ITVORTEX
SIMPLIFY. PROTECT. EVOLVE.

FREE RESOURCE · INSTANT DOWNLOAD

Top 10 Disaster Recovery Mistakes.

The failover assumptions that quietly break, and the field test that exposes each one before an outage does it for you. Most DR plans fail not from bad technology, but from confidence in something nobody actually verified.

MISTAKES
10
failover assumptions that quietly break

FIELD TESTS
10
one concrete drill to expose each gap

BUILT FOR
50–500
seat businesses across NJ, NY, CT

SURPRISES LEFT
0
what a tested recovery plan is for

Where recovery quietly fails.

A DR plan you haven't tested is a hypothesis, not a safeguard. These are the ten assumptions we see break most often in mid-market environments. Each one looks fine on paper and on the dashboard. Each one has a field test that turns the assumption into a fact before an outage does.

1 You back up, but you've never tested a restore.

A job that reports success only proves data was written, not that it reads back into a working system. Corrupt media, broken application consistency, and missing dependencies all surface at restore time, which is the worst possible moment to find them.

TEST IT Schedule a full restore of a real workload into an isolated environment every quarter, and time it end to end.

2 Your RPO and RTO are numbers nobody has validated.

Leadership signed off on "four hours" without anyone proving the environment can hit it. Real recovery includes DNS, dependencies, and validation, not just spinning up a VM. The gap between the target and reality is where outages live.

TEST IT Run a timed failover drill and compare actual recovery time and data loss against the numbers on paper.

3 Your DR copy lives in the same failure domain as production.

Replication into the same datacenter, the same SAN, the same power feed, or the same cloud region means one event takes both. Ransomware and regional outages don't respect "it's a separate server."

TEST IT Trace every DR copy to a distinct site, account, and provider, and confirm none shares a fate with production.

4 Your backups aren't immutable, so ransomware encrypts those too.

Attackers hunt down and delete or encrypt reachable backups before they trigger. A backup that an admin credential can modify is a backup an attacker can destroy with that same credential.

TEST IT Confirm at least one copy is immutable or air-gapped, then try to alter it with a privileged account to prove the lock holds.

5 You protect servers but not Microsoft 365 and SaaS.

Microsoft's shared-responsibility model covers the platform, not your data. Retention policies and recycle bins are not backup. A deleted mailbox or a compromised SharePoint site can be gone for good.

TEST IT Stand up a third-party backup of M365 and your other SaaS, then restore one mailbox and one file to prove it works.

The gaps you find in a drill.

6 The runbook lives in one person's head.

When recovery depends on tribal knowledge, the incident that takes out your systems can take out your one expert too, or they're simply unreachable at 2 a.m. Undocumented steps are the ones that get skipped under pressure.

TEST IT Hand the written runbook to someone who has never run it and have them execute a recovery unaided.

7 Nobody is actually watching the backup jobs.

Silent failures stack up for weeks until the night you need the data. A dashboard nobody opens is the same as no monitoring at all.

TEST IT Route job results to an alert that pages a human on failure, then deliberately fail a job to confirm the alert fires.

8 You can recover the data but not the environment.

Restoring files means little if Active Directory, networking, certificates, and licensing aren't in the plan. Applications come back broken, or not at all, without their supporting fabric.

TEST IT In your drill, recover a full application stack rather than just its data, and log in as a real user to confirm it works.

9 The plan assumes the building, and the team, are available.

DR plans written for a single server failure quietly assume people can still reach the office, the network, and each other. A fire, flood, or regional event breaks all three at once.

TEST IT Run one drill assuming the primary site and its network are completely gone, using only out-of-band communications.

10 The plan is a year old and the environment isn't.

New applications, new dependencies, and decommissioned systems turn last year's runbook into fiction. An outdated, untested plan fails at exactly the moment it's needed most.

TEST IT Re-validate the DR plan after every major change, and on a fixed quarterly cadence regardless of changes.

From hoping to knowing.

Every mistake on this list shares one cure: test it before reality does. That's the entire premise of how we build and run recovery for the businesses we protect. Here's where each gap gets designed out instead of discovered the hard way.

Disaster Recovery (DRaaS)
theitvortex.com/disaster-recovery-as-a-service/

Tested failover with validated RPO and RTO, in a separate failure domain from your production.

Backup as a Service (BaaS)
theitvortex.com/veeam-baas-offerings/

Veeam-powered, immutable, and monitored, covering servers, M365, and SaaS against 3-2-1-1-0.

Managed IT Services
theitvortex.com/managed-it-services/

A documented runbook and a team watching every job, so silent failures never become outages.

IT Calculators
theitvortex.com/interactive-it-calculators/

Put real numbers to downtime cost and recovery targets before you set them in a plan.

Talk it through with our team: (201) 225-8670 · www.theitvortex.com

FIND THE GAPS ON YOUR TERMS

Bring this list to a working session with an IT Vortex engineer. We'll run the tests against your environment and tell you which assumptions are holding and which are about to break.

BOOK A DR REVIEW