

EBOOK

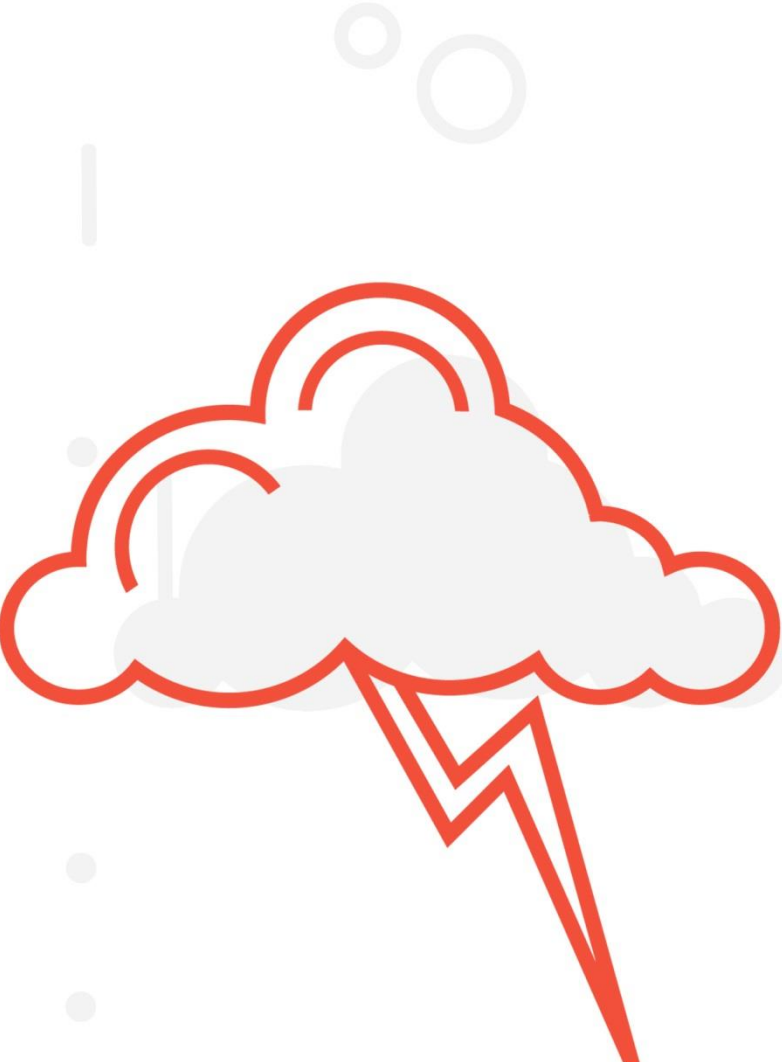
---



# 5 Tips to Ensure Your Business Continuity

Before, during and after a disaster.





Disaster recovery and business continuity planning is critical to keep your business running. However, many just “wing it,” hoping a disaster will never happen. When it comes to disasters (natural or manmade) It’s not a matter of “if” but “when.” If you don’t plan ahead, it can cost you time, money, customers, and ultimately your livelihood.

You may think your business can survive a disaster if you just backup your data.  
*You're wrong.*

Data is essential, but you need so much more to ensure your business can continue operating when:

- Your building is flooded
- Your employees are stuck at home without power
- You don't know how to reach them

You must think about your business as a whole in order to ensure Business Continuity after a disaster. But there’s so much to think about.

***Where do you begin?***

# With the 5 Tips We Share Here.

## 1. Develop a communication plan in advance.

*How will you ensure employees are safe during and after the disaster?*

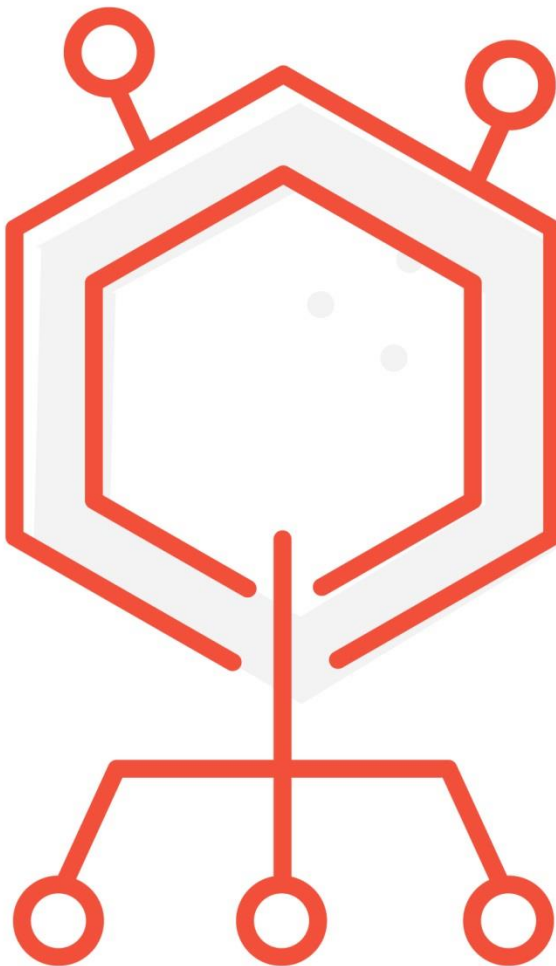
*How will you communicate essential information to employees following the event?*

Email is the easiest way to reach employees, but if your email server is down, this won't help. In this instance, a phone or text chain is a good way to distribute important information to employees during and following a disastrous event.

First, make sure all your contact information for employees is up to date. Designate one employee as the first caller. (Make sure you have a backup person in case this employee is injured or otherwise unavailable). From there, each employee called should call another on the list (as designated in your chain) until everyone is reached.

You can also set up automated emergency calls via communications software/services.

Emergency communications should be as brief and helpful as possible. And be sure to test your plan on a regular basis, much like you would a fire drill in your office.



An illustration in red and grey outlines. At the top left, a person stands at a whiteboard, pointing at it. Below the whiteboard, another person is seated, facing the presenter. In the bottom left corner, there are two interlocking gears of different sizes. At the very bottom center, there is a small grey cross-like symbol.

## 2. Keep your clients and customers informed.

This is critical to the ongoing success of your business, as well as your good reputation. If you're forced to "shut your doors" you need to let them know. Depending upon your particular business, this might require direct communication via messaging, or a mass-media message online.

You will also need to plan for incoming communications following a disruption. Your response (or not) to your customers' needs following an event will have an impact on reputation. It's important that you respond as quickly as possible, and explain how you'll resolve their issues. Develop a plan to send a clear and consistent message. Pre-scripted messages are helpful in this case.

Consider setting up redundant phone lines/services, hosted PBX systems, cloud-based email, or redundant Exchange servers, etc. to ensure you can reach your customers. Or invest in a secondary call center, temporary workplaces, or mobile data centers to manage inbound and outbound communications.

Whatever system you use, be sure to test it often to identify and resolve weaknesses.



### 3. Are You Ready for An IT Disaster?

No matter what kind of business or organization you run, you need effective and secure technologies to access, process and share information. You may believe that you're doing everything possible to ensure your IT is up to date, stored securely offsite, and is on hand when you need it. But are you really doing everything you can do to ensure your business survives an IT disaster?

**How long can you survive without your data?** You should determine how long your business can operate without access to your data. Most businesses won't be able to do this for more than a day or two without feeling a financial pinch. Be ready and have a disaster plan of action in place that your employees understand and can follow. This may mean that you need to set up a secondary work site where your staff can relocate if your primary site is unusable.

**Have you addressed change management as a part of your mission-critical recovery objectives?** Mission-critical applications change frequently. To ensure they can be restored in a timely fashion, you must conduct ongoing tests to ensure their availability. Most importantly, you must ensure your daily management tasks are in tune with your production demands. Change is constant, and you must properly record these changes at your recovery site. Without this, your current procedures will be out of sync with your recovery capabilities.



### **Have you recently updated your “run book” in regard to disaster recovery?**

Your run book is a set of defined procedures for maintaining the operations of your network. It contains all the information your employees need to perform their daily operations. Procedures defined in your run book include those for starting and stopping the system, instructions for handling special devices, how to perform backups and recovery, and more. Step-by-step recovery procedures are a critical component of your run book and should be updated and vetted regularly.

### **Have you tested your disaster-recovery capabilities and ability to failback?**

Failback and failover are critical to any disaster recovery plan. The failover operation switches production to your backup facility. Failback returns production to your original location after a disaster, and saves specific data to cover any lapses. It's imperative that these procedures are tested regularly, documented and controlled. Plus, be sure that you have the bandwidth in place to be fully recoverable.

The good news is that today's data-protection technologies have greatly improved the IT piece of business continuity and disaster recovery. There's a wide array of solutions your IT professional can provide to ensure you have everything in place before a disaster hits, and you can recover afterwards.





## 4. Continue Operating However Possible.

IT downtime is only one factor that can impact your business continuity. There are many considerations depending upon the size and type of your business.

### **Your Facilities — Make sure you have:**

- Generators to power essential equipment
- Uninterruptible power supply systems for essential servers
- Surge-protection systems
- Alarm/intercom systems to alert employees of emergencies, and notify you if someone tries to break into your site if you must abandon it.

**Insurance** — The proper Insurance is essential in your recovery effort. Select the proper insurance coverage for your business' unique needs. Document all your business insurance information such as plan numbers, insurance agent/company contact information, online login information, how to file for claims, and more.

**Training** — Identify essential and non-essential employees beforehand. Essential employees might be doctors, nurses, executives, department managers, and IT staff — Whoever you'll need to keep critical operations up and running. Define business continuity roles and responsibilities. And be sure to cross-train employees on essential tasks, if an essential employee is unavailable following the event.





## *5. Test, Test and Re-Test*

As mentioned, it's essential to test your business continuity/disaster recovery plans. Testing is the only way to reveal gaps in your plans and address them proactively — not while you are frantically trying to pull the pieces back together after heavy rains deposited a foot of water in your lobby!



**For more information, or help to develop your IT Business Continuity/Disaster Recovery Plan, contact Pegas Technology Solutions at 207-835-4053 or [sales@pegas.io](mailto:sales@pegas.io).**