SMARTER TECH FOR AMBITIOUS BUSINESS

PLAN YOUR BUSINESS CONTINUITY

A guide to keeping your business operational through a disaster

Introduction

You're busy running your business but what if something big happens to interrupt your operations? How much you've prepared for an event like this could make all the difference. Could you still serve clients, protection your reputation and ensure the safety of your team?

We've developed this guide for business owners and managers. It covers the four essentials every SMB needs to prepare a business continuity plan (BCP).

Whether faced with a natural disaster, an IT failure, or anything in between, a well-structured BCP provides you with the roadmap to navigate these challenges, minimise downtime, and protect your revenue and reputation.

Our goal? To help you to create a BCP tailored to your unique needs. It doesn't need to be incredibly detailed or lengthy. But in a time of need it will provide resilience to disaster and get you back to normal operations quickly.

Let's get started...

Prioritise employees

Your people are the lifeblood of your operations so prioritising their safety and communicating with them is your priority.

This section of your plan should address two things:

- Establish how the company will ensure employee safety during a disaster.
- Document how the company will communicate with employees in the hours, days and sometimes weeks after the event.

The first part hinges on your business's nature and location. Safety planning for a large manufacturing operation will differ significantly from a small real estate office. There's no one-size-fits-all solution.

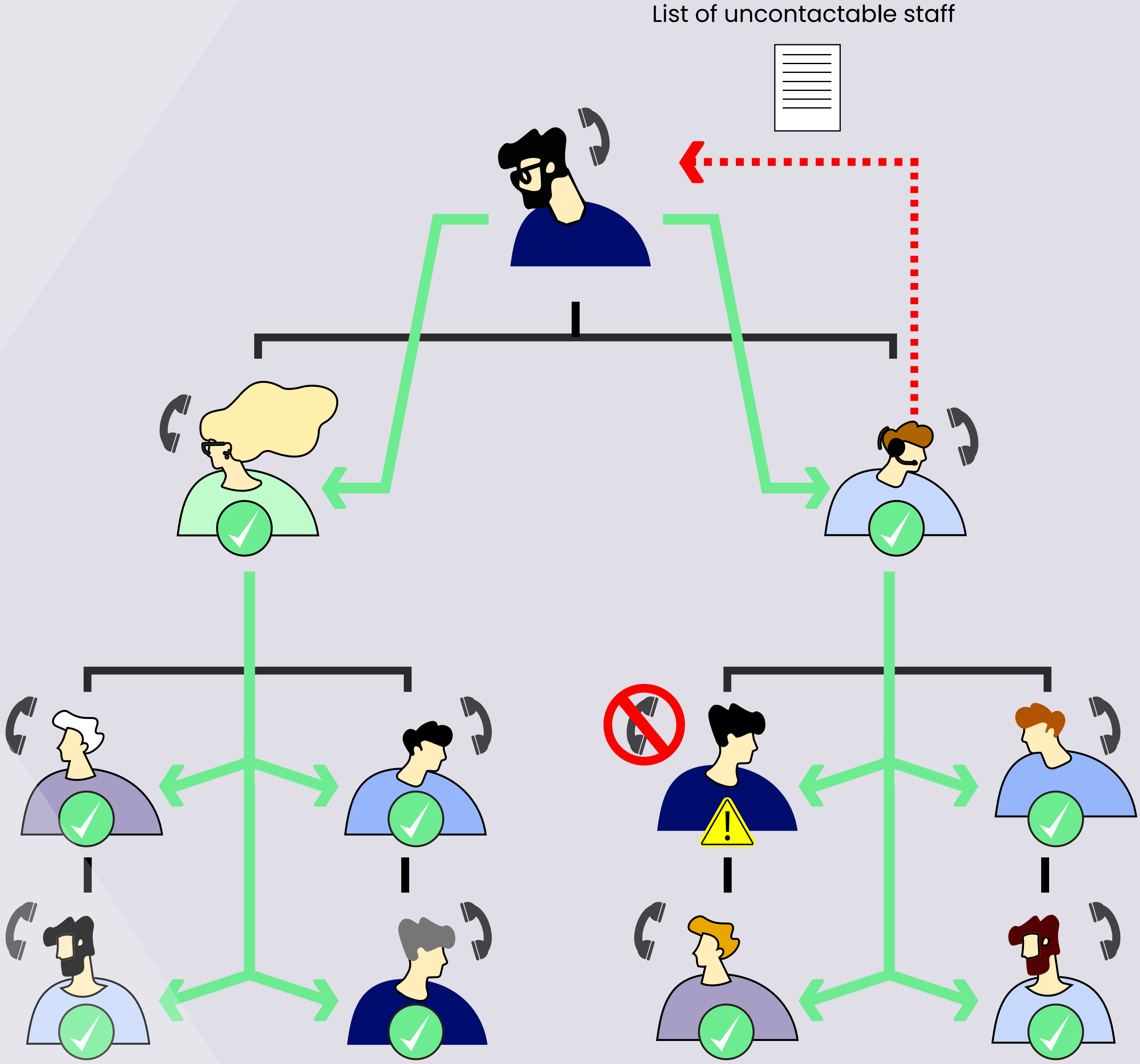
The second part requires collecting and securely storing your employee information, ensuring it's well-documented, easily accessible and kept in multiple secure locations that your key people can access. This includes up-to-date employee contact details (email, mobile and home phone numbers, emergency contacts) and a protocol for reaching out to them.

Reliable communication

Sending an all-hands email may be the first tactic you'd think of in your disaster scenario planning. But what if the email server is compromised or offline, or your team don't have access to emails?

Consider a call tree. Also known as a phone tree, call list, phone or text chain, here's how it works: A predetermined employee initiates the call chain with a call to the next person on the chain. That employee contacts the next person on the list and the chain continues until everyone on the call tree has been reached.

Call Tree Process



Do these 3 things to ensure your employee communication plan is reliable...

1

Ensure the plan is comprehensive, executable by those nominated in the plan, and flexible to accommodate various potential emergencies.

2

Communications should be brief, accurate, and, depending on your organisation's structure, may be disseminated through managers to their direct reports based on a "need-to-know" basis.

3

Review and update the communication plan regularly. Reviews will expose any gaps, like outdated employee lists or contact information.

Maintain clear customer communication

With your employees safe and up-to-speed, your attention should quickly turn to your customers.

Create a plan for delivering information to your customers during and after a disaster so they know what they can reasonably expect from you while the business recovers. The extent of your customer communication plan will vary based on your business type.

If an incident is likely to impact customers, it's crucial to detail the problem and your mitigation steps. This could mean direct customer communication and/or posting updates on social media.

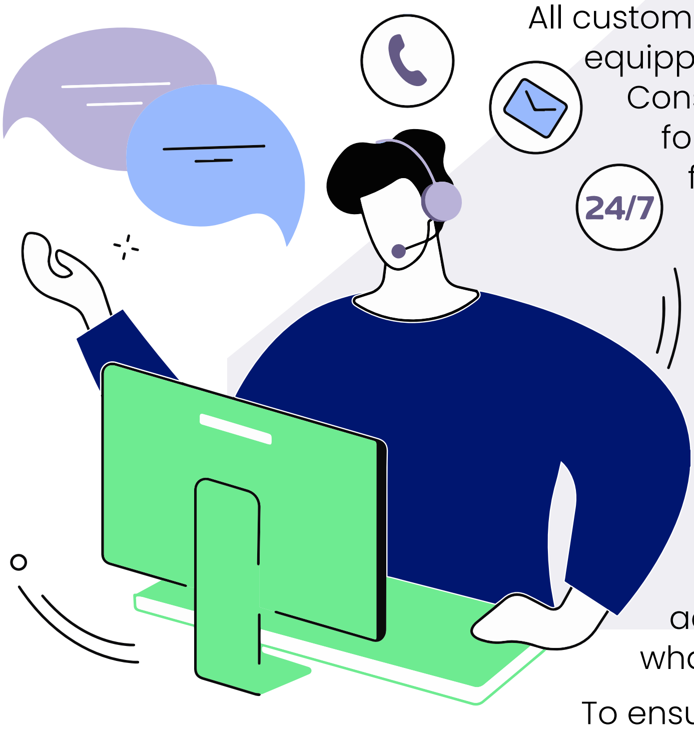
Post-disruption, you may have to manage a surge of incoming communications, possibly involving support requests, a flood of emails and calls, upset customers on social media, and possibly media interest. Your organisation's ability to jump in and address customer needs post-event will have an impact on your reputation.

Preserving reputation

How do you safeguard your reputation? With preparation and readiness. Have a plan that addresses who, how, when and what will be communicated. Your customers won't need every last detail about the disaster that's hit your business, but they'll want to know how it's impacting them and what steps you're taking to minimise those impacts.

All customer-facing staff should be briefed and equipped to deliver a clear, consistent message. Consider using script templates you can adapt for various events. You may also need a plan for how your team can access phones, internet and computers should your office and homes be inaccessible or damaged (e.g. from a flood). This could include using a disaster recovery centre outside your immediate area. You also need to guarantee access to communication infrastructure (phone, email, internet). This could mean redundant phone lines/ services, hosted PBX systems, cloud-based email, redundant exchange servers, etc. or access to a disaster recovery centre. Figure out what will work best for you.

To ensure your plan is robust, review it regularly and adjust it as necessary.

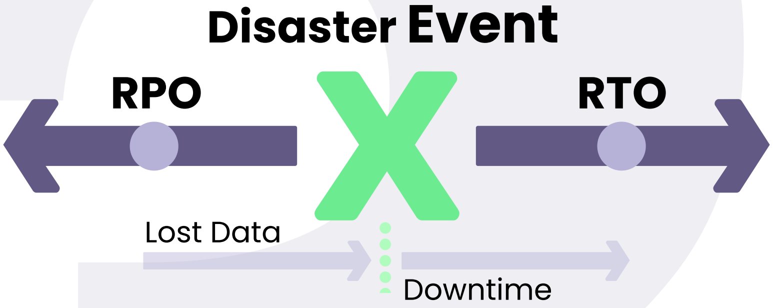


Ensure IT continuity

There are two key IT objectives you should factor into your BCP:

1 Recovery time objective (RTO) - RTO is the time it takes to restore a system after a failure or disaster. For example, if you store a physical back up of your server at an offsite location, consider how long it would take to retrieve the last back up and rebuild the server.

2 Recovery point objective (RPO) – RPO is the point to which data can be restored post-event. If you back up at 6pm each night, and a server fails at 5pm the next day, your RPO is 23 hours, meaning any data created in that time is lost. Each business will need to consider how much data is an acceptable amount to lose or re-enter manually.



Considerations: Recovery-in-place and DRaaS

Advances in virtual server backup and cloud computing have changed the game. Users can now run applications from image-based backups of virtual machines - a capability known as “recovery-in-place” or “instant recovery”. This greatly improves RTO as operations can continue while primary servers are restored and reduces RPO with common practices like snapshot-based, incremental backups every 15 minutes. Virtual machine images can also be replicated to an alternate site or cloud for disaster recovery.

An on-premise server can be used for local backup and recovery, with data replicated to the cloud for disaster recovery if there’s ever an issue with the on-premise server. In this scenario, you can run applications from the onsite server or the cloud following an outage or disaster, a process known as “cloud disaster recovery” or if you outsource the cloud back up to an IT partner it’s called “disaster recovery as a service” (DRaaS).

Keep business moving

Operations can be stalled when IT infrastructure is down. This negatively impacts productivity and revenue.

The scenarios below give an idea of the cost implications of downtime and underscores the importance of maintaining operations while your primary systems are restored.

Calculating the cost of downtime*
No. of employees: **100**
Revenue per hour: **$1,500**
Size of critical data stored: **2 TB**
Back up: **Daily, incremental @ 6pm**

Scenario 1	Scenario 2
Location: **Local back up server**	Location: **Cloud**
Time required to restore: **8.5 hours**	Time required to restore: **6 days, 9 hours, 42 minutes**
Lost revenue: $34,000	**Lost revenue: $614,800**

*Using the Datto RTO calculator: http://tools.datto.com/rto/

You can try the Datto RTO calculator on their website to estimate the revenue you could lose if you couldn't access your business data for a period.

Continuity of operations

The impact on your bottom line isn't just due to application downtime. There are numerous factors you should consider:

- **Insurance** - It's crucial to have adequate insurance coverage to replace goods or infrastructure lost to disasters like fires or floods. It's equally vital to document and safely store all your insurance information.
- **Training** – Identify employees essential to your recovery processes, assign business continuity roles, and cross-train staff on vital tasks. Your plan is a live resource, and it should also have an owner dedicated to ensuring the information remains current and ready to action at a moment's notice.
- **Facilities** - The physical sites your business operates from need to be evaluated for proper fire suppression systems, generators, uninterruptible power supply systems, surge protection systems, and emergency alert systems.
- **Dependencies** - Dependencies within and outside your organisation should be considered. For instance, if a vendor that supplies essential parts for your products is hit by a disaster, it could disrupt your operations. Your business continuity plan should include alternative suppliers or a recommendation for stockpiling critical parts.

Conclusion

The importance of disaster recovery and business continuity planning for any business can't be overstated, yet it's often overlooked, inadequately implemented, or pushed down the to-do list. We hope this guide has given insight into the potential costs and time associated with the recovery process following a disruption.

The positive side is that contemporary data protection technologies and services can significantly simplify the IT component of business continuity. There's a wide range of solutions available in the market to support you if you need it, catering to different budgets and requirements, so you can choose a product or service that aligns best with your unique needs.

Finally, remember to continually review your plan. We can't stress enough how valuable it could be one day. Regular reviews will expose flaws so you can fix them proactively, rather than in a panic during a crisis. This ensures your business is prepared for whatever comes its way, allowing you to get back to business sooner.

efex

SMARTER TECH FOR
AMBITIOUS BUSINESS

efex.com.au