solutions and how to test, maintain and activate your plan.

UNDERSTANDING DISASTER RECOVERY

Disaster recovery is the process of restoring and resuming essential business functions following a disruptive event. It can be used broadly to apply to physical infrastructure and in-person operations. But in the context of this guide, it refers to the recovery of the technology infrastructure that major business features and operations, including data, hardware, networks and applications, rely on to operate.

The primary goal of disaster recovery is to minimize downtime, mitigate damage and restore essential operations and services. The cost of downtime can be devastating. A single hour can range from a little over $25,000 for some small businesses to over $500 million for large enterprises. Then there are the harder-to-calculate costs due to factors such as customer dissatisfaction and the impact on a business's reputation and credibility, which can be long-lasting.

Being able to recover quickly in the face of a disaster is critical to a business's bottom line and even its survival. For example, the Federal Emergency Management Agency (FEMA) states that around a quarter of businesses do not reopen after a disaster. Some of these are caused by cybersecurity incidents, including attacks and breaches. It's also important to note that it's not just large enterprises that are at risk of being targeted by hackers. Nearly three-quarters (73%) of small business owners in the U.S. reported experiencing a cyber attack in 2023. The European Union is bringing into force measures to ensure a level of cybersecurity readiness and remediation through the NIS2 directive, which mandates backup and recovery requirements, among other directives.

Many organizations abide by the 3-2-1 backup strategy. This recommendation requires three backups on two different types of media, with one copy located offsite. However, disaster recovery involves more than simply backing up data and systems. Backups need regular attention and testing, as restores can fail due to corrupted data or configuration errors. Restoring data and getting systems back online may take hours or days.

A disaster recovery plan is essential to facilitate a rapid and complete recovery. A comprehensive plan combines a set of carefully thought-out strategies, policies and solutions that span people, processes and technology, including:

- Selecting and implementing backup and recovery solutions to protect critical data
- Establishing employee roles and responsibilities
- Regular testing, maintenance and updates

Understanding the requirements of effective disaster recovery and developing a strong plan tailored to the specific IT environment, helps businesses become more cyber-resilient and more likely to maintain continuity in the face of a major disruption. As data breach rates continue to rise, disaster recovery planning should be a top priority.

ASSESS YOUR RISKS AND VULNERABILITIES

The types of disasters and cyber threats an organization is most likely to face depend on its activities, size, technology system configuration and many other factors. Evaluating your technology infrastructure's vulnerabilities and the specific risks that could disrupt operations can help you create a recovery plan for your unique needs.

A complete assessment holistically examines the entire IT environment, including cybersecurity policies and procedures and the infrastructure. This framework should ensure you have taken everything into consideration.

Inventory your entire network infrastructure. This should include hardware devices and equipment (servers, laptops, desktops, hard drives, modems, routers, etc.) and software like operating systems, databases and applications. If necessary, this detailed documentation will help rebuild the system, especially if there are multiple offices or employees work remotely.

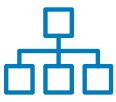
Identify potential threats. Research the risks of cyber threats based on the nature of your business and emerging methods of attack. For example, some of the industries facing the most cyberattacks include manufacturing and finance.

Natural disasters and other events can impact your infrastructure. Consider factors like geographic location and climate patterns. For example, keeping all backups on-site presents a serious risk if the business is located in an area prone to earthquakes or wildfires.

Remember that employees are a major cause of data loss and leaks. One study shows that 88% of security breaches are the result of human error.

Conduct a risk and business impact analysis. After you have identified the threats, assess the likelihood and potential impact of each one on your infrastructure and operations. This analysis should also incorporate dependencies between different systems, processes and teams to understand and illustrate the cascade effect across the business. Then, develop scenarios for the most likely risks and outline the operational and financial impact for each. These could include lost or reduced revenue from sales, regulatory fines, legal action and negative customer reviews. Use this information to assign each risk a severity level.

Assess current organizational vulnerability. Identify areas where the business may be more vulnerable to your identified risks. These could include gaps or weaknesses in network security, a lax device management policy or inadequate employee security training and awareness. Talk to managers and leaders across the company to get a full picture of the landscape.



Do a gap analysis. Compare your current ability to recover from a disaster with the risks and vulnerabilities this process uncovered. Where do you need more preparation? Where do you need additional resources? Are your technology solutions sufficient to quickly recover critical functions? Can you simulate your recovery processes? If your recovery files are stored in the cloud, will limited bandwidth hamper your ability to recover them?

The outcomes of this assessment will guide your disaster recovery planning with insights on where you should focus attention and resources to secure the best outcome in the event of a crisis.

CHOOSE A DISASTER RECOVERY SOLUTION

Disaster recovery software uses automated processes and workflows to reduce the manual burden on IT teams, minimizing downtime and enabling faster restoration. However, just as all organizations are different, so are disaster recovery solutions. Finding the right one requires research to identify capabilities and features that align with business needs and the IT environment. These are some of the main considerations when researching and ultimately investing in a disaster recovery solution.

- Consider the nature of your business. The types of data, systems, equipment and applications the organization uses can point you to specific features that might be required. For example, downtime for a manufacturer can cause production lines to stop, so seek solutions with rescue features that can restore data and systems from backups within an acceptable amount of time. You should also investigate how well the solution will integrate with existing infrastructure.

- Decide if you need cloud or offline backups. Cloud backups offer a convenient and low-maintenance option, although they require ceding a certain amount of control to the provider. In addition, confusion over whether the customer or the provider is responsible for security configurations can leave data vulnerable. Offline backups offer organizations more control and are an essential defense against ransomware attacks. They may also be the only option for networks with legacy systems.

- Know your downtime parameters. Recovery Time Objective (RTO) is the maximum amount of time a business can take to get critical functions back online. Recovery Point Objective (RPO) is the maximum acceptable amount of data loss or interruption after a disaster. Setting these metrics will help you pinpoint a disaster recovery solution that offers the speed and reliability you need. These values will vary by organization and industry. In sectors such as manufacturing, extended downtime and data loss can cause production to cease, while for sectors like emergency services, even a few minutes of downtime can be disastrous. An RTO for mission-critical applications in manufacturing, for example, might be half an hour, with an RPO of 15 minutes or less.

- Assess the capacity for scalability. You want a solution that can accommodate your business as it grows and you add more users, data and infrastructure. Key areas include the ease of adding additional computers to the solution and new or existing backup plans, licensing new systems, adding new users, assigning relevant permissions, adding storage and even potentially adding new storage sites. Features such as centralized enrollment, installation and monitoring can ensure users and devices are protected as systems expand.

- Ensure it offers ample security measures. Backups should be encrypted and password-protected with multi-factor authorization.

- Calculate the long-term costs. Beyond the upfront price, consider ongoing expenses over the life span of the solution, such as maintenance, upgrades and other potential expenditures.

- Focus on automation. Automation minimizes the possibility of human error and reduces IT workload by streamlining the recovery process. For example, backups can be scheduled and created automatically. Notifications can be set and enabled to tell the IT team if there is a problem. This frees up their time to focus on more complex recovery tasks or issues that require special attention.

- Consider compliance requirements. A solution should include ample security measures to protect sensitive data while backing up and during the recovery process. Make sure it has adequate measures in place to meet industry regulations or applicable legislation regarding data security and privacy while in storage and in transit.

- Look for testing and validation features. The solution should have the capacity to test backups in virtual environments to avoid impacting normal business operations.

- Make sure it's user-friendly. Features like a single dashboard and intuitive tools support faster training, adoption and optimization.

- Evaluate customer support. Is assistance available if the solution doesn't work as planned? If so, what is the typical response time? Does the vendor offer other resources, such as training tutorials or a knowledge base?

- Research customer reviews and the company's reputation. Look for ratings from verified reviewers, such as Trustpilot and Google Reviews. Remember that reviews in industry publications and other online sites could have been paid for by the company. Talk to the in-house IT team for their recommendations.

These considerations are just a start. Every business will have its own set of requirements and priorities when sourcing a disaster recovery solution. But carefully considering these and other factors can help you make an informed choice that supports your needs.

U.S. e-commerce company Factory Direct Craft carefully considered different options when its backup solution became too expensive. The business ultimately chose Macrium because its features and capabilities were aligned with its need for reliable backup and speedy recovery. While price was a secondary consideration, the cost was also more affordable than competitor offerings.

BUILD YOUR DISASTER RECOVERY PLAN

If only recovering from a disaster were as easy as pushing a button. While technology makes restoring data and systems faster and easier than ever, full recovery still requires real-world efforts from the IT team as well as employees across the organization.

A disaster can cause confusion and panic. Having a disaster recovery plan in place is critical to provide guidance and make sure recovery efforts run smoothly and proceed as quickly as possible. Remember, when it comes to cybersecurity, the question is not *if* but *when* it will happen to your business.

Follow these steps to create your recovery plan.

1. Identify and prioritize critical functions. Decide which operations are the highest priority for business continuity purposes, such as customer service or communications. This will help you identify in what order system components should be restored to support critical, essential and nonessential functions.
2. Create a disaster recovery team. Identify the individuals on the IT team who will be responsible for leading disaster recovery efforts and assign them clear roles and responsibilities. Make sure the relevant team members know where backups are, how to retrieve them and how to initiate restoration. Non-IT employees can take on tasks like leading internal communications, public relations and customer outreach.
3. Document hardware, software and network configurations. This will be critical to recovery efforts if the network is corrupted or if infrastructure and IT teams are geographically dispersed. Include serial numbers for hardware and vendor contact information in case their assistance is needed.
4. Outline procedures for responding to different types of disasters. Create detailed processes for the most likely threats the business faces, such as a data breach or a ransomware attack. In addition to IT concerns, include directives for employees to support business continuity by prioritizing tasks and designating alternative work sites.
5. Establish a backup strategy customized to business needs. Businesses should have a consistent schedule for backups and ensure they have multiple copies in different locations and formats, such as on servers and in the cloud. Depending on the nature and size of the organization, you may wish to implement a schedule for incremental and differential backups to save space and minimize the costs associated with multiple full backups. Features like bandwidth throttling and CPU priority control can also reduce the number of system resources required to perform backups. This makes it easier to run more frequent backups, even during business hours.
6. Create a communication plan. Consider implementing a phone tree or text chain to alert employees and keep them informed. Employees should also be directed to a channel they can access for updates. You should also be able to alert your customers and let them know when operations will be restored.
7. Document the recovery plan. Store it where authorized employees can access it during a disaster and make sure they know where it is.

Regular backups are essential for peace of mind. Macrium Reflect gives the IT team at the University of Leicester the ability to see when backups are scheduled. It also sends alerts if issues arise, enabling team members to act quickly and ensure clean backups are always available.

TEST AND MAINTAIN THE PLAN

Disaster recovery planning shouldn't be a one-time or occasional event, it should be integrated into a business's operations. Carry out regular training and drills to ensure employees understand their responsibilities and execute them correctly. These activities can help employees stay focused during an incident and prevent the confusion and uncertainty that can hamper recovery.

Test your plan regularly to check that processes and technologies work as expected. Conduct an evaluation after each test to identify where modifications need to be made, where the plan can be optimized and to resolve any technology issues. Then test your plan again. This iterative process will help ensure that it aligns with current technology infrastructure and organizational resources.

Finally, test the backups themselves. Data may be lost or corrupted due to unexpected technology hiccups, such as issues with integration due to upgrades or added infrastructure. Backups can also be targeted by ransomware or be infected with other types of malware. More than one in four businesses fail to recover data from a backup after a ransomware attack. You don't want to find out your backup is corrupted, incomplete or otherwise damaged in a real crisis—another reason to keep multiple backups.

Keep Up with Evolving Risks

Technologies evolve and so do threats. Criminals are always developing new ways to gain access to networks and systems. This makes it critical to continuously monitor the digital landscape for new methods of attack that could affect your infrastructure and your ability to respond to a disaster.

Regularly review your disaster recovery plan, as well as the technologies you use to perform backup and data recovery, to make sure they offer the protection you need against cybercrime.

It almost goes without saying, but staying on top of updates and security patches for all software and applications is imperative to fully protect data and systems and ensure they can be recovered in the event of a disaster.

Manage Technological Drift

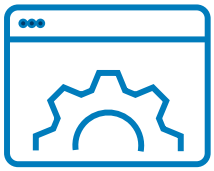
Drift refers to how system configurations in IT environments change over time. It's an inevitable result of ongoing hardware and software changes due to updates, new applications and hardware, manual changes and many other factors.

However, unchecked and undocumented drift can cause data recovery to be delayed or even fail when a disaster recovery plan is no longer aligned with the technology infrastructure.

You can manage the risks associated with drift by:

Addressing configuration issues quickly

Documenting configuration changes as they occur



Automating configuration across systems to avoid human error

Regularly testing and updating disaster recovery software and plans

When Disaster Strikes

In the event of an incident that threatens networks, systems and data, the value of having a detailed recovery plan that has been tested, maintained and updated will quickly become clear.

Disaster response can be divided into four phases.

- **ACTIVATE**
  Direct members of the disaster recovery team to take action as outlined in the plan.
  Initiate communication plans to alert the workforce, as well as customers who may be affected.
- **ASSESS**
  Determine the type, nature and scope of the disruption.
- **EXECUTE**
  Put the appropriate recovery strategy into action.
- **EVALUATE**
  When the restoration is complete, check that data and systems are complete and functioning normally.

FUTURE-PROOFING YOUR BUSINESS

Focusing on disaster recovery helps ensure data and systems stay safe and secure, even as threats evolve and change. An integral part of any proactive strategy is to ensure the integrity of networks, systems and data.

But this is just one aspect of safeguarding your IT ecosystem. An organization that focuses on cyber resilience across all aspects of its operations—from embracing new technologies to keeping abreast of cyber threats—will be better positioned to bounce back from a disruption with minimal damage and delay.

1. *https://uptimeinstitute.com/about-ui/press-releases/2022-outage-analysis-finds-downtime-costs-and-consequences-worsening*
2. *https://orangematter.solarwinds.com/2023/07/12/true-cost-of-downtime/*
3. *https://www.fema.gov/press-release/20230502/stay-business-after-disaster-planning-ahead*
4. *https://www.idtheftcenter.org/post/2023-business-impact-report-record-level-attacks-still-high-confidence-in-defense/*
5. *https://www.nis-2-directive.com/*
6. *https://www.forbes.com/advisor/education/it-and-tech/cybersecurity-statistics/*
7. *https://www.statista.com/statistics/1315805/cyber-attacks-top-industries-worldwide/*
8. *https://cisomag.com/psychology-of-human-error-could-help-businesses-prevent-security-breaches/*
9. *https://www.macrium.com/resources/factory-direct-craft*
10. *https://www.macrium.com/resources/University-of-Leicester-Case-Study*
11. *https://www.at-bay.com/press_releases/report-reveals-businesses-fail-to-recover-backup-when-hit-by-ransomware/*
12. *https://www.macrium.com/*

ABOUT MACRIUM

Macrium Software designs solutions to protect the most valuable asset in the world—your data. We're dedicated to creating dependable software, providing quality service and maintaining superior relationships with our customers and partners.

Launched in 2006, Macrium is known today as one of the most reliable, scalable and dependable backup companies in the industry. Millions of people across the world rely on us to keep their valuable data safe and accessible and our easy-to-use solutions can be found in homes, small businesses, public sector networks, multinational companies and more.

Macrium Software

www.macrium.com/site-backup-demo