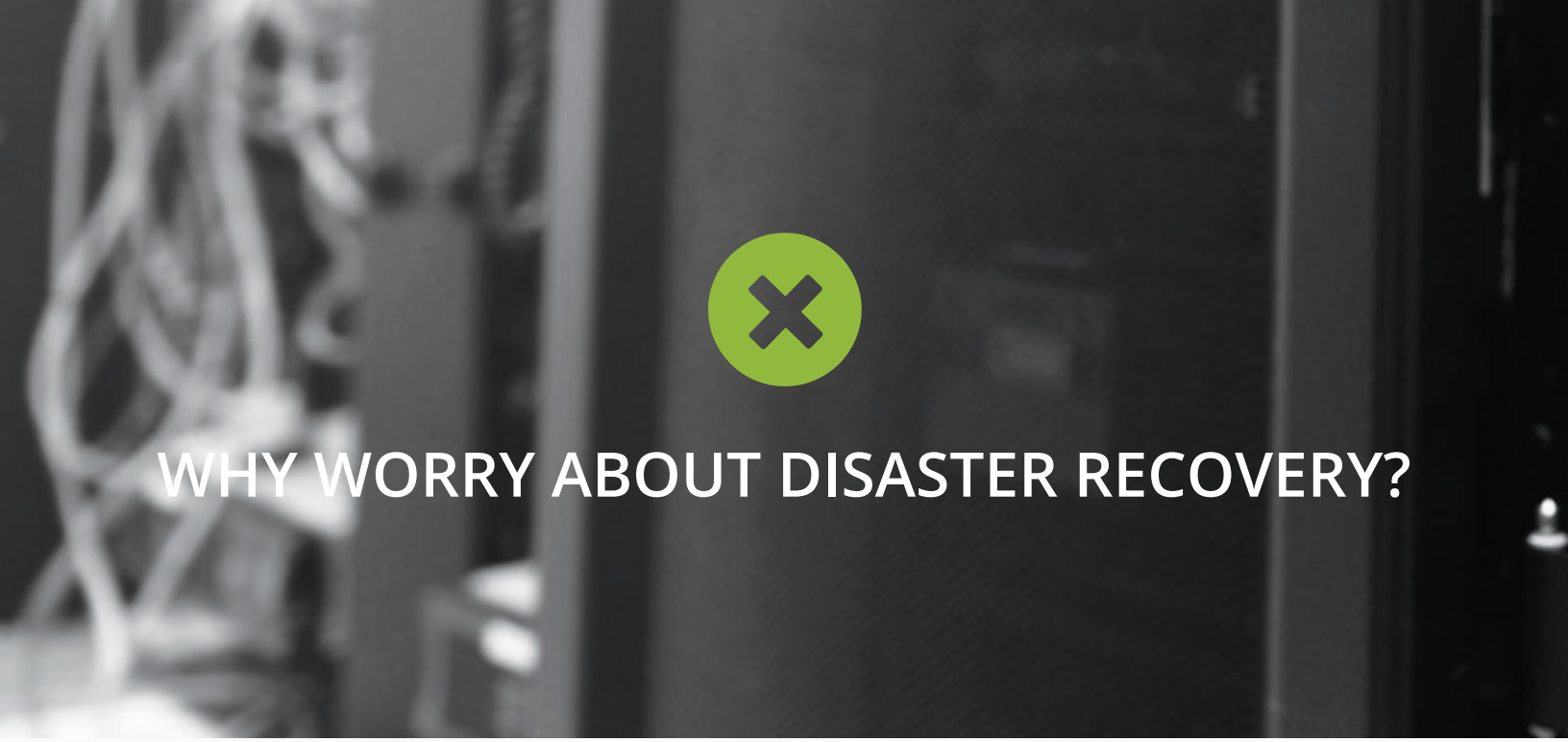
5 Things Small Businesses Need to Know About Disaster Recovery

CARBONITE



WHY WORRY ABOUT DISASTER RECOVERY?

THERE WOULD BE NO NEED TO THINK ABOUT **DISASTER RECOVERY** IF ANY OF THE FOLLOWING WERE TRUE:

- Your chance of losing data over the next couple of years was slim to none.
- Losing data would have no impact on your business.
- It's not that costly for a small or midsize business (SMB) to lose data.
- Disaster recovery is for big businesses and not practical or affordable for SMBs.
- Even if you do lose data, you could get it back in no time.

The fact is, none of these are true. But don't take our word for it. We talked to IT professionals at small and midsize businesses, and we hired top experts to dig into the data behind data loss, downtime and disaster recovery for SMBs.

Here's a sample of what we found:

1. **You most likely will lose data, probably this year if you haven't already.**
2. **The "disasters" that cause data loss come in many different forms.**
3. **When you lose data, the cost of losing it will far exceed the cost of prevention.**
4. **You may be without your data for longer than you think.**
5. **The time it takes to recover data depends greatly on your backup method.**

As data becomes more essential, so does protecting it. For SMBs, implementing critical technologies when you don't have a huge IT budget or IT resources at your disposal can be a big challenge. That's why we put together this e-book of **5 Things Small Businesses Need to Know About Disaster Recovery**. By gaining a view into the experiences and best practices of other small business owners and IT pros, you can make better decisions about your disaster recovery plan.

5 Things Small Businesses Need to Know About Disaster Recovery

1

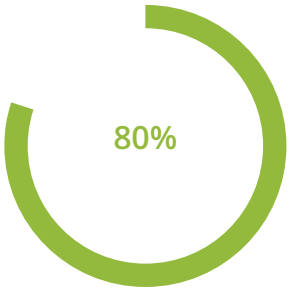
YOU WILL HAVE TO PERFORM DISASTER RECOVERY

It's not a matter of if, it's when.

There are two kinds of companies: those that have lost data and those that will. Study after study has shown that virtually no company is immune to data loss.

In our survey of 160 IT pros from the online IT community, Spiceworks, **48% of respondents reported losing data** in the last year alone.[1] This includes hardware failures, power surges and natural disasters. In a survey of more than 700 SMBs worldwide by the International Data Corporation (IDC), **80% reported experiencing downtime**.[2]

48% of IT pros reported losing data in the last year[1]



Over **80%** of small businesses have experienced downtime[2]

Number of downtime events in the last 12 months

Best-in-class	Average	Laggard
0.56	**2.26**	**3.92**

Companies cited an average of **2.26** downtime events over a recent 12-month period.[3]

While the scale of data loss varies greatly, almost one-fifth of SMBs had to perform a full data center recovery in the year 2014.[4]

The frequency of these events illustrates the inevitability of the need for SMBs to perform disaster recovery.

STRIKE A DEAL FOR DATA?

If there's one thing we learned from talking with IT pros, it's that they **don't like losing data**. Here's a list of things they would gladly give up instead of losing their organizations' data:

Internet connection

Cell service

Internal organ

Wedding ring

Robot lawnmower

Bacon!

Knowing the likely sources of data loss will help you prepare your disaster recovery strategy.

2

DISASTERS COME IN MANY FORMS

While natural disasters, such as hurricanes and floods, tend to grab more attention, the source of most forms of data loss and downtime has nothing to do with weather.

When we asked IT pros what they considered to be the highest risk factors for data loss, they cited technology failures first, followed closely by man-made disasters and security incidents.[1]

Perceived risk factors for data loss

Technology Failures	Man-Made Disasters	Security Incidents
65%	60%	59%

Of those who actually experienced an incident requiring disaster recovery, the leading cause by far was man-made, like accidental file deletions and spilled coffee.

After man-made disasters, IT Pros cited technology incidents as the next cause for having to perform disaster recovery. This includes equipment failures, lost or stolen devices and network outages.

The third major cause for having to perform disaster recovery was security incidents. This includes social hacks, viruses and ransomware.

Actual risk factors for data loss

Man-Made Disasters
65%

Technology Failures
29%

Security Incidents
22%

DON'T FORGET NATURAL DISASTERS
Natural disasters, though occurring less frequently, carry a huge potential for disruption and should not be left out of disaster planning.

STORAGE ≠ BACKUP

Many small businesses use cloud storage services as an ad hoc form of file backup. Storage as backup is very unreliable, as you could easily accidentally delete, overwrite or simply forget to upload a full set of your data before a disaster strikes. Cloud storage is generally for sharing information with co-workers or being able to access work on mobile devices.

True backup doesn't rely on users to manually drag and drop files or upload them to the cloud. It works automatically and in the background, backing up all user files and data, and scanning for changes along the way. This significantly reduces the chances of data loss due to human error.

There are financial costs associated with losing data, as well as productivity costs.

3

A DISASTER RECOVERY STRATEGY IS A BUSINESS IMPERATIVE

Like all businesses, SMBs are under pressure to reduce costs and increase efficiency.

Measuring the financial cost of recovering data is the first part of forming a disaster recovery strategy.

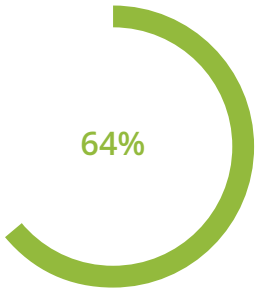
A recent IDC survey provided estimates for the per-hour cost of downtime for very small, small and midsize businesses. Every hour of unplanned downtime costs $8,220 for very small businesses (fewer than 10 employees); $10,790 for small businesses (between 10 and 99 employees); and $25,600 for midsize businesses (between 100 and 499 employees).[2]

Mean cost of downtime per hour among SMBs

SMB Segment	Mean Cost per hour
Very Small Business (<10 employees)	$8,220
Small Business (10-99 employees)	$10,790
Midsize Business (100-499 emplyees)	$25,600

The total cost of downtime depends on how long systems are offline. It could be anywhere from hours to days. Taking into consideration the per-hour cost, a single event would be devastating for an SMB that lacks an effective disaster recovery strategy.

50% of SMBs would go out of business within two years following a full-scale disaster[4]



64% of IT pros said they would go out of business without data backup in place[1]

If you have a backup plan in place, successful recovery will depend very much on how fast you can recover and how much data you lose, and whether these fall within the tolerances you've established for your organization. Determining your tolerances is the next part of forming an effective disaster recovery strategy.

Downtime costs include lost productivity when employees can't access critical applications such as email.

Mission-Critical Applications as cited by SMBs[2]

Email Systems
65.7%

IT Infrastructure and Systems Management
39.5%

Industry-specific Applications
31.2%

Web Serving and Internet Content/Video
28.8%

More than half of IT pros said it would take 100% of IT resources to recover from a complete data loss.[1]

There's a big gap between user expectations for disaster recovery and what IT can reasonably deliver within a given budget.

4

IT MAY TAKE LONGER THAN YOU THINK TO RECOVER FROM A DISASTER

76% of SMBs expect no less than one hour of data loss

61% of SMBs expect full recovery for mission-critical applications in no less than four hours[4]

72% of IT pros said 24 hours or less was a realistic recovery time

Only **24%** of IT pros said they could recover in less than 4 hours[1]

There's a very simple way to set realistic expectations for disaster recovery, and it involves figuring out two things:

1. **How long your business can go without access to mission-critical applications and data. This is called your recovery time objective (RTO).**

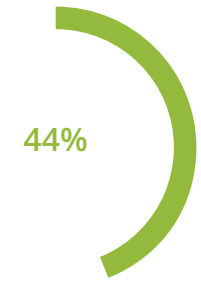
2. **How much data loss is acceptable for your organization. This is called your recovery point objective (RPO).**

Knowing your RTO and your RPO is a very important part of building an effective disaster recovery strategy. Once you know your strategy and budget, you can better evaluate your infrastructure options.

One study found that the best performing companies calculated their RTO for each mission-critical application in their portfolio, since these are the ones most directly tied to the cost of downtime.[3]

Best-in-class Determine RTO per Application

Best-in-class	Average	Laggard
73%	**45%**	**35%**



44% of SMBs reported that mission-critical applications make up 10-20% of their total application portfolio.

Mission-critical applications include email, IT systems management, industry-specific applications and Internet service.

RTO and RPO defined

Recovery Time Objective	The amount of time that a business intends to restore or make available a process after interruption
Recovery Point Objective	The maximum amount of acceptable data loss, measured in time

Knowing which applications you need to restore first and how long you can operate without them helps you establish your RTO. Your ability to deliver on your RTO will depend greatly on the method you choose to back up your systems and data.

The first step to ensuring you can restore your data is making sure you're backing it up the right way.

5

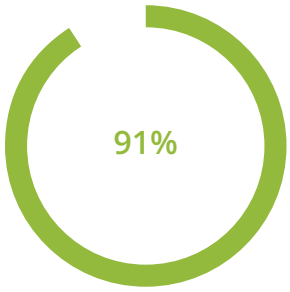
BACKUP IS THE KEY TO SUCCESSFUL DISASTER RECOVERY

If you're using a storage product as a backup solution, you may miss backing up critical files.

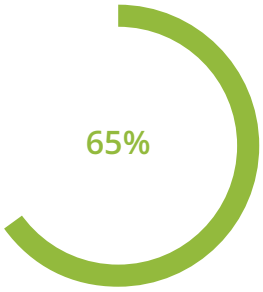
Onsite backup provides the fastest achievable restore times, since data is transferred from a local network to local hardware. The danger is if there is a local failure, such as a power outage or natural disaster, the onsite backup becomes unusable.

Offsite backup provides an extra layer of reliability and protection from local failures and natural disasters, but recovery time from an offsite location is generally slower. There's also the cost to maintain a secondary site, which can be prohibitively expensive for many SMBs.

If you're only backing up files and your server crashes, you won't be able to restore your databases, applications or operating system. And, if all your backups are stored onsite and you incur damage to your local infrastructure, you may be left without any backup at all.

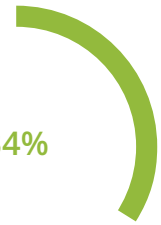


91% of SMBs are using some form of onsite backup[1]



65% of SMBs are using disk or tape for backup[2]

29% of IT pros backup at an offsite location owned by their organizations[1]



34% of SMBs have no offsite approach[2]

A hybrid approach, backing up both onsite and offsite, offers the speed of local backup with the reliability of a secondary location.

54% of IT pros use both onsite and offsite backup[1]

The best-of-both-worlds approach is keeping a local copy of your data and using a cloud backup and recovery service to provide added reliability in the event of a local disaster.

Ultimately, the goal of any disaster recovery solution is to help businesses withstand the coffee spills, lost laptops and power outages, as well as unexpected natural disasters, and maintain business as usual.

What's appropriate for your environment depends on what information is critical to your business and how long you can go without it. The right functionality and feature set combined with ease of use, at a price point your business can absorb, can help you achieve the recovery objectives that you've established for your organization.

The ideal disaster recovery solution for SMBs is one that includes:

- **Functionality for achieving your desired RTO and RPO**
- **Simplicity in deployment and maintenance**
- **Security and reliability equal to enterprise-level protection**
- **Affordability appropriate for SMB budgets**
- **Access to a dedicated customer support team**

TRUE DISASTER RECOVERY FOR SMBs

Carbonite provides a comprehensive suite of backup and recovery solutions designed specifically for SMBs.

Carbonite Server Backup key features:

- Granular database backup and recovery
- Hybrid backup (cloud & local)
- Hot backup (data is accessible during backup)
- Support for physical and virtual environments
- Advanced customization options (compression, scheduling, bandwidth allocation, retention)
- Unlimited license model (no per-server or per-application fee)
- Valet install to get you up and running in 15 minutes

Carbonite Pro for Workstations key features:

- Automatic cloud backup of critical business data
- Backup for unlimited computers and external storage
- Simple and reliable file recovery
- Advanced encryption for security and compliance
- Anytime, anywhere access & file sharing
- U.S.-based support 7 days a week

Sources:

1. Spiceworks: Carbonite Backup & Disaster Recovery Research; June, 2015
2. International Data Corporation: The Growth Opportunity for SMB Cloud and Hybrid Business Continuity Sponsored by: Carbonite, by Raymond Boggs, Christopher Chute & Laura DuBois; April 2015
3. Aberdeen Group: Downtime & Data Loss: How Much Can You Afford?; August 2013
4. International Data Corporation: Holistic Data Protection: Establishing a Best Practice Framework; by Carla Arend, Laura DuBois, Phil Goodwin and Ashish Nadkarni; April 2015

NONSTOP PROTECTION FOR NONSTOP BUSINESS

Carbonite provides cloud and hybrid backup solutions for better protection and faster recovery of all your business data.

carbonite.com

CARBONITE