Prescient Solutions

Don't Fall for the Disaster Recovery Myths

GUIDE

Don't Fall for the Disaster Recovery Myths

There are a lot of myths about disaster recovery (DR), and falling for them can cause big problems when a crisis occurs. Even though a disaster can shut your business down—sometimes permanently—many companies fail to create a disaster recovery plan. That's because they believe the biggest myth of all: that disaster won't happen to them.

While your company may never be inundated during a 100-year flood, there are plenty of smaller everyday disasters that put every business at risk, including those as minor as someone tripping over a cord.

And even companies that have a disaster recovery plan can still be at risk if they fall for these 5 disaster recovery myths.

1 Disaster Recovery Myth #1: Having A Disaster Recovery Plan is Enough.

So you didn't fall for the uber-myth and recognize that you need a disaster recovery plan. That's great, but don't stop there. Having a disaster recovery plan alone isn't enough to get your business recovered.

First of all, if you don't test your plan you have no idea whether it works. It's easy to miss critical steps, even critical systems. It's also common to be overly optimistic about how quickly systems will come back online.

Secondly, getting your business operational again requires business continuity, not just disaster recovery. You need to know how the business will resume functioning once systems are back up. This requires addressing all aspects of the business, not just the IT processes. Even if your DR plan gets your systems up at a secondary data center, if you don't have a secondary office site or remote access capability, you still won't get any business done.

Disaster Recovery Myth #2: You Should Use the Same Strategy Across the Entire Business.

Since a DR plan isn't something your employees work with every day, you need to make it as simple as possible for them. That means taking the same approach to DR across the entire business, right?

In fact, that's exactly the opposite of what you should do. While making the recovery straightforward for operational personnel is important, the primary goal of disaster recovery is getting the business running again. That means it's important to take a hard look at all the business applications and processes and determine which of them are critical to business functioning.

Every application should be evaluated to determine its importance to the business, and then a specific, targeted Recovery Point Objective (RPO) and Recovery Time Objective (RTO) should be set for that application. Once you know how much data you're willing to lose from that application (the RPO) and how long you're willing for that application to be down (the RTO), you can craft a recovery strategy that matches the application's needs.

Disaster Recovery Myth #3: End of Day Backups Are Enough.

Recovering your systems requires having a copy of your data, but relying on last night's backups means you may end up losing almost an entire day's work when disaster strikes. Manually reproducing that much data will be time consuming and difficult at a minimum, maybe even impossible. To avoid this, you need a process that lets you recover same-day work (your RPO will let you know how much of that work you're willing to lose). Instead of just end of day copies, you probably need snapshots or replication to make intra-day data available.

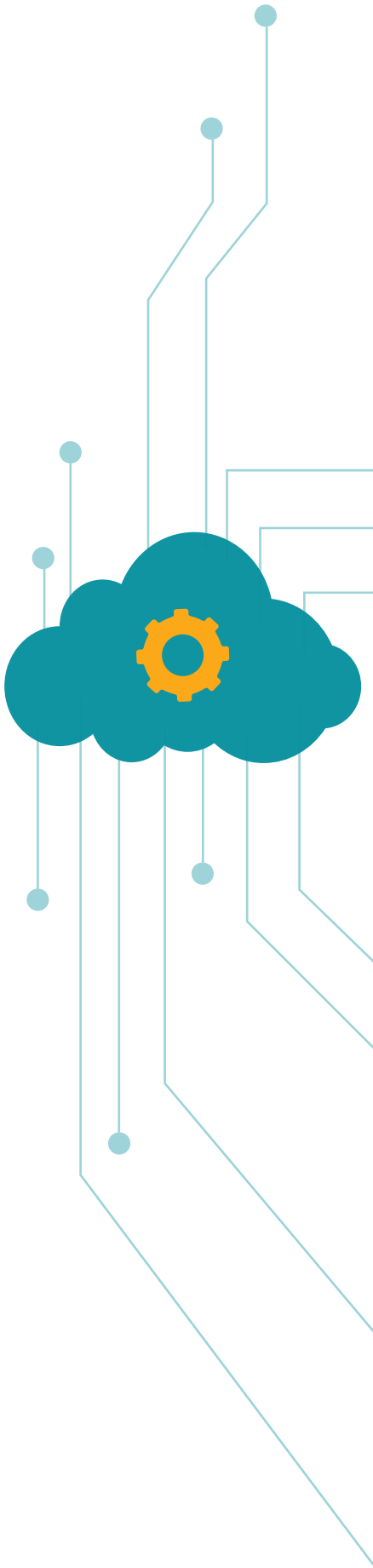
4 Disaster Recovery Myth #4: DR Requires a Secondary Site, and Having a Secondary Site Means You Have Adequate DR.

Many businesses assume that preparing for disaster recovery requires having a secondary site with exact duplicates of all their hardware and software assets. They also assume that having the secondary site is enough to ensure adequate DR.

Building a secondary site that's a true clone of your primary site is very likely to be very expensive and also unnecessary. Not all of your systems are vital to business functioning—your secondary site probably doesn't need to have copies of your development and test servers, and there are most likely applications you can function without during a crisis. You also may be able to get by with lower-powered machines in your secondary site, accepting slightly degraded performance for the relatively short duration of a crisis, enabling you to save some money.

Having the secondary site with servers and applications alone isn't enough, though. To be prepared for a disaster, the site requires all the security of the primary site. The site also needs to be fully up to date, with the same patches and updates installed as at the primary site. Setting up a secondary site isn't a one-time function; it's an ongoing maintenance commitment.

The placement of the secondary site is also a concern. It's fairly common for secondary sites to be located geographically close to the primary site. While that's convenient, it diminishes the effectiveness of the secondary site as protection against a disaster.



5 Disaster Recovery Myth #5: Using The Cloud Means You're Prepared for Disaster.

The cloud has many advantages and can provide solutions for disaster recovery. Running your primary site in the cloud provides high availability and makes data accessible from anywhere. Backup to the cloud and Disaster Recovery as a Service leverage the cloud providers' support to simplify preparing for disaster.

Yet the cloud is not a complete disaster recovery strategy. The cloud providers have outages of their own. Whether the cloud is your primary or disaster recovery site, you need a strategy for coping with those cloud outages.

Disaster Recovery Plans That Don't Fall for the Myths

Creating a disaster recovery plan that doesn't fall for the disaster recovery myths requires carefully analyzing your systems and your business' disaster recovery needs. An effective DR plan accounts for all your needs, including:

- **Servers.** All physical and virtual machines should be identified and configuration details such as patch levels noted.
- **Networks.** Document and plan for the connectivity required between servers and the bandwidth needed for minimally acceptable performance.
- **Storage.** The DR site may not need the same storage capacity as the primary site. Depending on your assessment and how long an outage you plan for, the DR site may need the ability to store only a few days' data, rather than a full archive.
- **Applications.** Each application should be identified, along with its criticality. Document the detailed steps needed to recover the applications and the RPO and RTO expected to be met.
- **Vendors.** Make sure your vendors and partners know about your DR strategy and that their systems will work with your secondary site.
- **Personnel.** Both IT and business staff will be affected by any outage and need to participate in the recovery. Identify the key roles, personnel, and contact information to ensure that critical personnel can be reached. Have alternate contacts in case some team members can't be reached during the outage.
- **Business processes.** Business users will need to participate in recovering data that was lost when systems went down. Users may need to follow unfamiliar manual processes to execute business functions until all systems are recovered.

Use the Right Technology to Achieve Disaster Recovery

Creating your disaster recovery strategy requires making smart choices from available technologies including:

- **Replication**
  Replication creates near real-time copies of your data and supports rapid recovery of applications with minimal loss of data. You can replicate to the cloud or to a standby, secondary site. Replication can't be used to recover from situations that include data corruption, as the corruption will be included in the replicated copy.
- **High availability**
  Clustering solutions mitigate the impact of a single hardware failure, with hot standby nodes automatically picking up the processing load.
- **Snapshots**
  Snapshots provide recent local virtual copies of data.
  It's important to note that snapshots by definition are only local and will not support a recovery where the storage device has failed.
- **Backups**
  End of day backups give you copies of data that you can use to recover from. Onsite backups are at risk in case of a site wide outage; backups stored offsite can be time-consuming to access and cause delays in recovery.
- **Secondary site**
  Traditionally, disaster recovery resumes operations at a secondary site that mirrors the primary site in terms of its hardware and software. Today, the cloud means many companies can avoid investing in hardware that isn't expected to be used.
- **Disaster recovery in the cloud**
  Using the cloud as a backup target eliminates the delays in accessing backups stored offsite. The cloud can provide backup processing capacity as well as backup storage capacity. Since cloud contracts are usage based, using the cloud for DR processing can be significantly cheaper than the capital expenditures needed to set up a secondary site.
- **Disaster Recovery as a Service (DRaaS)**
  DRaaS provides a supported, highly automated solution to disaster recovery in the cloud.

Your disaster recovery plan can use some or all of these solutions, tailoring the recovery process to the recovery needs of each specific application and business process. Choose the appropriate solution based on your RPOs, RTOs, existing technology base, compliance mandates, and budget. You'll also want to consider how effectively your team can manage supporting multiple solutions, even if you document your recovery procedures thoroughly.

Test Your DR Plan to Prove Its Effectiveness

A DR plan that's simply written and filed away is likely to be ineffective in case of a real disaster. Personnel who aren't familiar with the recovery tasks are more likely to make errors under the stress of a real crisis, and the plan is likely to contain critical errors and omissions that hinder the recovery process.

It's important, therefore, to test your DR plan to make sure it will actually work to recover your operations in case of disaster. A table read-through of the document is the simplest and least disruptive way of reviewing the plan but is also the least likely to catch errors.

Actually executing the DR plan will help you thoroughly verify the plan both for its comprehensiveness and the accuracy of its steps and its time estimates. Running a DR test requires careful planning to make sure it doesn't impact business operations. Depending on your DR strategy, you may be able to run the test in parallel with production work, but it's often safest to run the test during non-business hours when the primary systems can be shut down. Running the test during off-hours lets you include business personnel as well as the technology staff and get full confirmation that the recovery process was successful.

Following a DR test, be sure you evaluate whether the test was successful and correct the plan to address any errors. If the test showed that your time estimates were wrong, you may need to rethink your approach to recovery and invest in other technology that will help you recover faster.

Disaster Recovery Planning is an Ongoing Process

Don't expect to file your DR plan away, even after a successful DR test.

Your business' technical infrastructure and business procedures aren't static, and as applications and servers retire and new applications and servers are brought online, the test plan needs to be updated. The contact information in the document also needs to be updated as well to reflect the changes in your staffing. Once the plan is updated, it should be tested again. In most cases, annual tests are adequate, but if you have special concerns or brought new mission critical applications online you may want to do a DR test more frequently.

Rely on Prescient Solutions to Support Your Disaster Recovery

Prescient Solutions has provided IT services to Chicago area businesses, government agencies, and other organizations for over 20 years.

Our team's expertise crafts disaster recovery plans tailored to your requirements; monitoring identifies the onset of problems; and support makes your recovery smooth and rapid.

Prescient Headquarters
1515 Woodfield Rd, Suite 880
Schaumburg, IL 60173
Phone: (847) 240-3900

Prescient Managed IT Services
141 W. Jackson Blvd, Suite 3850
Chicago, IL 60604
Phone: (888) 343-6040

About Prescient Solutions

Prescient Solutions has been providing managed technology services both on site and remotely to small, medium and large enterprises and government agencies for over 20 years. With certifications in key technologies spanning hardware, software, network, security, and other specializations, our team has the insight and experience to address the technical challenges that are holding back your IT team and your business. For more information about Prescient Solutions, or to request a complimentary IT consulation, call 888-343-6040, or visit www.PrescientSolutions.com.