

All About...

Business Interrupted: The Unexpected Disaster Your IT Provider Should Be Planning For

Power outages, cyberattacks, hardware failures and natural disasters rarely arrive with a warning, and when they hit, the impact on small businesses can be devastating. Many assume that having a backup is enough, but the truth is, restoring a file isn't the same as staying operational. If you can't access systems, support remote work or keep your team and clients in the loop, even a short disruption can turn into a long-term setback. A reliable IT partner should prepare you for these moments – not just with backups, but with a complete plan to keep your business running no matter what.

Backups Aren't Enough – You Need Continuity

Let's be clear: backups are essential. But they're only part of the equation. What you need is a business continuity plan, a proactive strategy that ensures you can continue operations during and after a major disruption.

When your systems go down, files become inaccessible or your office is compromised, a backup file on a local server doesn't help much. Without a clear plan to restore operations quickly, you risk major losses in revenue, reputation and compliance.

Backups vs. Business Continuity: Know the Difference

Here's where many businesses go wrong:

- **Backups** help you restore data
- **Continuity** helps you stay operational, no matter what happens

A strong continuity plan answers key questions like:

- How fast can we recover?
- Where can the team work if the office is inaccessible?
- Which systems are mission-critical?
- Who's responsible for activating the recovery plan?

It also includes essential components like:

- Encrypted, off-site and immutable backups

- Prioritized recovery timelines (RTO/RPO)
- Remote work readiness
- Redundant systems and failovers
- Regular disaster simulation testing

If your IT provider can't walk you through these points confidently, you're not protected, you're just lucky so far.

Will This Actually Happen To Me?

This isn't just a theoretical warning we're using to "scare" you into a business continuity plan. These are real disasters with real consequences. In recent years:

- **Florida** hurricanes displaced hundreds of businesses, leaving those without cloud access completely paralyzed
- **North Carolina** flooding destroyed on-site servers, erasing months of records and invoices
- **California** wildfires leveled entire office buildings in the Pacific Palisades, many with no off-site recovery in place
- And countless small businesses hit by **ransomware** have learned the hard way that their backups were corrupted or never tested

Disasters don't just hit enterprise-level organizations, they hit businesses like yours every day.

You Should Be Asking These Questions Right Now

If disaster strikes tomorrow, will your business be able to keep going?

Ask your IT provider:

- If ransomware hits, how fast can we recover?
- Are our backups tested regularly, and what systems are included?
- What's the plan if a flood or fire takes out our office?
- Is our continuity plan compliant with industry regulations?
- Can we keep serving clients if our team has to work remotely?

If you're not 100% confident in the answers, you may already be at risk.

Disasters Happen. Downtime Doesn't Have To.

You can't stop every power outage, storm or cyberattack, but you *can* control your response.

A good IT provider helps you recover.

A great one makes sure you never skip a beat.

Want to find out where your business stands?

Click here to book your [Network Assessment](#) now and let's make sure a disaster never turns into downtime.

Questions? Call our Glenside, PA office today at 267-699-2551. Or visit us on the web at AOR-ITS.com to learn more about our proven managed IT solutions, including cybersecurity, for small local businesses.