

Backup isn't enough: Why businesses struggle to recover

You may have backup, but can your business keep running when critical systems go down?



Benefits

To reduce risk, growing businesses must move beyond backup to a complete disaster recovery strategy focused on business continuity.

This requires four key capabilities:

- A clear recovery plan
- Regular testing and validation
- Defined recovery objectives
- Simplicity for lean IT teams

Most growing businesses rely on backup solutions to protect their data. But when disaster strikes, from ransomware, infrastructure failure, or a site outage, backup alone does not ensure the business can continue running.

The real challenge is not if your data is recoverable, but whether your systems, applications, and operations can be up and running quickly enough to meet business expectations. For many, this gap between protection and recovery carries significant risk. While backups may be recoverable, restoring them can still take days or weeks.

Backup creates confidence, but not continuity

Backup enables data to be restored, but assumes infrastructure and systems are still usable. In a real disaster, such as ransomware or physical damage, that assumption breaks down.

For example, after a ransomware attack, IT may not be able to trust the original servers as safe restore targets. Or in the event of physical damage or a site outage, the servers may be unavailable or unusable.

Even if a business purchases new servers, procurement and delivery can take weeks or months.

Meanwhile, customers may have backups but nowhere safe or available to restore them.

Because of this, without a defined and tested disaster recovery solution:

- Employees may be unable to access systems.
- Customers may not be served.
- Revenue generation may stop entirely.
- Vendors may not be able to transact with you.

See how this impacts your business

[Try our recovery and downtime calculator](#)

The impact is significant. Growing businesses can lose **\$5,000–\$100,000 per hour during downtime**, depending on size and industry. Even more concerning, while most businesses believe they are prepared, only **26 percent actually have a formal disaster plan**.¹

Businesses often assume they can recover quickly from backups, but in practice, recovery times and restoration success can differ significantly from expectations. In practice, recovery times and the chance of successful restoration can be quite different from their expectations.

Complexity, ownership, and changing environments

Disaster recovery (DR) is often treated as a secondary IT task, but it can be confusing, expensive, and difficult to manage.

1. Self-managed complexity

Traditional DR approaches require IT teams to own:

- Recovery workflows and runbooks
- Testing and validation
- Failover and failback execution
- Secondary disaster recovery infrastructure and replication

This requires specialized expertise that many teams at lean businesses do not have.

2. Infrequent or incomplete testing

Recovery plans are rarely tested end to end. Testing is often:

- Time-consuming
- Disruptive
- Deprioritized
- Hard to schedule internally

As a result, gaps in recovery processes only surface during outages.

3. Constant business and environmental changes

IT environments evolve continuously:

- New applications and systems
- Infrastructure updates
- Cloud and network changes
- Employee changes, including retirements, turnover, and role changes

Without consistent updates, DR plans quickly become outdated, increasing the risk of DR failures and lost productivity.

4. Unclear ownership and accountability

Whether DR is handled internally or through a third party, responsibility is often fragmented. During an outage, uncertainty around who is in charge can delay recovery and increase the impact on the business.

¹ AlphaCIS, *IT Downtime Costs Small Business: 2026 Guide & Calculator, 2026*; Systech MSP, *What IT Downtime Really Costs*, 2025

Moving beyond backups to tested disaster recovery solutions

To reduce risk, growing businesses must move beyond backup to a complete disaster recovery strategy focused on business continuity. The goal is getting mission-critical systems up and running as quickly as possible.

This requires four steps:

1. A clear disaster recovery plan

Defined workflows that outline:

- What systems are recovered
- In what order
- Within what timeframe and with what recovery time objectives

2. Regular testing and validation

Recovery must be tested in real-world scenarios—not assumed. This pressure tests the recovery plan and ensures it aligns with business priorities.

3. Defined recovery objectives

Businesses need clear targets for:

- Recovery time (RTO)
- Recovery point (RPO)

These targets align IT capabilities with business needs and expectations.

4. Simplicity for lean IT teams

Any recovery solution must be:

- Easy to implement and operate
- Practical for non-specialist IT teams
- Designed to reduce, not increase, operational burden

Ultimately, the goal is not only data recovery, but ensuring the business can continue operating during disruption.

A simpler path to reliable recovery

OpenText bridges the gap between backup and business disaster recovery with our white-glove, fully managed disaster recovery service. We provide the software, cloud, people, monitoring, testing, runbooks, and execution.

Instead of requiring organizations to piece together multiple technologies, vendors, and processes to build a recovery strategy, OpenText provides a more unified and practical approach—one that focuses on simplicity, consistency, and confidence.

At the core of this approach is a fully managed disaster recovery model. With this model, OpenText delivers a fully managed disaster recovery service with all the key components you need to achieve successful disaster recovery outcomes, including:

- **People:** Direct access to disaster recovery experts and support
- **Software:** Proven, real-time replication technology continuously protects critical systems
- **Cloud:** A secure recovery environment where systems can run when primary infrastructure is unavailable

Backup ≠ business continuity

\$5K–\$100K+
downtime cost
per hour

Only 26% have
a formal DR plan

Recovery must be
tested, not assumed

- **Monitoring:** Ongoing visibility into system health and recovery readiness
- **Testing:** Regular validation of recovery processes
- **Runbooks:** Documented and updated recovery plans
- **Execution:** Structured, repeatable recovery processes

Together, these capabilities provide a more consistent and reliable path to recovery without requiring organizations to design, maintain, and coordinate each component themselves.

This is a key distinction.

Most approaches to disaster recovery rely on a mix of software, third parties, and established internal processes. This often introduces complexity, fragmented ownership, and uncertainty during an outage.

OpenText brings these elements together in a unified, fully managed disaster recovery model.

When you work with us, it means:

- **No dependency** on multiple disaster recovery vendors.
- **No ambiguity** around responsibility during an outage.
- **No gaps** between technology, infrastructure, and execution.
- **No reliance** on a single internal employee.

It is not just a collection of tools or a managed overlay. It is a unified disaster recovery model designed to work as one.

This integrated approach also supports the practical realities of lean IT teams. It reduces architectural complexity, streamlines testing, and provides clearer recovery workflows, enabling organizations to achieve their DR outcomes more confidently—without requiring deep specialist expertise or significant operational overhead.

The result is a shift in how organizations think about resilience.

Instead of asking, “Do we have a backup?”

They can confidently answer:

“Can our business still operate while we attempt to restore from backups or get new hardware on site?”

“If restoring from backups takes two days to a week, can we still service customers, keep employees productive, and support vendors?”

OpenText brings software, cloud infrastructure, recovery expertise, and support together in one fully managed disaster recovery solution. Because every layer is designed and operated as a unified service, customers avoid the complexity, coverage gaps, and finger-pointing that come with managing disaster recovery on your own. The result is simpler operations, faster recovery, guaranteed recovery times and executive level confidence in your disaster recovery plan.

Ready to change the way you protect your data? [Contact us](#)