3PLPERSPECTIVES

November 2026

Common Gaps in Disaster Recovery Plans and How to Fix Them

By Michele Vayle, Renovo

Operations

4 Minute Read



Disaster recovery (DR) planning has become a non-negotiable part of modern IT strategy. Despite widespread awareness of cyberthreats, many 3PL's still struggle to recover effectively when disruption strikes. In fact, organizations with a tested disaster recovery plan are 2.5x more likely to recover quickly than those without one.

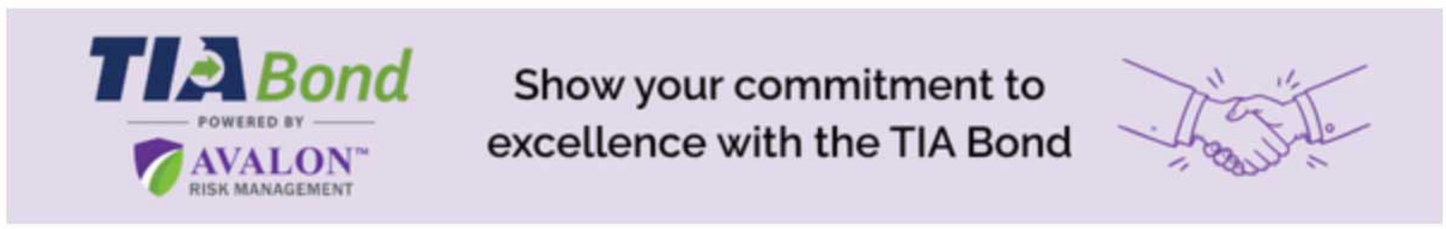
For example...

• 74% of companies that regularly test their plans experience fewer disruptions

• 81% see measurable improvements after testing

• 72% report higher confidence in their recovery capabilities

However, simply having a DR plan isn't enough. Plans must be continuously evaluated, updated, and tested frequently to ensure they remain effective as business operations, infrastructure and third-party dependencies evolve. This is especially important for 3PL's, where critical operations depend on external partners and interconnected software. Without proper planning, a disruption in one system or service can quickly ripple across the business and affect customers, vendors and internal operations.



One of the most common and dangerous gaps in Disaster Recovery Planning is the lack of clearly defined recovery objectives. Many 3PL's claim to have a DR Plan but cannot answer critical questions such as how quickly systems need to be restored, how much data lost is acceptable, which systems are most critical to operations, or which third-party vendors are essential to maintaining business continuity.

To address this, organizations should begin with a comprehensive Business Impact Analysis (BIA) across departments. Validating recovery expectations with leadership, application owners, operational teams, and external partners helps establish clear priorities and rankings of criticality. A proper BIA identifies critical applications and services, operational and vendor dependencies, and the financial and operational impact of downtime. From there, 3PL's can establish measurable Recovery Time Objectives (RTOs), which define how quickly systems can be restored, and Recovery Point Objectives (RPOs), which define how much data loss is acceptable.

> During a disaster, unclear communication, undefined responsibilities, and poor coordination often delay recovery more than the technical issue itself. These risks increase significantly when vendors, managed service providers, and cloud platforms are involved in the recovery process.

Another common misconception is that backup equals recovery. Backups are only one component of a complete disaster recovery strategy. Without a plan for restoring systems, validating data integrity, coordinating failover processes, and minimizing downtime, backups solutions alone provide limited value. This challenge becomes even greater when 3Pl's rely on external providers such as cloud platforms, SaaS applications, or TMS systems for critical operations.

A modern DR strategy should go beyond simply storing backup copies of data. 3PL's should automate backups offsite routinely, verify their integrity, implement immutable and air-gapped backups to protect against ransomware, and use replication for critical systems to reduce downtime. Recovery architecture should align with business recovery expectations, while recovery procedures involving third-party vendors and platforms should be regularly validated. In addition, backup retention strategies should align with operational and compliance requirements, including how long historical data must be retained and whether legacy systems still require recoverability. The goal is not just to preserve data, but to restore operations quickly, reliably, and with minimal disruption.

People and process failures are another major weakness in many DR Plans. During a disaster, unclear communication, undefined responsibilities, and poor coordination often delay recovery more than the technical issue itself. These risks increase significantly when vendors, managed service providers, and cloud platforms are involved in the recovery process.

Common communication issues include undefined responsibilities during an incident, lack of communication planning, single points of failures tied to key individuals, poorly documented vendors or dependencies, or unclear escalation procedures between internal and external teams. Effective DR plans assign responsibilities, outline communication expectations, and define escalation paths for decision-making. Organizations should also review vendor contracts to understand support expectations and service-level agreements, while cross-training employees to reduce dependence on individual personnel. Strong coordination between internal teams and external partners is essential to maintaining operational continuity during an outage.

Perhaps the most damaging gap in disaster recovery planning is the lack of real testing. Many organizations either do not test their plans at all or test far too infrequently. Without testing, there is no reliable way to determine whether recovery procedures will actually work under real- world conditions.

Effective testing should be continuous, measurable, and documented. Organizations should routinely perform backup restoration tests to verify data integrity. They should also measure actual recovery times against established RTO's and RPO's, validate failover procedures involving vendors, document testing results, and continuously refine recovery procedures based on lessons learned. Different forms of testing provide different operational insights. Backup and restore testing validate the speed and accuracy of recovery processes. Tabletop exercises walk teams through incident scenarios to identify procedural gaps. Simulation testing validates responses to cyberattacks or infrastructure outages. Parallel testing restores systems in a test environment while production remains operational. Full interruption testing executes a complete failover scenario to validate end-to-end recovery readiness. Each testing method helps strengthen recovery capabilities and uncover weaknesses before a real disaster occurs.



Closing these gaps requires more than a one-time review of disaster recovery plan. It requires ongoing commitment, regular testing, and continuous improvement. As technology environments become more interconnected the risks associated with downtime can continue to grow.

The organizations that recover most effectively are not necessarily those with the largest IT budgets. They are the ones that clearly define recovery objectives, understand their dependencies, test their plans regularly, and adapt as their business evolves. A disaster recovery plan should be treated as a living process, not a static document. When disruption occurs, preparation and execution often determine the difference between temporary setbacks and a major business interruption.