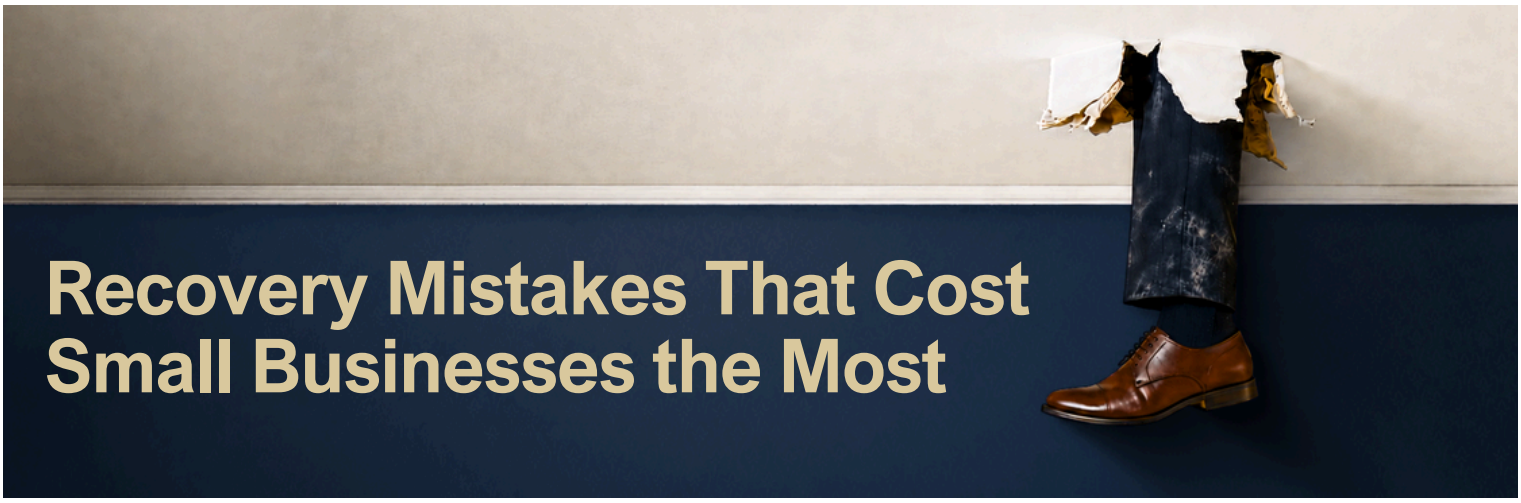
September 2026

Moonshot Insider

Insider Tips To Make Your Business Run Faster, Easier and More Profitably



Recovery Mistakes That Cost Small Businesses the Most

No business can prevent every disruption, but a handful of common mistakes can turn what should be a fast recovery into a prolonged, costly one. The good news is that every single one of them is fixable long before an incident strikes. Recognizing what they are and acting on them early is the first step toward ensuring your business is never caught unprepared.

Keep an eye out for these gaps that look small during normal operations but become expensive during recovery. The sooner you spot them, the easier it is to fix them before pressure, downtime and confusion make every decision harder.

MISTAKE 1: ASSUMING BACKUPS ARE ENOUGH

Backups help you get your data back, but they don't explain what happens next. Your team needs to know which systems come online first, who's responsible and how long it should take.

Recommendation:
Create a recovery plan showing what needs to be restored, in what order and by whom.

MISTAKE 2: NEVER TESTING THE RECOVERY PLAN

A plan that's never been tested is a gamble. Testing reveals gaps while there's still time to fix them.

Recommendation:
Run the plan at least once a year. Treat every surprise as something urgent to fix.

MISTAKE 3: NOT DEFINING ROLES

When a disruption hits, decisions need to happen fast. If responsibilities aren't clear, your team loses time figuring out who's in charge.

Recommendation:
Assign roles before an incident. Each person should know what they own and when to escalate.

MISTAKE 4: FORGETTING ABOUT COMMUNICATION

Employees need to know what to do, customers need to know what to expect and vendors may need to adjust. When normal tools go down, confusion spreads without communication.

Recommendation:
Build a communication plan with backup channels and assign someone to own the updates.

MISTAKE 5: TREATING RECOVERY PLANNING AS A ONE-TIME TASK

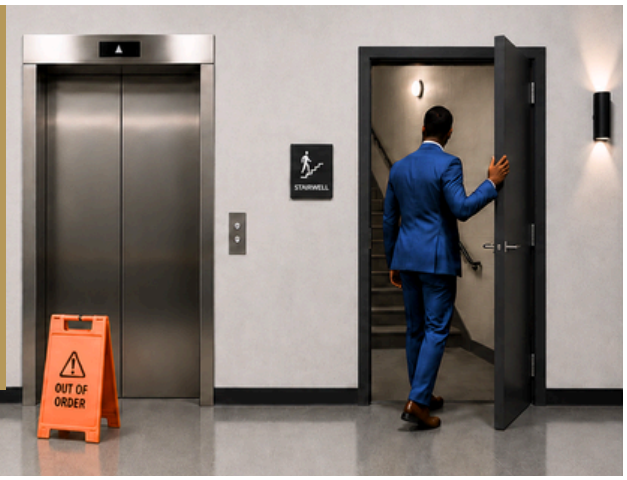
Plans quickly become outdated. Employees leave, systems change and priorities shift. Old contacts or retired systems in the plan slow recovery instead of helping it.

Recommendation:
Review and update the plan after any significant changes to your team, systems or vendors.

Key Takeaway:
Most recovery failures trace back to five avoidable mistakes. Fix them before an incident, not during one.

The Most Common Business Disruptions

and How to Prepare for Them



Most business disruptions don't come with warning sirens. Sometimes it's a Monday morning when the internet is down and no one can access customer records. Or a key employee is out and the only person who knows how to run payroll isn't available. Or someone deletes a wrong file and a backup nobody has tested in months turns out to be useless. The disruptions may not look like disasters at first, but they stop work, delay customer service and leave your team scrambling for answers.

Here's a look at the most common disruptions businesses like yours face and the steps you can take to mitigate the impact before they happen.

1. CYBERATTACKS AND RANSOMWARE

Cyberattacks and ransomware can block access to the files and systems your team depends on, slowing daily work and making it harder to serve customers.

Preparation starts with an incident response plan, tested backups and employee training in spotting suspicious links. These three things keep the door closed before a cybercriminal finds it.

2. HARDWARE AND SOFTWARE FAILURES

Devices, applications and systems can fail without warning.

The best way to prepare is by making sure data is backed up regularly, recovery steps are documented so your team knows what to do first and backups are tested before something goes wrong.

3. HUMAN ERROR

A deleted file, a misdirected email or a changed setting can halt work when there's no clear way to fix it.

Limiting employee access to only what their role requires reduces exposure. Documented recovery steps and regular training on handling sensitive data help your team respond quickly and correctly when a mistake happens.

4. INTERNET OR CLOUD SERVICE OUTAGES

When a connection drops, your team can lose access to customer records, communication tools and key systems all at once.

Have a backup internet connection or mobile hotspot ready, know which tasks can still run offline and set a clear communication plan to keep your team and customers informed.

5. SEVERE WEATHER AND NATURAL DISASTERS

Storms, floods and power outages can shut down operations for hours or days, especially when backup systems weren't in place prior to the event.

Enabling remote work beforehand, storing backups offsite or in the cloud, and having a documented continuity plan means your team can keep operating even when the office is inaccessible.

6. KEY EMPLOYEE UNAVAILABILITY

If the only person who knows how to run payroll or manage a vendor account is suddenly unavailable, work stalls even when everything else is running.

Documenting critical processes, cross-training team members and storing credentials in a secure shared system means the business keeps moving even when that person isn't available.

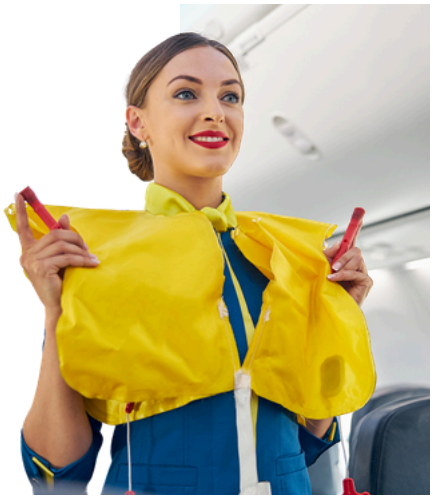
BUILD THE PLAN BEFORE YOU NEED IT

What all of these scenarios have in common is simple: The sooner you prepare for these risks, the less likely they are to disrupt your business.

Key Takeaway:

Every disruption has a fix. Document your plan, test backups, assign roles and train your team.

6 Things Every Incident Response Plan Needs



Most businesses hope they'll never face a major disruption. But hope isn't what determines how well a business recovers. Preparation does. An incident response plan gives your team a clear path: who does what, in what order and what comes next.

Here are the six things every incident response plan should include.

1. ROLES AND RESPONSIBILITIES

When a disruption hits, confusion can slow down recovery. Even capable teams lose valuable time when ownership isn't clearly established beforehand.

Your plan should define who makes decisions, who communicates with employees, who works with IT contacts, and who handles customer and vendor updates. Without this clarity, multiple people may step into the same role while other tasks go ignored. That creates overlap in some areas and serious gaps in others.

When roles are defined upfront, decisions don't stall and communication stays consistent. Each person understands their responsibility and can act without waiting for approval or direction.

2. EMERGENCY CONTACT INFORMATION

In the middle of an incident, small delays add up fast. Searching for contact details or confirming who to call wastes time your team doesn't have.

Your plan should include contacts for internal leadership, IT support, software vendors, cyber insurance providers, legal counsel and key business partners.

This information needs to stay accurate and easy to access. A missing vendor contact or an outdated number can slow recovery at a critical moment.

Keeping everything in one place removes friction. Your team makes the call immediately rather than tracking someone down first.

3. COMMUNICATION PROCEDURES

Communication tends to break down when systems go offline. Email, chat tools and internal platforms may not be available when you need them most.

A strong plan outlines internal communication methods, employee notification procedures, customer communication expectations and vendor processes. This ensures updates continueeven when primary tools fail.

GADGET OF THE MONTH

A Monitor That Works Smarter:

Benq RD280UG

Some upgrades don't transform the way you work. They simply make every day a little easier. The BenQ RD280UG's taller 3:2 display fits more on screen, so you spend less time scrolling and switching windows. USB-C connectivity, built-in eye care features and an anti-glare display make long workdays more comfortable. It's a thoughtful upgrade that helps you stay focused without adding complexity to your workspace.

The Essential Disaster Recovery Checklist

How prepared is your business?

Your people: Contacts are clear, roles are defined and key team members know the plan.

Your plan: Recovery steps are documented, critical systems are identified and updates happen regularly.

Your technology: Data is backed up, restores are tested and recovery timeframes are acceptable.

Your readiness: Procedures are practiced, outage communication is planned and preparedness gaps are reviewed.

The more items you have covered, the better prepared your business is.

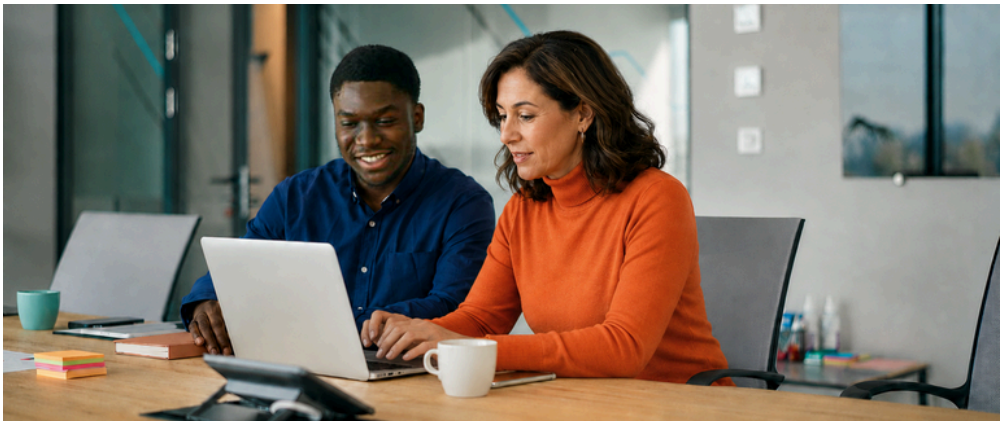
Your team knows alternative ways to stay connected, and leadership can keep everyone informed without delay.

It also sets expectations externally. Customers and partners hear from you at the right time with clear, consistent messaging instead of inconsistent updates or radio silence.

5. RECOVERY PROCEDURES

During an incident, people need direction they can follow immediately. Unclear steps lead to hesitation, miscommunication and wasted effort.

Your plan should outline initial response actions, escalation procedures, recovery priorities and decision-making processes. These don't need to be overly technical. They just need to give teams enough clarity to know their next step. A planned response reduces errors and helps every team member act confidently under pressure.



6. TESTING AND REVIEW SCHEDULE

A plan only works if it reflects how your business currently operates. Changes in systems, vendors or team structure can make parts of it outdated quickly.

Test the plan at least annually, update contact information regularly and evaluate lessons after every test or incident.

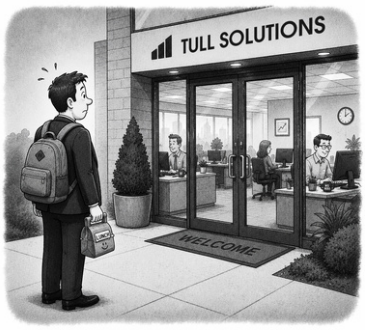
Testing shows how the plan performs under real conditions and gives your team a chance to practice their roles well before something forces them to.

.....

Key Takeaway:

Six elements: clear roles, updated contacts, communication procedures, system priorities, recovery steps and a testing schedule, separate a plan that holds under pressure from one that doesn't.

Cartoon of the month



"First day jitters never really go away."

COMING NEXT MONTH

CYBER MYTHS DEBUNKED

Next month, we'll address today's most common cybersecurity misconceptions to help you implement stronger security practices and protect your business from AI-powered phishing scams, insider threats and more.