

The Step Most Businesses Skip (and Regret) When It Comes to Data Protection

Opinions expressed by Entrepreneur contributors are their own.

Key Takeaways

- Most businesses invest in backup recovery tools, but fail to actually test them. Testing should occur at least once every year or every three months for critical systems.
- To carry out a successful backup recovery testing plan, start by defining your goal, then test real-world scenarios, set clear success criteria, assign a team and conduct follow-ups.
- Be sure to also conduct an analysis and post-analysis to identify vulnerabilities and improvement points.

Over 67% of businesses suffer from data loss, either because of an attack or mismanagement. Most companies understand the importance of investing in backup recovery tools, but miss the crucial step of actually testing them.

Testing the effectiveness of your backup recovery systems is one of the easiest ways to save your data from being lost forever. This can, at times, mean the difference between survival and failure of the business.

In fact, 93% of small businesses that suffer from consistent data loss go bankrupt within a few years.

Related: 5 Data Backup Mistakes that Could Bankrupt Your Startup (and How to Quickly Fix Them)

The importance of testing backup recovery

Companies spend a lot of money on software, tools and hardware to ensure their data is secure and easy to recover. The idea is to make sure that in case of theft, attacks or other failures, you can always recover your data.

At the same time, no system is 100% fail-proof, and if not tested regularly, your data recovery might fail at the most crucial times. Testing can help identify key failures in your infrastructure. Therefore, it is recommended to test backup recovery at least once every 12 months, across all systems. However, for more critical systems, tests should take place every three months.

Common reasons for backup failures

- If data is not backed up completely, you might encounter corrupted files that have become inaccessible.
- Recovery paths can be misconfigured. This can be due to human error, improper settings or incorrect permissions.
- Some files might be incompatible due to a lack of updates or the use of the wrong software.
- Basic performance issues can also occur. For example, the recovery software crashes, making the backup system redundant.

These are simple problems that can be solved easily, but if these issues are not identified and rectified, the damage can be huge.

Companies invest a lot of money into collecting, maintaining and protecting data. Customer information, inventory logs and trade secrets, if lost, can lead to financial loss, reputational damage and impact a company's competitiveness.

The bottom line is simple – test your backups regularly to ensure your systems are reliable and working when you need them the most.

Plan your backup recovery testing

As a regular business operation, it is important to first design a comprehensive backup recovery testing plan. The idea is to simulate a real-world disaster, test different scenarios and validate recovery systems.

The plan must include:

- **Start by defining aims:** What is the goal of the test? Are you testing software, data integrity, a specific system or the whole company's backup recovery systems?
- **Establish scenarios:** Plan to test real-world scenarios such as ransomware attacks, hardware issues, human error, etc.
- **Define success:** Set clear success criteria – e.g., data integrity, software readiness, recovery time objectives (RTOs) and recovery point objective (RPO) targets.
- **Assign a team:** There should be a set of SOPs and a team designated to carry out regular testing. They will provide a signed report at the end of every test to ensure there is a clear record of findings.
- **Follow-ups:** If failures are detected, there should be an immediate and clear line of action to resolve all issues.

Related: One of the Most Overlooked Risks in Business – and How to Protect Yourself Before It's Too Late

Implementation of the plan

- Conduct testing on planned dates and inform all stakeholders. It's possible that some of the servers or tools might be unavailable, and everyone should be prepared.
- It's important to keep records and logs of every step and outcome with timestamps.
- Record all data integrity issues, faults and errors. Do not ignore them, even if they feel like a non-issue.
- Document the performance of the backup recovery infrastructure. When simulating a real-world scenario, also test human response times.

Conduct an analysis:

- Compare your outcomes and report with the expected RTO/RPO targets.
- Identify vulnerabilities and improvement points.
- A detailed report for each test will provide historical data that can help plan for the future.
- Include insights from across the organization. It is not only the IT sector's responsibility to understand the results. Human errors can happen in any part of the company.

Post analysis:

- Analyze the backup recovery test. Did the process work as planned? Were there internal hindrances? Identify weaknesses in the process and suggest improvements.
- Address faults and vulnerabilities found. How will we make sure they do not happen again? Provide reports and suggestions.
- Aim for continuous improvement. Maintain a core document with logs and test results to give a holistic diagnostic picture of the backup tools.

Related: What Every Business Leader Must Know About Data Management to Avoid a Compliance Nightmare

Common barriers to backup recovery testing

One of the biggest barriers to backup recovery testing comes from within companies. Most managers believe it takes up time and resources that can be better utilized elsewhere. What they fail to understand is that regular testing pays for itself, especially when a real disaster occurs.

Also, having an automated backup recovery does not mean the system is reliable. Backups fail, software crashes, and hardware can malfunction. Automation does not equal reliability.

There is also an impossibility fallacy – a belief among management that since the company has never lost data before, it might not happen at all.

Many assume that it only happens to the largest companies in the world and try to downplay the risk. This “belief” has cost

many companies a lot of money.

Backup recovery testing is a cost-effective way to improve your data security. At the same time, it is important to involve the top leadership and all other stakeholders. This is crucial for progress, accountability and resource allocation. With a bit of time and effort, any organization can protect its data and save itself from financial and compliance issues.

Key Takeaways

- Most businesses invest in backup recovery tools, but fail to actually test them. Testing should occur at least once every year or every three months for critical systems.
- To carry out a successful backup recovery testing plan, start by defining your goal, then test real-world scenarios, set clear success criteria, assign a team and conduct follow-ups.
- Be sure to also conduct an analysis and post-analysis to identify vulnerabilities and improvement points.

Over 67% of businesses suffer from data loss, either because of an attack or mismanagement. Most companies understand the importance of investing in backup recovery tools, but miss the crucial step of actually testing them.

Testing the effectiveness of your backup recovery systems is one of the easiest ways to save your data from being lost forever. This can, at times, mean the difference between survival and failure of the business.

The rest of this article is locked.

Join Entrepreneur+ today for access.

<https://www.entrepreneur.com/science-technology/how-to-ensure-your-data-backup-recovery-system-doesnt-fail/498233>