



When IT Stops, Business Stops.

5 Steps for Disaster Recovery Planning

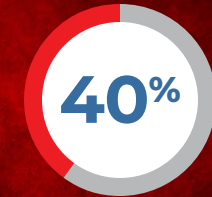
Your Business Runs on IT

When IT stops, business stops and depending on the severity of the outage it can cost companies hundreds of thousands of dollars or more. Regardless of whether the outage is the result of a natural disaster, technology failure, or a host of other causes, you need a tried-and-true disaster recovery (DR) plan to protect your business.

How do organizations plan for the unexpected?

- **Identify potential disasters.** Are your operations and equipment exposed to natural disasters, cyber attackers, or malicious acts? Understanding the potential disasters will guide the development of your plan.
- **Think about business continuity.** Focused on how an organization survives a disaster, this planning includes developing risk and business impact analyses, identifying major threats, and making plans to keep the entire business operational.
- **Consider your disaster recovery.** This tends to be more IT-focused in nature which includes developing plans to restore systems, recover data, and return other business processes to normal.

In today's world, planning how your organization will respond to disasters is not just a good idea. It's imperative.



**of businesses do not
reopen following a
disaster and another
25% fail within 1 year.
Over 90% of companies
fail within 2 years of being
struck by a disaster.**

—FEMA and U.S. Small Business
Administration

Know your DR Objectives

At the core of your DR strategy should be an in-depth analysis that identifies the impact and cost of various disaster scenarios. By utilizing this analysis, you can determine the appropriate level of disaster recovery your business requires and the budget to deliver it. Companies that invest in a DR strategy without doing their due diligence risk deploying a solution that doesn't mitigate risk to the extent that is necessary, or they overspend on a solution that doesn't deliver the value they need.

To develop this strategy, you must first understand the three Rs — RTO, RPO, and RCO.

Recovery Time Objective (RTO)	Recovery Point Objective (RPO)	Recovery Cost Objective (RCO)
The maximum acceptable amount of time between an unexpected outage and the resumption of normal operations/service levels.	The maximum amount of data – as measured by time – that can be lost after a recovery from a disaster, failure, or comparable event.	The budget amount you plan to spend on your disaster recovery solution. This amount will impact your solution options.

The ideal disaster recovery strategy will balance the cost of an outage to the business with the cost to mitigate that outage.

DR planning without clear objectives is like asking Siri® for directions without a destination.

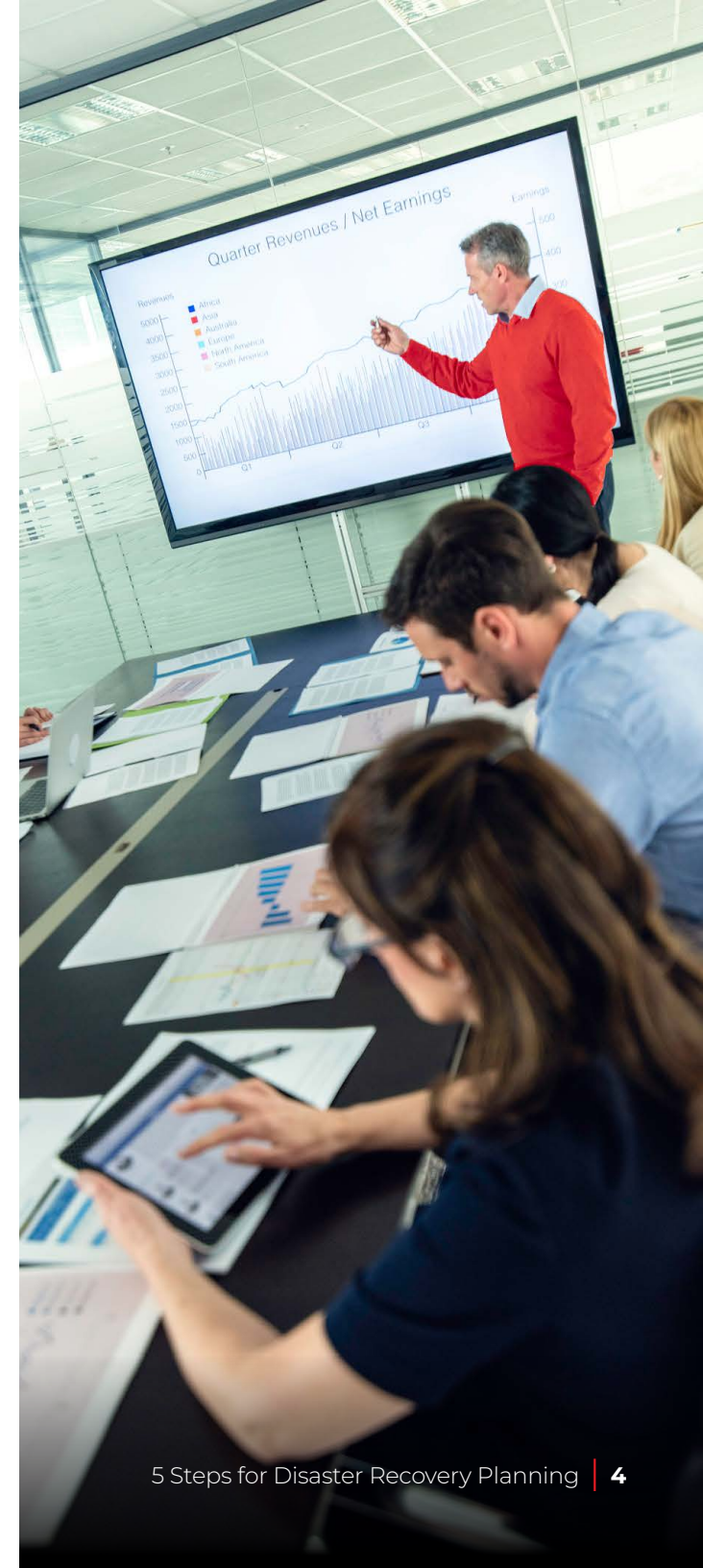
Assemble the Right Team

Disasters come in all shapes and sizes. Some will be very IT specific, like a server crash, while others, like a natural disaster, will have a much broader impact. With the worst-case scenario in mind, you need to make sure that you have some key functional areas of your business engaged in the development of your disaster recovery strategy and that they are ready to execute their part of the plan.

Who should be on the team?

- **Executive management:** Funding your disaster recovery plan starts at the top. Educate them on the business risks and the costs to mitigate them to justify allocating the budget.
- **IT management:** This person or group is responsible for building out the disaster recovery team, securing executive buy-in, and overseeing the development of comprehensive disaster recovery plans.
- **System administrators:** This includes administrators for networking, telecommunications, servers, storage, and backups who are responsible for the operations of your IT assets or infrastructure.
- **Outside consultants:** Experts in disaster recovery planning can be worth the investment to help you avoid common mistakes and pinpoint proven solutions to meet your recovery objectives.
- **System users:** Having a team available to test systems can help you get IT systems up and running after a disastrous event. This group can also support testing for your disaster recovery plans.
- **Facilities management:** If your data center is on-premises, you'll need to make sure a facilities manager is involved to access the site, do any clean-up, or make necessary repairs.

A cross functional team that takes ownership of the plan will increase your chances of success.



Choose the Right Solutions

Once you have defined your disaster recovery objectives and identified your team, you're ready to begin looking at solutions that will allow you to achieve your goals. Ask these questions to get started:

Where will recovery take place?

- Cold site: Reserved infrastructure that can be used to restore data and operations.
- Warm site: Available infrastructure pre-built and ready to restore data and operations.
- Hot site: Fully redundant infrastructure that's in sync with your primary data center.
- Cloud solution: Infrastructure outside your organization that's ready to go in a disaster.

Which disaster recovery solutions meet your recovery objectives?

When evaluating disaster recovery solutions, the general rule of thumb is that the faster you want to recover and the less data you can lose the more expensive the solution will be. As you explore your options, don't lose sight of all your objectives.

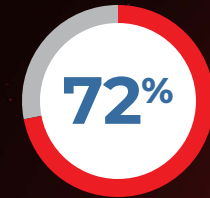
Do you have the network infrastructure to provide access to restored resources?

It's one thing to be able to recover your critical systems, but you can't stop there. Once systems have been restored, you need to have network connectivity that allows remote locations and end users to gain access to those systems.

Does your disaster recovery plan protect your security and compliance?

When a disaster strikes, organizations can get so focused on recovery that they overlook protecting themselves against future threats. Build checks and balances into your recovery process to make sure you restore all required security and compliance measures.

RTO, RPO, and RCO identify the goals you are building towards and help you select the right solutions to achieve those objectives.



**According to Gartner®,
72% of organizations are
poorly positioned in terms of
disaster recovery capabilities,
with 63% likely suffering from
“mirages of overconfidence.”**

—Gartner, *Market Guide for Disaster Recovery as a Service*, 17 May 2023.

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

Best Practices for DR Planning

While this may be the first disaster recovery plan you have created there are plenty of people that have gone before you and built a roadmap to success. As you develop your plan, make sure you include these best practices.

Write it down. A plan in someone's head is hard to share — especially in disaster conditions. Document your plan and distribute it to everyone who would be involved in addressing a disaster.

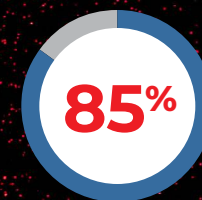
Make it accessible. Consider storing your plan in the cloud or another offsite location. You don't want to have a great plan that you can't get to during a disaster.

Plan for post-recovery. The recovery process doesn't end when your systems are running in the DR environment. Make sure your plan includes the steps to return to normal.

Update regularly. Your business and technology environment are constantly changing. Make regular updates a standard part of your change management processes so your plan stays up to date.

Test your plan. Many companies have been disappointed when their theoretical plan was put into practice and failed miserably. We have dedicated the next section to testing your plan.

It is important to understand that DR planning is not a one-time thing, it must evolve with your changing business needs. Consider this plan a living document that needs to be taken off the shelf at least once per year and validated against the current environment.



of organizations suffered at least one cyber-attack in the preceding 12 months.

—Data Protection Trends Report, 2023

Testing your DR Plan

The time to identify gaps in your DR plan is during testing, not during a disaster, yet many companies assume their plan will work and never test it. Add an annual test to your DR plan that includes the following steps:

- **Set goals for your test.** Create a plan, with clear success criteria, that allows you to test your disaster recovery solution to ensure it meets your recovery objectives.
- **Establish ground rules for your test.** Implement good project management and make sure everyone knows what their role is during the test. Set clear expectations for when milestones need to be completed.
- **Develop a realistic disaster scenario.** To make your test as accurate as possible, consider simulating real-world situations like a natural disaster, hardware failure, or cyber-attack as part of your test.
- **Complete a disaster recovery test.** Run through the exercise from start to finish. Document failures and determine how you'll follow up and update your plan.
- **Consider your third-party vendors.** If you will be relying on any third-party vendors as part of your disaster recovery, be sure to include them in your test.

Testing your disaster recovery plan should be done at least annually — and more often if there are major changes to your IT systems or within your organization.

Among survey respondents, DR testing frequency is very low.

Just 50% are testing only annually or at less frequent intervals, while 7% didn't test their DR at all.

—Computing Research, 2021

Why Racksquared?

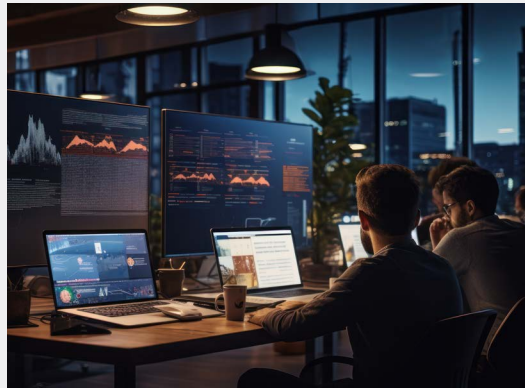
We deliver disaster recovery solutions you can count on, while you focus on your core business. How do we do it?

EXPERTISE



Racksquared's experts have the knowledge and experience to help you create and implement a disaster recovery plan to meet the RTO and RPO of your business. This enables you to focus on your core business and customers rather than worrying about a service outage.

TECHNOLOGY



Racksquared leverages industry leading technologies from IBM, Veeam, and Cybernetics to perform SAN replication and VTL backups. This ensures that customers have multiple copies of their data with one being off-site and the option for immutable storage.

ENVIRONMENT



Racksquared's infrastructure and environment are designed to be secure, reliable, and resilient so your business is always up and running. In the event of a disaster, our multiple data centers can be leveraged to recover quickly reducing downtime and data loss.



CASE STUDY

Compass Health Brands Improves its Well-Being with Disaster Recovery.

CHALLENGE:

For years, Compass Health Brands recognized that it needed a stronger disaster recovery plan in place, but the pandemic and subsequent supply chain issues made it a top priority. The company, which distributes medical products and equipment to retailers and healthcare providers, wanted a vendor that could handle both its IBM Power and Intel systems.

SOLUTION:

Compass Health Brands discovered Racksquared and appreciated its focus on small- and medium-sized businesses and their unique challenges. Racksquared's team drew on its expertise in iSeries, Intel, and networking to develop a high-availability disaster recovery solution tailor-made for the company.

RESULTS:

In the event of a disaster, Compass Health Brands can be back up and running quickly with only minutes of data loss. The company also gained a true partner in Racksquared. No matter when they need assistance, they've found Racksquared to be responsive and work through problems together.

What our Customers Say

“We run mission critical applications on the IBM Power platform and while it is extremely reliable, our company and the customers we service can’t afford extended downtime. By making a hardware reservation with Racksquared, we know that in the event of a disaster we will have resources available to us.”

— Duane Kunze, Director of Technology, Arrow International, Inc.

“During our initial DR test, Racksquared carefully outlined all the tasks involved in the process, creating a playbook for use in the event of a disaster. This playbook is a huge value add for us. Now, we have a plan that tells us everything we need to do, both from a technical and business perspective.”

— Mark Biegert, Director of IT, Freelancers CO-OP



Get Started Today

Interested in learning more about disaster recovery solutions?

LEARN MORE

Visit racksquared.com/disaster-recovery-solutions to learn about the disaster recovery solutions we have available to support your business needs:

- Veeam Cloud Connect backup and disaster recovery solutions
- Cybernetics VTLs and replication solutions
- Colocation with backup solutions
- High availability solutions
- Reserved infrastructure solutions
- Disaster recovery plan testing

CONTACT US

Our team is available to work with you to understand your current disaster recovery strategy and the challenges your business is facing. Let's talk about solutions to protect your business.

Give us a call at (855) 380-7225 or email sales@racksquared.com.

**Your business runs on IT.
Let Racksquared keep your business up and running.**



Racksquared can help simplify IT so that you can focus on growing your core business and evolve to meet the changing demands of customers. We do this by providing access to technical expertise, the latest technologies and a secure, reliable, resilient environment for your IT systems. We become an extension of your team, providing flexible designs and solutions while managing, monitoring, and supporting your infrastructure, so that your business is always up and running.