Top Business Continuity & Disaster Recovery Mistakes

AND HOW TO AVOID THEM!

Tekie Geek

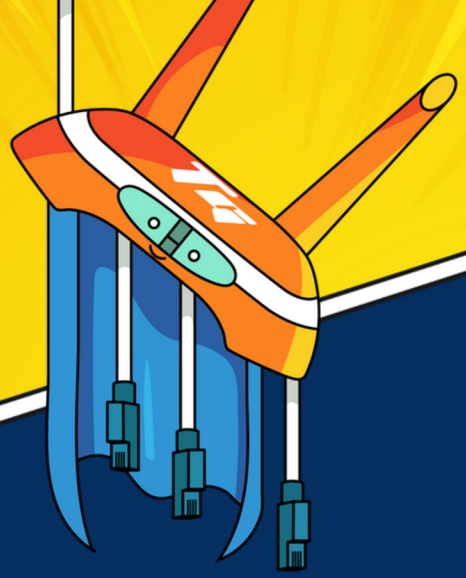


TABLE OF CONTENTS

WHY CONTINUITY MATTERS MORE THAN EVER

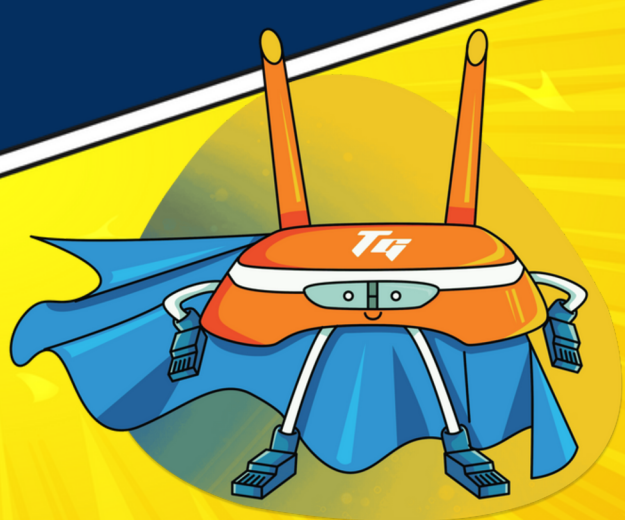
Power outages, cyberattacks, software glitches—business disruptions come in many forms. And when they strike, the impact can be immediate: halted operations, lost revenue, shaken customer trust, and damage to your reputation.

The good news? You don't have to be a tech guru to protect your business. What you do need is a clear, practical plan that keeps you in control when things don't go according to script.

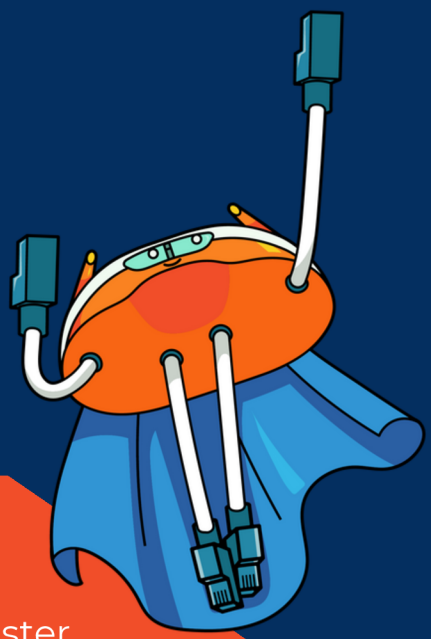
That's where a Business Continuity and Disaster Recovery (BCDR) plan comes in. Think of it as your playbook for resilience — guiding your team through challenges so you can minimize downtime, protect your reputation, and get back to business faster.

In this eBook, we'll explore the most common BCDR mistakes and, more importantly, how to avoid them. You'll discover how to identify hidden gaps, dodge costly downtime, and build a continuity strategy that's both practical and tested.

Because when the unexpected happens — and it will — the difference between chaos and confidence comes down to how well you've prepared.



Mistake #1:
SKIPPING THE IMPACT CHECK



THE PROBLEM

One of the biggest mistakes businesses make is diving into disaster planning without gathering the facts first. If you don't identify your critical functions, dependencies, and recovery priorities, you're essentially planning in the dark.

Without a simple Business Impact Analysis (BIA), it's easy to misalign priorities, waste resources, and end up with a recovery plan that fails when you need it most.

THE SOLUTION

A BIA shines a light on what matters most. With a clear view of your priorities, you can design a recovery plan that protects the essentials, aligns resources effectively, and actually works when disruption strikes. That clarity builds confidence — because you'll know your business is prepared for whatever comes next.

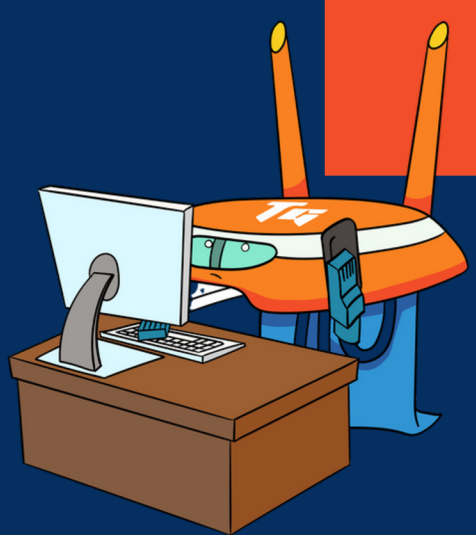
Mistake #2:
TREATING CONTINUITY LIKE JUST AN IT JOB

THE PROBLEM

BCDR isn't just about servers and data. Ignoring departments like HR, finance, and customer support leaves gaps and confusion when disruption hits.

THE SOLUTION

BCDR works best when it's a team effort. Make it clear that continuity is everyone's responsibility — not just IT's. Involve leaders from finance, HR, operations, and other departments in both planning and testing.



Mistake #3:
TRUSTING BACKUPS AS YOUR ONLY SAFETY NET

THE PROBLEM

Some businesses assume that backing up their data is enough. While backups are a critical part of disaster recovery, they won't keep your business running during a crisis.

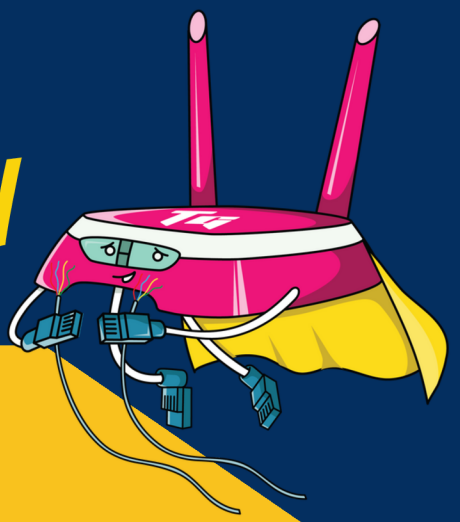
THE SOLUTION

Backups should support a full recovery plan. Ask:

- Where are they stored, and how do you access them?
- How fast can systems be restored?
- Does your team know the steps?

A tested plan covering people, processes, systems, and timelines turns backups into real business protection.

Mistake #4:
FAILING TO TEST THE PLAN



THE PROBLEM

Building a BCDR plan is only half the job. If it's never tested, you don't know if it will work when a crisis hits. Too often, businesses assume that "having a plan" equals readiness — but in reality, untested plans often break down when speed and clarity are most needed. What looks solid on paper may hide flaws that jeopardize the entire recovery effort.

THE SOLUTION

Run regular mock tests with the people who would respond in a real event. These drills reveal weaknesses, clarify responsibilities, and prepare your team to act under pressure. Start with simple scenarios:

- What happens if the network crashes right now?
- How quickly can you switch to backups?
- Who will communicate with clients and stakeholders?

By practicing before disaster strikes, your team gains confidence, reduces confusion, and ensures your plan delivers when it matters most.

Mistake #5:
LETTING YOUR STRATEGY COLLECT DUST

THE PROBLEM

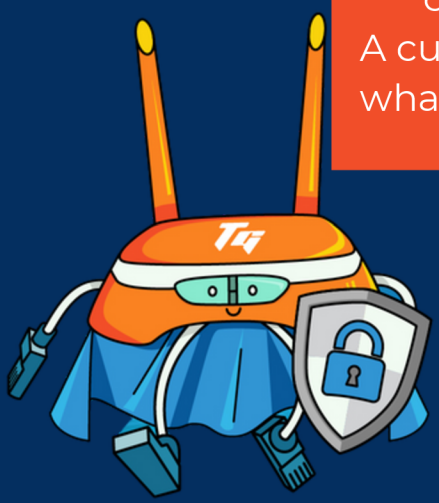
Businesses change constantly—new systems, new vendors, new team members. If your BCDR plan doesn't keep pace, it leaves dangerous gaps. An outdated plan can slow recovery, confuse responsibilities, and put operations at greater risk when disaster strikes.

THE SOLUTION

Keep your plan fresh and aligned with your business:

- Review at least once a year (or more if big changes occur).
- Update for new hires, software, and vendors.
- Ensure quick access so the plan can be used immediately in a crisis.

A current, well-maintained plan ensures your team knows exactly what to do when disruptions hit.

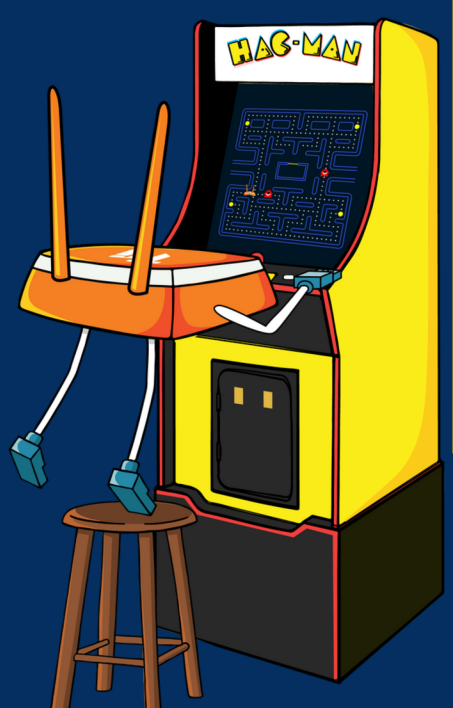


Mistake #6:

IGNORING THIRD-PARTY WEAK LINKS

THE PROBLEM

Most businesses depend heavily on third-party vendors — from internet providers to logistics partners. But if those vendors experience outages, disasters, or delays, your business feels the impact too. Even if the disruption isn't your fault, the fallout still affects you: frustrated customers, downtime, and lost revenue.

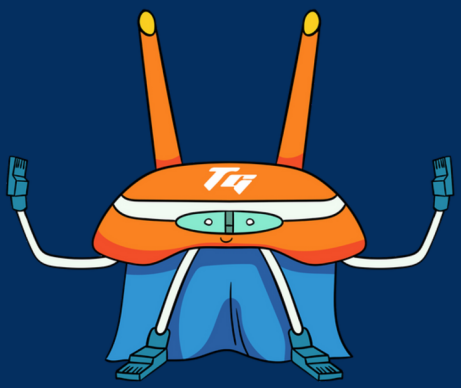


THE SOLUTION

Account for vendor and supplier risks in your BCDR plan:

- Evaluate vendor reliability and review their continuity practices.
- Identify dependencies — know which business functions would be disrupted if a partner goes offline.
- Have backup options for critical services like internet, shipping, and cloud providers.
- Review contracts to ensure response times and responsibilities are clear.

By planning for third-party risks, you protect your operations from problems that start outside your business but hit you directly.



Mistake #7:

NOT ASSIGNING CLEAR LEADERSHIP

THE PROBLEM

The worst time to ask “Who’s in charge?” is during a crisis. Without clearly defined roles, confusion stalls decisions, delays recovery, and increases downtime costs. What could have been a manageable disruption can quickly spiral into a major setback.

THE SOLUTION

Strong BCDR planning assigns leadership and roles before disaster strikes:

- Response lead – designate who takes charge.
- Responsibilities – clarify what each person must handle.
- Documentation – put it in writing, share it, and test it with drills.

When everyone knows their role, your response is faster, smoother, and far more effective.

Mistake #8:
BREAKING DOWN ON COMMUNICATION

THE PROBLEM

Even the best recovery plan can fall apart if communication fails. During a disruption, unclear messages, missing updates, or mixed signals cause panic, delay decisions, and frustrate customers. Poor communication can end up doing more damage than the disaster itself.

THE SOLUTION

Build communication into your BCDR plan:

- Define communication channels – email, phone, messaging apps, or all of the above.
- Assign a spokesperson – designate who updates employees, clients, and partners.
- Create message templates – save time and reduce confusion in a crisis.
- Test your process – run drills to ensure messages flow quickly and clearly.

Clear, consistent communication keeps everyone aligned and builds trust when your business needs it most.

BUILDING A CONTINUITY PLAN THAT ACTUALLY WORKS

Disasters, outages, and **cyberattacks** aren't a matter of if — they're a matter of when. The difference between businesses that bounce back and those that don't often comes down to **preparation**.

Avoiding these **common mistakes** means your **continuity** and **recovery plan** is more than words on paper — it's a practical, tested strategy that keeps your people, systems, and customers **protected**.

At **Tekie Geek**, we help **businesses design** and **maintain** BCDR strategies that work in the **real world.** From identifying critical functions to testing recovery plans and managing vendor risks, our team makes sure you're covered from every angle.

Don't wait until a disruption exposes the gaps. Partner with **Tekie Geek** today and give your business the resilience it needs to thrive — **no matter what comes your way.**