

Your Guide to Business Continuity



Businesses are used to planned network downtime like scheduled maintenance and migration events. In these scenarios, IT leaders can set when the outage starts and when it's slated to end, along with a backup plan if things don't go accordingly.

But, what about unplanned downtime?

You've likely read about all the horror stories from enterprises: when Amazon's AWS S3 outage caused several business websites like Business Insider, Slack and others to crash, or even when human error caused a Microsoft data center in Ireland to crash, leaving European businesses without access to the company's popular cloud service, Azure. These examples demonstrate that enterpriselevel outages — like the very cloud data centers that you've come to rely on — can affect small- and medium-sized businesses (SMBs) and also show the ubiquity of downtime.



SMBs experience an **average of 2.6 downtime events per year**, compared with an enterprise's three.¹ A worst case scenario played out for a local flower shop in Colorado last year, when the store's Internet provider planned for regular maintenance on Valentine's Day. On its busiest day of the year, the store suffered a network outage, leaving it unable to process credit cards.

Is your business equipped to handle such situations?

At first glance, it may seem difficult to prepare for the types of circumstances that can lead to unplanned network downtime, but that's not always the case. Just look at the common culprits²:



Power Outage



Hardware Error



Human Error



Virus/Malware Attack



Natural Disaster



On-site Disaster

Notice that many of the causes are preventable. Yet, SMBs say that the unplanned downtime they experience annually lasts an average of seven hours per incident.³ And, that takes a toll on your bottom line.

See how much every hour of downtime costs your business [with this free calculator](#).



of SMBs lose at least
\$20,000 PER HOUR



of SMBs lose at least
\$100,000 PER HOUR⁴

Those amounts can grow even higher should you lose critical business data, making downtime a more formidable opponent. So, what's the best way for your business to guard against it?

Business continuity initiatives.

Read on to learn how to create your own business continuity plan, along with strategies you can use to bolster your business's position in preventing network downtime.

Business Continuity Basics

Business continuity initiatives are those that maintain or quickly resume operations in the event of an outage. They typically make up part of a plan that lays out detailed instructions on how to proceed company wide and have three key elements⁵:

Resilience: the ability of your mission-critical business functions and their framework to be “materially unaffected” by disruptions

Recovery: the restoration of business functions that fail

Contingency: the preparation for coping with an outage, particularly if the resilience and recovery arrangements fail

It seems intuitive, yet 48 percent of SMBs are operating without a business continuity plan.⁶ So, why do almost half of businesses take that gamble? A few misconceptions:



of SMBs **don't have a business continuity plan**

This won't happen to you. Many SMB owners still believe that by nature of their size and scope, certain events — whether it's a cyberattack or on-site disaster — cannot or will not happen to them. That couldn't be further from the truth, as many such catastrophes are out of your hands and cyberattacks do not discriminate based on business size.

You can handle unscheduled downtime when it happens. Don't expect your all-star employees to know what to do during a crisis. People respond to emergencies in such different ways than how they would in a normal situation. Not having a plan in place means employees will be responding without any coordination, which can delay recovery efforts.

You don't have the time or resources to build a plan. First, there are now enterprise-level business continuity services at prices SMBs can afford. It's also important to remember that putting in the time and money to build a contingency plan will help you bounce back after a disaster — reducing revenue losses.

You think insurance would cover all your losses. Insurance can give you financial reimbursements if you meet certain conditions that are covered by the policy. It won't, however, prevent outages or cover indirect losses, such as lost data or a damaged brand reputation.

You think business continuity and disaster recovery are one in the same. Disaster recovery should be one part of your business continuity plan. Where disaster recovery is reactive, business continuity is more proactive. Where disaster recovery hones in on operations, typically IT, business continuity takes a more comprehensive approach.

Building Your Plan

Are you feeling a little overwhelmed at the prospect of preventing disasters? Thinking that there's only so much you can do? Know that the end goal of your business continuity plan is to reduce the effect that downtime has on your business — in essence, make it a blip in your overall operations.

So, how do you go about building an effective, proactive plan? Use this checklist to ensure you've got all your bases covered:

Conduct a Business Impact Analysis (BIA).

Survey your employees to identify operational and functional impacts of downtime.

- Lost income
- Delayed income
- Increased expenses
- Financial obligations from contracts or regulations
- Customer experience

Identify important functions and processes, and use that data to develop risk profiles.

- Assign a financial value to all of your business functions and processes.
- Prioritize your business functions based on their impact to your income and expenses.
- Identify recovery time objectives (RTOs), or how long each of these functions can be down before it eats into your revenue.
- Identify recovery point objectives (RPOs), or how much data you can lose, recover or recreate per function before it eats into your revenue.
- Identify the IT resources needed to run these functions and processes.

Build a BIA report to document the order in which operations should be restored.

Start strategizing.

Identify the resources you'll need, such as personnel, facilities, utilities, technology or thirdparty vendors.

Find any gaps between the resources you'll need and those that you currently have.

Develop strategies with your team for the different types of disasters you could realistically face (e.g., hardware errors, hurricanes, etc.). These strategies could range from telecommuting, stocking enough fuel for emergency generators and entering into third-party partnerships.

Develop your plan.

Document business continuity and disaster recovery procedures.

Include a checklist of what needs to be done and when.

Assign specific employees to specific tasks.

Create check-ins with those employees to ensure everything gets accomplished.

Test, review and improve.

Conduct audits, drills or other exercises regularly to find any holes in your plan.

Document results.

Update your plan with the lessons learned and any new procedures.

Educate and regularly train employees on the latest version of your plan.

What More Can You Do?

Putting together your business continuity plan may have let you rest a little easier, but now you've really got your eye on downtime prevention. After all, in an increasingly digitized business environment, your network is one of your most important assets, and your tolerance for outages is likely pretty low.

Are you on the lookout for more ways you can make your business IT infrastructure more resilient? Try these strategies:

1. Invest in a reliable network.

Different types of broadband Internet connections offer varying levels of reliability. Among the main three — DSL, cable and fiber — fiber is the most dependable, as it is not affected by the environmental factors by which the other types are plagued. Another option — though at a higher cost — is dedicated Internet, which typically comes with an SLA, making it the optimal solution for industries that require uptime guarantees and a higher level of security.

2. Invest in diversity and redundancy.

Having just one way to connect to the Internet can be problematic, especially if you face an outage. That's where network diversity and redundancy come into play.

Businesses can achieve diversity and redundancy by:

- Provisioning different types of connections (e.g., fiber and 4G backup)
- Subscribing to multiple Internet service providers

Here's how you can accomplish those on budget:

- **4G LTE Wireless Backup:** This is by far the simplest way to achieve diversity and redundancy. Wireless backup will detect when your primary connection goes down and will implement automatic failover until that connection is restored.
- **SD-WAN:** Your second option is an SD-WAN solution, which can also provide automatic failover. But its work doesn't stop there: a software-defined WAN can combine the bandwidth of all active connections — wired or wireless, from one provider or many — giving your business the most reliable and redundant network infrastructure that can intelligently route traffic through the best possible path.

3. Invest in cloud technology.

If you recall, many network outages are the result of power failures or hardware errors. Just how frequently do these occur?

140,000 hard drives fail in the U.S. each week.⁷



of businesses experience a **power outage once a year or more.**



of businesses experience one **power outage once a month or more.**⁸

The best workaround for these kinds of interruptions is the cloud. Instead of storing and maintaining physical equipment and software, your business can continue using those very services online. The beauty of the cloud is that users can access information anytime, anywhere, using any device.

If employees need a new computer due to a hard drive failure, they can easily gain access on a new computer to their previously stored data in their cloud-based, or SaaS, apps. If a power outage drags on and on, employees can simply pack up their laptops and work remotely with all their resources available online.

Besides business applications, the cloud has increasingly become home to another business continuity service — backup.

Nearly 78% of SMBs will use cloud-based data backup methods by 2020.⁹



Redundancy is key here, too. You won't want your critical business information stored in just one spot — even if it is the cloud. Of the SMBs that currently use cloud backup, 84 percent do so online and on-site.

Business continuity can seem like a daunting task, but it's one that is necessary — and within reach — for small- and medium-sized businesses. Use the checklist and recommendations above to get started on your business continuity plan and safeguard your business today.

¹<https://community.spiceworks.com/topic/268672-infographic-the-cost-of-downtime-for-small-and-mid-sized-businesses>

²Zetta State of Disaster Recovery 2016 Survey

³<https://www.aberdeen.com/techpro-essentials/downtime-is-money/>

⁴<https://www.techradar.com/news/computing-components/storage/network-downtime-is-incredibly-costly-for-smb-1256263>

⁵<https://acp-international.com/resources/business-continuity>

⁶<https://www.travelers.com/resources/business-continuity/why-is-business-continuity-important>

⁷www.mozy.com

⁸<https://www.sandc.com/globalassets/sac-electric/documents/sharepoint/documents---all-documents/technical-paper-100-t120.pdf>

⁹<https://www.forbes.com/sites/louiscolombus/2015/05/04/roundup-of-small-medium-business-cloud-computing-forecasts-and-marketestimates-2015/#6f35ec9132b0>

To learn more about Kinetic Business, visit kineticbusiness.com

