# Six disaster recovery pitfalls and how to avoid them

[Disaster recovery](https://www.computerweekly.com/resources/Disaster-recovery) (DR) is the ability to return to “business as usual” operations after an IT failure, natural disaster, or other unexpected event, and is a key function of IT.

After all, the IT department is responsible for maintenance of core business systems and for protecting their data, for providing desktop or other personal computers, networks and more often than not today, voice communications.

But [disaster recovery planning](https://www.computerweekly.com/feature/Five-essential-steps-to-a-sound-disaster-recovery-plan) is a business-wide challenge and responsibility. Organisations depend ever more on their data, and IT is becoming more and more adept at providing access to that data anywhere in the world.

Against this, IT departments need to deal with ever larger volumes of data, as well as users and customers who are less tolerant of downtime, and a growing number of bad actors who see attacking data as a way to bring down organisations for financial gain.

The international standard for business continuity, ISO 27031, sets [a framework for organisations’ disaster recovery plans](https://www.computerweekly.com/feature/DR-101-The-disaster-recovery-plan-and-disaster-recovery-strategy).

But given the increasing complexity of both business operations and IT systems. there are plenty of traps for the unwary.

**DR pitfall 1: Failure to plan**

The greatest failing is to fail to plan for disaster recovery at all.

A DR plan need not be complex. In the case of a small business or branch office, it might comprise little more than [regular backups to disks stored offsite](https://www.computerweekly.com/feature/Time-to-restore-from-backup-Do-you-know-where-your-data-is) or, increasingly, to the cloud, and a plan for how to access the data and restore applications if the worst happens.

For larger organisations, a plan will go into far more detail about which applications are protected, how they will be recovered, and arrangements for alternative workspaces for staff, such as in [this example from IBM](https://www.ibm.com/services/business-continuity/disaster-recovery-plan).

Tony Lock, an analyst at Freeform Dynamics, stresses that a plan should state in what order various platforms must be recovered. “Sometimes this is obvious from application or service requirements, but where a major site recovery is required, then internal politics may also come into play,” he says. “There is also the question of who can initiate a DR action and under what circumstances.”

Further problems occur when organisations have a DR plan, but it is too limited in scope. Here, IT and the board can be lulled into a false sense of security. In such cases, there is a DR plan, but it fails to cover all applications and, vitally, their interdependencies.

“Only about 38% of applications are protected by a DR plan,” cautions Phil Goodwin, an analyst at IDC. “Most organisations provide DR for mission-critical applications, but then move on to other projects. The result is often that these mission-critical applications are missing data or connections to less critical applications. And the entire environment can’t be stood up rapidly enough.”

The plan must also set the [recovery point objective (RPO) and recovery time objective (RTO)](https://www.techtarget.com/searchstorage/feature/What-is-the-difference-between-RPO-and-RTO-from-a-backup-perspective) – how far back the organisation needs to go to obtain a clean and stable set of applications and data, and how quickly that needs to happen.

**DR pitfall 2: Failure to test**

The next, and perhaps greatest, pitfall is failing to test. [A frequently cited statistic](https://community.spiceworks.com/blog/3138-data-snapshot-how-well-equipped-are-businesses-to-bounce-back-from-disaster) is that 23% of organisations never test their DR plans, with a further 29% testing just once a year.

Whether an annual test is adequate will depend very much on the size and nature of the business. But a plan that is never tested is really only one step up from having no plan at all.

Almost a quarter of organisations never test their DR plans – a plan that is never tested is really only one step up from having no plan at all

“The other big issue concerns [testing of disaster recovery processes](https://www.computerweekly.com/feature/Disaster-recovery-testing-Technology-systems-to-test-DR),” says Freeform Dynamics’ Lock. “This is essential because until you test DR you really cannot be certain it will work, or whether all systems that should have been protected have been.”

Ensuring a robust testing regime needs strong leadership from the CIO. Effective DR testing can be disruptive and expensive. But failing to recover from a disaster will be more expensive still.

“The problem can be that either business users or budget holders may be reluctant to allow testing to take place,” warns Lock. This is why strong advocacy from IT leaders is so important.

Closely related to failing to test the DR plan, is failing to update it. A disaster recovery plan is a living document. As the business changes through growth, acquisition, business process changes or technology updates, DR requirements and methods will change too. A detailed plan that sits on a shelf will not be effective.

If the organisation does test the plan, CIOs need to ensure that any lessons learned – and there will be lessons learned – are used to update the plan. The updated plan needs to be tested, and the cycle repeated.

**DR pitfall 3: Failure to protect backups**

Malware, and [especially ransomware](https://www.computerweekly.com/news/252473457/Ransomware-authors-seeking-new-ways-to-avoid-being-spotted), is one of the reasons DR has moved back up the agenda in the past few years.

Protecting systems against ransomware in particular means [creating an air gap between production systems and backup copies](https://www.computerweekly.com/feature/Key-storage-choices-Cloud-vs-tape-for-archive-storage), or using [immutable storage technologies](https://www.techtarget.com/searchstorage/tip/Immutable-storage-What-it-is-why-its-used-and-how-it-works), not least because attackers have learned to target data backups first. Some organisations have returned to tape as a relatively low-cost way to move data offsite.

Unfortunately for DR teams, this is not always easy. Business continuity plans and shorter recovery time objectives rely on continuous data protection.

“But you can’t airgap on a continuous basis,” warns IDC’s Goodwin. Instead, organisations might need to accept 12-24 hours of data loss as the price for clean data.

**DR pitfall 4: Command, control and communication problems**

In a disaster recovery situation, [clear lines of communication](https://www.techtarget.com/searchdisasterrecovery/tip/How-to-build-a-strong-crisis-communications-team) and a clear idea of who is in control is vital.

Organisations also need to decide who can invoke the DR plan, and make sure all the key staff can continue to communicate during an outage. A robust DR test will usually expose any failures in command and control, and crisis communications should be part of the plan for larger businesses.

But there is a need for ongoing communication around DR and business continuity, too.

“Users have a perhaps unrealistic expectation of instant recovery for everything, and it is easy for things to go wrong as pressure mounts,” says Lock.

Clear communications will help manage expectations about which data and systems can be recovered, in which order, and how quickly, adds IDC’s Goodwin.

**DR pitfall 5: Neglecting human factors**

IT departments, naturally enough, focus their DR planning on systems and data. But effective plans need to also cover where and how people will work if the main business location is compromised.

It might be that staff can work from home initially, but how long can they sustain that?

Do some staff need desktop computers, or more bandwidth than domestic or mobile connections can provide? What about meeting spaces, and what about the physical and mental wellbeing of the team? Keeping up morale in the event of a disaster is often as important as the technical aspects of the recovery plan.

**DR pitfall 6: Overlooking the cloud**

Cloud computing is making some aspects of disaster recovery much easier, especially with [the growth of online backup services](https://www.computerweekly.com/feature/SME-disaster-recovery-made-easy-with-cloud-hybrid-and-HCI).

But the cloud can add complexity to IT operations, especially in hybrid and multicloud environments.

Also, there is ability of business lines to spin up their own cloud resources, or to buy software-as-a-service (SaaS) applications, which means IT might no longer have a full picture of the organisation’s IT infrastructure. And does the plan include what to do if a cloud service goes down?

Research by Spiceworks found that just 28% of organisations included cloud or hosted services in their DR plans. And relying on the cloud provider’s own [backup and business continuity plans](https://www.techtarget.com/searchdisasterrecovery/tip/Dont-cut-corners-with-disaster-recovery-and-backup) is not enough.

There might be little the cloud provider can do, for example, if a user accidentally deletes data.

And a partial failure – for example of an onsite data store that serves a cloud-based application – can be harder to recover from than a conventional stack where the data and applications are in the same place.

But thorough testing should show up any weaknesses in recovery plans for cloud infrastructure too.

**4 Major Challenges with Traditional Disaster Recovery**

Every company knows that you need tested backups of your data, and those backups must be kept offsite. What most companies don’t know, however, is that new data-protection and cloud technologies take disaster recovery to the next level. In this chapter, you’ll learn about these new technologies, how they work, and how they will modernize your disaster recovery systems to ensure that your enterprise is prepared when unforeseen disasters, small or large, hit the data center.

## Challenges with Traditional Disaster Recovery

While most companies have a disaster recovery (DR) plan of some type, there are still many companies who don’t have any plan at all. The sad thing about this fact is that, according to the National Archives and Records Administration (NARA) in Washington, D.C., 93% of companies that lost their data center for ten or more days due to a disaster filed for bankruptcy within one year of the disaster. Additionally, 60% of companies that lose their data shut down within six months of the disaster.

Hopefully you aren’t employed by one of the 48% of companies we surveyed that don’t have a plan and, if you are, it’s time to make DR a priority. After all, disasters do happen and many of those disasters aren’t large-scale catastrophes like fire, flood, tornado, or hurricane. Most disasters are much smaller in scope, such as human error, unexpected data corruption (e.g., due to a firmware upgrade on the SAN), or ransomware attacks.

For companies that do have a DR plan, so many of those plans are out of date, using outdated technologies, or both.  
Let’s review the top 4 the challenges that enterprise companies face with traditional disaster recovery.

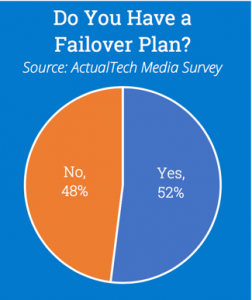
Can your organization survive a disaster? Find out by downloading our eBook: [Top Reasons Why Your Disaster Recovery is Destined to Fail](https://anexinet.com/resources/ebooks/top-reasons-why-your-disaster-recovery-is-destined-to-fail/)

### Challenge #1: Tape and Offsite Storage

The tried-and-true tape backup has been around forever. The great thing about tape storage is that it’s very reliable. The not-so-great thing about tape storage is that tapes are difficult to inventory, they can be easily lost or stolen, and they are time-consuming to test. Additionally, if your company needs fast restoration of applications and data after a disaster, tape storage isn’t going to be able to provide that; tapes must be recalled and restored—all of which takes a significant amount of time.

While offsite tape storage is still a reliable and affordable option for long-term offsite archival and data protection, it’s not the best option available today for disaster recovery, because businesses need better RPOs and RTOs than what tape can provide. Speaking of RPO and RTO, what are they and what are the challenges around them?

### Challenge #2: Meeting RPO / RTO

  
Recovery point objective (RPO) is the minimum amount of data that is acceptable to lose in the event of a disaster. Recovery time objective (RTO) is the amount of time that is acceptable to recover applications in the event of a disaster.

For most companies using tape backup, their RPO is 24 hours (because they do a backup each night) and the RTO might be 48 hours, because that’s how long it would take them to recall the tapes, recover the data, and bring the applications back up.

While that timeframe and amount of data loss might be fine for a small business it’s not going to be acceptable at medium and large enterprises. With thousands of employees working every day, the thought of losing a day’s worth of data (24-hour RPO), and the cost to try to re-create that, is unacceptable.

With a 48-hour RTO, the company could be down as much as two days before all applications are restored. Again, for most companies, that amount of downtime is going to be unacceptable.

Certainly RPO and RTOs can be reduced but that leads to high costs…

### Challenge #3: High Costs

In the past, it’s been widely known that “the shorter the RPO and faster the RTO, the greater the cost of the disaster recovery solution” (in terms of hardware, software, and data transmission); however, that is changing with new DR solutions (which we’ll talk about later in this blog series).

With traditional DR solutions, to obtain short RPOs and fast RTOs, you had to use a SAN with synchronous replication and have dedicated wide area network (WAN) circuits between sites. In most DR designs this required you to have your own secondary data center to send the replicated data to and run your secondary servers and storage in the event of the disaster. Many DR replication solutions were designed just for specific application. When you wanted replication for another application, you had to purchase another replication solution for that app. All this semi-custom disaster recovery technology, plus the monthly bandwidth to support the movement of the data, resulting in a very high cost for a high-quality DR solution. Unfortunately, this put disaster recovery out of the financial reach for many companies.

### Challenge #4: Maintaining the DR Plan / Runbook

Another challenge associated with traditional disaster recovery solutions is that of maintaining the DR plan itself. This plan is the actual runbook, as it’s called, as to the steps that the actual administrators would take in the event of a real disaster. That runbook must include a plan for every application, its associated data, and user connectivity, and the sequential recovery steps for the application. With applications changing and moving at a constant rate in the modern data center, the task of maintaining the disaster recovery runbook has become overwhelming for most companies. The result is that their DR runbook is out of date, and, should a real disaster occur, they would be unable to meet the recovery time objective and maybe be unable to recover at all. This is because their runbook doesn’t provide the necessary information required to get the applications back up and running.

These examples aren’t just the challenges of the past, they are still the disaster recovery challenges faces by most companies today. Continue reading in our next post, [Top 7 Innovations for the Next Phase of Disaster Recovery.](https://www.anexinet.com/blog/top-7-innovations-next-phase-disaster-recovery/)

Finally, if you need help updating any aspect of your company’s disaster recovery plan, or would like to begin the process of adopting a new DR plan, check out our [Disaster Recovery Strategy Kickstart](https://anexinet.com/cloud-hybrid-it/disaster-recovery-strategy/). Our expert consultants will be happy to help keep your company safe.

# Know the 9 Critical Disaster Recovery Scenarios to Test

Disaster recovery testing helps to ensure that businesses can effectively recover from an operational disruption. But knowing which disaster recovery scenarios to test can be tricky, especially when some threats seem to be constantly evolving.

Should you only test for scenarios that affect your IT systems? Only your data backup systems?

What about recovery plans for a pandemic? For example, what if you face staffing shortages, supply-chain disruptions or shelter-in-place orders that require your workers to work remotely?

In truth, there are endless disaster recovery scenarios to test if you want to be 100% prepared for every imaginable situation. But not all businesses have the resources or time for such robust testing. So let’s look at some of the most crucial scenarios to test for.

Which disaster recovery scenarios to test for?

**1) Data loss & backup recovery**

This is one of the most important disaster recovery scenarios to test for. When data loss occurs, it’s vital that your business is able to quickly restore it from a backup. That’s true whether a single file has been deleted or an entire server has failed. If data can’t be restored, then the situation could become a costly nightmare.

So, what exactly do you test?

First and foremost, you want to test that your backups are viable and can be restored. Run tests on both file-level restores and full machine recoveries to ensure that both can be completed in a real-world event.

Some things to consider after this testing:

How long did the recovery take?

Were RTO and RPO objectives met?

What unexpected issues hindered the recovery process, if any?

What improvements could be made to speed up the recovery?

All tests should be well documented. If issues arise that call for changes to the recovery process (including technology deployments, protocols or even the testing scenarios themselves), then the disaster recovery plan should be updated accordingly.

**2) Failed backups**

What happens when a backup can’t be restored? This is a common situation for businesses that rely on traditional incremental backups, because of the data corruption that can occur in the backup chain. So, it’s another important scenario that businesses should test for.

Testing for a failed backup typically involves two types of response:

Troubleshooting the problem to see if the failed backup can be restored (time permitting)

Restoring from another backup

If a secondary backup is available and can be quickly restored, that is usually preferable over spending time trying to “fix” or reconstruct the failed backup.

Restoring from another backup will require its own set of additional testing scenarios.

Example tests:

Recovery from a cloud backup

Bare metal restore

Backup virtualization

Hypervisor restore

Export of backup image

iSCSI Restore

Some data backup systems will of course have additional restore options, such as the Rapid Rollback option on the Datto SIRIS (a feature that lets you undo widespread file changes, such as those caused by ransomware). Since each BC/DR solution is unique, you’ll want to periodically test every possible recovery method to ensure those options are actually usable in a real disaster.

**3) Backup verification testing**

Manually testing your backups is always a good idea, but it also can be time-consuming. Many backup systems now feature automated backup verification / validation checks that make this process more efficient.

The purpose of backup verification is to verify that a backup can actually be restored. It automates the testing process, checking each new backup for signs of data corruption or any other issues that could impede the recovery process.

While verification testing is designed to be automatic, it still requires oversight. Some things to consider:

How often does backup verification occur?

Is it configured properly?

How is a successful verification (or failure) communicated? Is somebody actively reviewing the test results?

What types of issues is the verification looking for? Do you have control over these scans?

4**) Network interruptions & outages**

A prolonged network outage can be just as disruptive as a data-loss event. When the network goes down—or even if a single workstation suddenly can’t connect—IT managers must react quickly.

Testing your preparedness for network interruptions is the best way to ensure that you’ll be able to rapidly resolve issues when they actually occur. There are a variety of network testing tools that can help to simulate common disaster scenarios.

Example tests include:

Testing for unexpected surges in network traffic

Mock tests that replicate the effects of a crippling network attack

Network health testing that identifies potential problems in specific parts of the network

Readiness tests that ensure that IT teams are able to rapidly respond

Remember, these tests should never be limited to just software-based testing. It’s critical that network administrators routinely test these disaster recovery scenarios and actually go through the recovery protocols to ensure that they know exactly what to do during a real disruption.

**5) Hardware failure**

Hardware failure is one of the most common causes of data loss and operational disruptions, but how do you test for it?

Above, we touched on the importance of backup and recovery testing. But that’s specific to the data. How quickly will you be able to repair or replace the bad hardware? The answer largely depends on how well your recovery teams have prepared for this scenario.

What is the process for determining whether hardware can be salvaged or should be replaced?

If replacement is needed, how fast can the new hardware be deployed?

How can disaster recovery planning help to speed up the process? For example, are there vendor relationships that can ensure same-day replacement?

All of these questions relate to processes that should be routinely reviewed and tested. Restoring lost data is only the first part of this disaster scenario. A full recovery of the hardware and associated systems is critical for maintaining business continuity, which is why testing all recovery protocols is so essential.

**6) Utility outages**

Another important disaster recovery scenario to test is a sudden loss of electricity or other utilities. These scenarios are most common during severe weather and other natural disasters, but they can happen for a number of reasons.

Who can forget the NYC blackout in 2019 or the massive 2003 blackout that left large swaths of the Northeast without power?

When these and other everyday brownouts occur, businesses are usually at the mercy of the utility provider to restore power. But that doesn’t mean they can’t do anything. The costs of a power outage can quickly skyrocket, so every attempt should be made to restore operations through other means.

At the first signs of a utility disruption, recovery teams should be quick to work:

Assessing whether the outage is localized to the building or widespread

Communicating with the utility provider to report the outage and get ETAs for resolution

Inspecting backup power sources, if deployed, to ensure they’re working properly

Prioritizing critical services and personnel as it relates to the power limitations of the backup power sources, and/or having teams work remotely if power is available elsewhere

Each one of these protocols should be routinely reviewed and tested to ensure that recovery teams are prepared to act swiftly and know exactly what to do when an outage occurs.

**7) On-site threats & physical dangers**

There are a number of disaster scenarios that can be extremely harmful to your employees and operations—and yet have little to do with your IT systems. This is why disaster recovery testing (and business continuity testing) should not be strictly limited to IT.

What if the business faces an active-shooter situation? How should employees protect themselves? Where do they go for safety?

Testing for different crisis scenarios can greatly reduce the risk of harm to your most valuable asset: your people. And by protecting your employees, you also protect your operations.

Tests to consider:

Evacuation drills for fires, active shooters and other on-site dangers

Emergency procedures for tornados, earthquakes and other sudden natural disasters

Testing the communications systems that will be used to keep employees updated during a prolonged disaster

A fire drill is perhaps the most common form of testing for an on-site emergency and in some areas these drills are required by law for certain types of commercial buildings. However, fires aren’t the only scenario that employees should be prepared for, especially in larger buildings.

Routine training should be conducted to educate employees on how to safely respond to all the on-site dangers identified in your disaster recovery plan. When employees know what to do in an emergency, they are at far less risk of harm. That’s good for their wellbeing of course, but it’s also good for the business.

**8) Workforce interruptions**

What happens when employees can’t make it to work? This could be a situation like COVID-19, in which a viral outbreak forces workers to stay home. Or, it could be a number of other disaster scenarios:

Terrorist activity

Transportation stoppages

Worker strikes

Building damage or structural deficiencies

Prolonged inaccessibility to building due to natural disaster or mandatory evacuations

Whatever the scenario, businesses can face a severe operational disruption if workers aren’t able to do their jobs. So, having a Plan B is essential.

In response to the coronavirus pandemic, businesses rapidly shifted to remote work, but many were unprepared to do so in an effective way. Stressed IT systems caused additional roadblocks and increased cybersecurity risks. Many companies also lacked the tools to streamline their remote workers, which hurt productivity even further.

This is where testing can help deliver far better outcomes. Businesses need to routinely evaluate their preparedness for a sudden workforce interruption and put those protocols to the test. That could involve:

Testing IT systems & platforms that facilitate remote work

Testing the procedures that will help to maintain critical operations

Testing the business’s ability to relocate operations

Essentially, any process or system that will be used in response to a workforce interruption should be tested.

**9) Cybersecurity**

Cybersecurity threats are constantly evolving, so it’s important to test your safeguards on a regular basis. Routine testing helps ensure that your cybersecurity systems will effectively detect and block known threats.

Some of the disaster recovery scenarios listed above will naturally be part of this testing, such as backup validation and network testing. But in addition to those tests, you’ll want to confirm that your cybersecurity systems are solid. This means running tests for not only full-blown cyberattacks, but also the myriad “little” threats that businesses face every day, such as malware infections via web, email and vulnerable software.

A comprehensive cybersecurity testing strategy can include:

Security audit: An extensive review of existing software, hardware and security policies to identify overall cybersecurity strength.

Penetration tests: Mock cyberattacks conducted internally (or by third-party cybersecurity firms) to test whether malware or hackers can penetrate your systems.

Vulnerability assessment: A comprehensive assessment of deployed systems to identify vulnerabilities, gaps and weaknesses, sometimes via routine automated scans.

Social engineering tests: Mock social engineering attacks, such as phishing emails, conducted internally to test how employees respond and how easily they can be deceived by such methods.

In tandem with your cybersecurity training, businesses should conduct routine cybersecurity training for all employees. The objective of this training is to educate all personnel on safe practices for Internet and email. Employees should be trained on how to identify a suspicious email and what to do with it. This training should ideally be conducted for new hires as part of their onboarding process, in addition to yearly training for all employees.

Cybersecurity training is one of the most effective ways to reduce the risk of an attack due to human error.