eBook

4 Business Continuity Planning Essentials

Think “big picture” to craft an effective business continuity plan

Introduction

For a business built to last, expect the unexpected

By definition, disasters are unexpected—misfortune written in the stars—and hopefully rare. But for a business to survive over the long run, it must be prepared to overcome major disasters and routine calamities. Major corporations may be cushioned by their financial reserves, while a smaller business forced to close its doors during a disaster may never reopen. When disaster strikes, you want to be the exception—the business that recovers swiftly because it was better prepared and more resilient.

In this eBook, we share some of the basic steps businesses of any size should take to protect themselves.

Crafting an employee safety and communication plan that works is absolutely essential.

1. Ensure employee well-being

Communication during and following an emergency presents a variety of challenges. Crafting an employee safety and communication plan that works is absolutely essential. The specifics vary widely from company to company, but your emergency safety and communication plan must address the following:

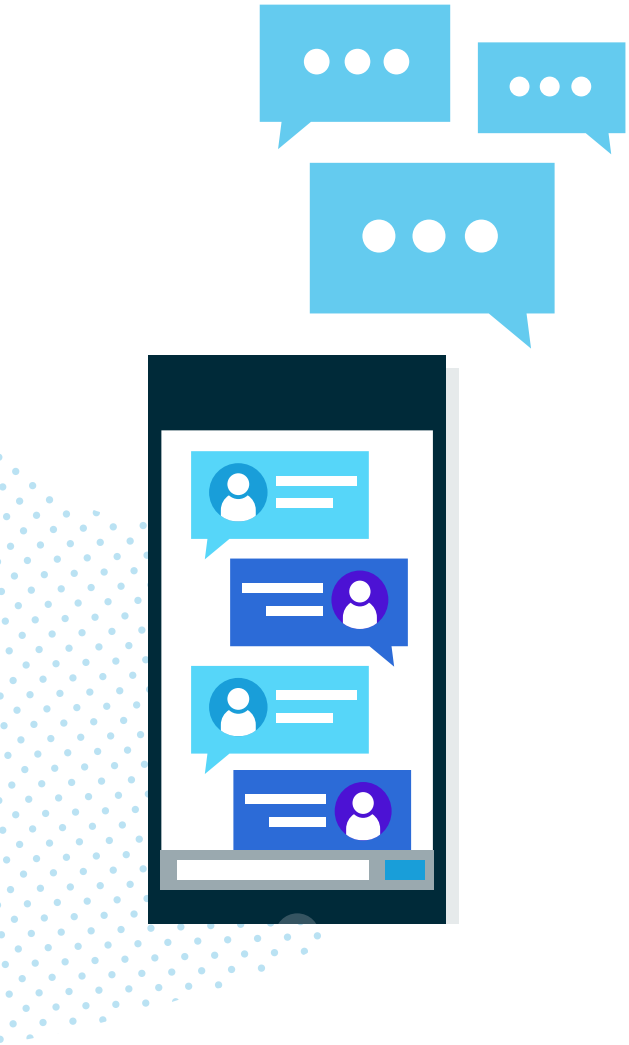
- How the company ensures employees are safe during a disaster event
- How the company conveys essential information to employees following the event

Your safety plan depends heavily on the nature and location of your business. Safety planning for a large manufacturing facility will be different than for a small real estate office, for example. Because of this, it's difficult to provide best practices that apply to everyone. The key is to match your safety plan to the needs of your organization.

For an effective communications plan, you must gather and document a variety of critical information. Verify that it is easily accessible and stored in a number of secure locations. This should include up-to-date employee contact information (email, mobile and home phone numbers, emergency contact information, and so on). It should also include a methodology for contacting employees.

Effective communication

Email is the easiest way to reach a large group of employees, but if your company's email server is down, you are out of luck. Some businesses employ redundant Exchange servers or cloud-based services to ensure email access. Of course, if you are without Internet access entirely, you'll need an alternative.



Managing customer relationships is obviously critical to the ongoing success of your business.

A call tree—sometimes referred to as a phone tree, call list, phone chain, or text chain—is another popular method for distributing important information to employees during and following an event. Here's how it works. A predetermined employee initiates the call chain with a call and/or text 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. To be effective, call tree procedures must account for what happens when the next person on the list cannot be reached, ensuring the chain will not be broken by a few missing links.

Alternatively, or in addition to planning for a call tree, you can automate emergency calls with purpose-built communications software and services.

Regardless of the methods you use to distribute information to your employees, your emergency communications plan should provide enough detail that it can be carried out by others if the plan's creator is not available or can't be reached during an emergency. Your plan should also encompass a variety of potential emergency situations. The response to a fire in your facility during working hours is very different from communications following the widespread distribution of a defective product, for example. Emergency communications should be brief and as accurate as possible. Depending on the structure of your organization, you may want to keep managers updated, allowing them to pass on information to direct reports on a "need-to-know" basis. Again, the specifics of your business dictate the correct approach.

Finally, it is essential to test and update the communications plan periodically. Test to find gaps in the plan such as out-of-date employee lists or contact information.

2. Keep customers in the loop

Managing customer relationships is critical to the ongoing success of your business. As such, it is important to craft a plan for distributing information to your customers during and following a disaster or major disruption. The scope of your customer communications plan will vary depending on the nature of your business.

Not every glitch in operations merits reaching out to your customers. However, if an event is likely to impact them, you should communicate the details of the issue and explain the steps you are taking to mitigate it. This might mean direct communication to your customers, but it could also mean messaging through traditional and social media. Failure to do so can have a negative impact on the reputation of your organization.

Take the way Toyota responded to reports of self-accelerating vehicles as an example. Instead of acknowledging the issue and assuring customers that the company was investigating the problem, the company opted to blame the victim by citing user error. The problem was eventually pinned on floor mats, gas pedal design, and faulty electronics. Although Toyota spent billions to replace accelerator components, their initial response created distrust among customers.

You also need to handle a wide array of incoming communications following a disruption. Depending on the nature of your business this could mean support requests, high volumes of email and phone traffic, social media activity from frustrated customers, media interest—the list goes on and on. Handling any of those poorly could hurt customer loyalty and damage your organization's image.

Protect your reputation and brand

How do you keep your good reputation intact? It comes down to careful preparation. First, you must be prepared from a personnel standpoint.

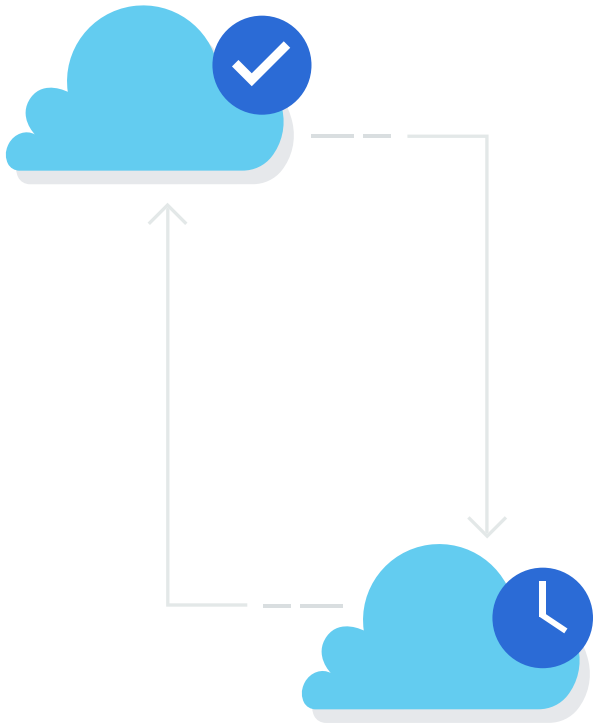
All customer-facing staffers should be briefed and ready to deliver a clear, consistent message. You may want to consider using scripted templates, which can be adapted to address various contingencies. Scripted messages can be developed and approved by management before disaster strikes, making it easy to quickly distribute them to customers following a disruption. Limit the need to improvise during a crisis.

You also need to ensure access to a communication infrastructure (phone, email, Internet access). This might mean redundant phone lines/services, hosted PBX systems, cloud-based email or redundant Exchange servers, and so on. Larger businesses may need to invest in a secondary contact center to manage inbound and outbound communications. A number of vendors offer call center services, temporary workspaces, and even mobile data centers.

Testing all or parts of your customer communications plan should be considered essential as well. Testing is the best way to identify and resolve customer support weaknesses and communication infrastructure issues.

3. Enable IT uptime

To understand the IT component of business continuity and disaster recovery (BCDR) today, it helps to look at the not-so-distant past. It really wasn't long ago that backup meant daily incremental and weekly full backups to tape or a dedicated disk backup target. Duplicate tape copies were created and shipped off site for disaster recovery—typically to a secondary site maintained by the business or to



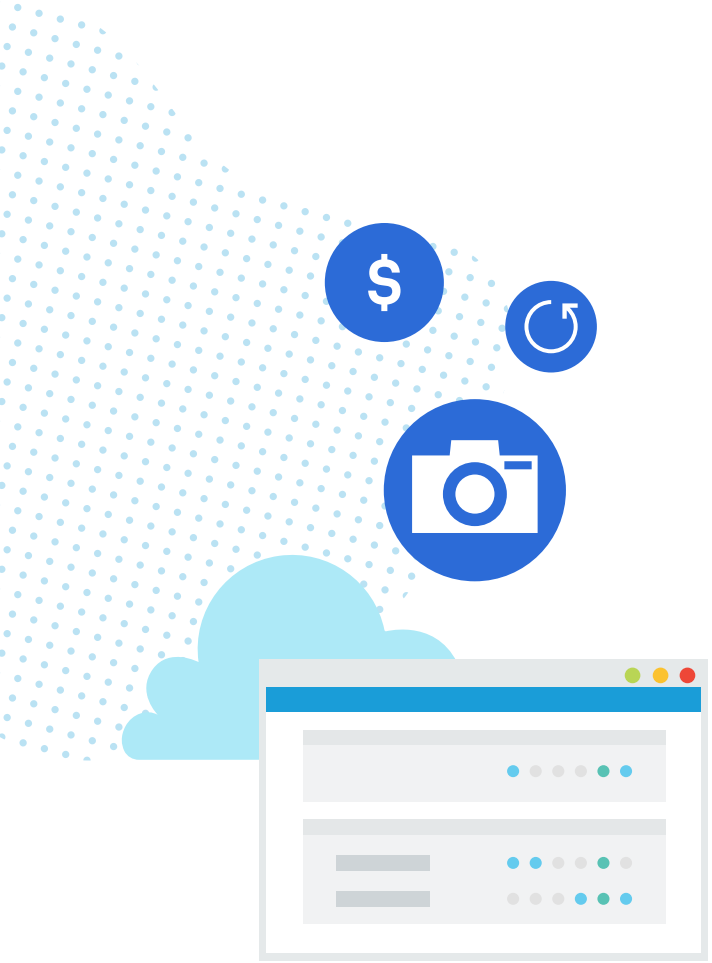
DRaaS offers the failover capabilities of traditional remote replication at a much lower price point.

a tape vaulting facility. Many businesses continue to use this model today, and depending on your recovery needs it may be perfectly adequate.

However, disaster recovery from offsite tape can be painfully slow. First, you need to retrieve the tapes from an offsite location. Once they are back on-premises, you must load the data onto your backup server before you can begin restoring data and applications to your primary servers. This means considerable system downtime, during which business applications will be unavailable or unreliable and business operations will be handicapped.

When creating an IT disaster recovery plan, it's important to understand two concepts: recovery time objective (RTO) and recovery point objective (RPO). RTO is the amount of time that it takes to get a system restored following a failure or disaster event. So given the example above, your RTO might amount to 48 hours or more. RPO is the point in time to which data can be restored following the event. So, if you performed a backup at 6 p.m. each night and a server failed at 5 p.m. the following afternoon, your RPO would be 23 hours and any data created during that span would be lost. For many organizations, this is unacceptable—particularly applications related to generating revenue or serving customers.

For faster recovery, you can replicate data to a secondary site that mirrors your data center and can quickly take over IT operations. However, this approach requires a massive investment in hardware because it requires two sets of identical servers, storage, switches, software, and so on. Not to mention a secondary data center facility. Remote replication to a backup data center allows users to fail over operations to a secondary site in the event of a disaster, which improves RTO—but is beyond the financial reach of most businesses.



Recovery-in-place dramatically improves RTO because operations can continue while primary servers are restored.

Recovery-in-place and DRaaS

Advances in virtual server backup and cloud computing have changed the equation, making remote systems recovery cost effective and practical for businesses of any size. Today, users can run applications from image-based backups of virtual machines. This capability is commonly referred to as "recovery-in-place" or "instant recovery." Recovery-in-place dramatically improves RTO because operations can continue while primary servers are being restored. RPO is reduced as well—snapshot-based, incremental backups at 15-minute intervals are a common practice. Virtual machine images also can be replicated to an alternate site or cloud for disaster recovery.

You can implement this type of system in a number of ways. Many backup software products today can perform these tasks. If your current backup software supports it, you can set it up yourself. If you rely on an older backup software product or you are starting from scratch, you might opt to outsource these tasks. In this model, an appliance is typically placed on-premises for local backup and recovery and data is replicated to the cloud for disaster recovery. Recovery-in place technology lets you run applications from the onsite appliance or from the cloud following an outage or disaster. This is commonly referred to as "cloud disaster recovery" or "disaster recovery as a service" (DRaaS).

DRaaS offers the failover capabilities of traditional remote replication at a much lower price point. Businesses typically pay a monthly subscription fee based on the amount of data they are storing in the cloud. Compared with the facilities, personnel, and technology expenses of setting up a secondary data center, DRaaS is far more cost effective. However, you should still pay attention to fee structures

that may differ substantially between DRaaS options—for example, whether the service provides you with flat-rate, predictable pricing or charges additional fees charged for the processing power necessary to run applications in the cloud during disaster recovery, which can substantially inflate your costs.

Testing IT disaster recovery plans is essential. Historically, this was a difficult and potentially risky process. Today's technologies and services have greatly eased the testing process. Because of the ease with which virtual servers can be created, users can set up DR test environments without the risk of harming production systems. Some DRaaS providers even perform DR testing for their clients.

4. Keep business moving

As noted above, many organizations today have limited tolerance for downtime. If your employees do not have access to essential applications and data—or public-facing applications are unavailable when customers are trying to access them—productivity and revenue will plummet. While this sounds obvious, many organizations do not attempt to calculate the actual costs of downtime for their business in any detail. You can do that now using Datto's Recovery Time and Downtime Cost Calculator. Here is an example, created using that calculator.

Let's say your business has 100 employees, and on a typical day, the average hourly revenue is $1,500. In order to perform daily tasks, employees need access to email, a large database, and a variety of file-based data. Let's say the sum of this data amounts to 2 TB. You perform an on-premises incremental backup at 6 p.m. daily, and this is replicated to a cloud backup service.

Given these parameters, a full restore from a local backup would take 8.5 hours, and downtime would cost your organization $34,000 in lost revenue.

When you look at restoring 2 TB from a cloud backup following a disaster, the picture gets considerably bleaker. To restore that same 2 TB from a cloud service would take 6 days, 9 hours, and 42 minutes. The cost to your business in lost revenue would be $614,800. These numbers will vary widely from business to business, but this example clearly illustrates the importance of being able to continue operations while primary servers and storage are restored.

Continuity of operations

Downtime is just one factor that can impact your bottom line. Again, there is a broad spectrum of possible considerations depending on the size and type of your organization. However, the following applies to many businesses.

Insurance—Insurance is an important factor in your recovery effort. For example, let's say your business has numerous warehouses full of goods awaiting distribution at any given time. The cost to replace goods in the event of a fire or flood could be massive and severely impact your ability to continue operations. So, it is essential to select the proper insurance coverage for your business's specific needs. Beyond that, it is also critical to document all insurance information including policy details, login information, the process for filing claims, and so on.

Training—It's likely your business will identify employees as critical to the recovery process. This might mean executives, department managers, and IT staff. Whatever the structure of your business, you will need to define business continuity roles and responsibilities. Cross-train staffers on essential tasks, in case a critical employee is unavailable following the event.

Evaluate the facility or facilities in which your business operates for their resiliency.

Facilities—Evaluate the facility or facilities in which your business operates. Considerations might include but are not limited to:

- Appropriate fire suppression systems
- Generators capable of powering essential equipment
- Uninterruptible power supply systems for critical servers
- Surge protection systems
- Alarm/intercom systems to alert employees of emergencies

Dependencies—It is important to consider dependencies within and especially outside of your organization. Let's say you are in the business of manufacturing medical devices. You might source parts from a variety of vendors—possibly worldwide. Let's say one such vendor suffers a flood or fire and production comes to a halt. This could limit access to the raw materials you need, directly impacting your ability to continue operations. Your business continuity plan should offer solutions to mitigate these issues—for example, identifying multiple suppliers or stocking up on essential parts.

Conclusion

Business continuity and disaster recovery planning should be considered a critical aspect of running a business. However, many organizations disregard it completely. Others may have a plan in place but fail to grasp how time consuming the recovery process and the associated cost of downtime can be. The good news is that today's data protection technologies and services have greatly improved the IT piece of the business continuity puzzle. There are a wide array of options in the market today at different price points, which enables you to select a product or service tailored to your specific business needs.

As you may have noticed, testing your plans has come up throughout this eBook. The importance of testing business continuity and disaster recovery plans cannot be overstated. 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.