

How

DISASTER RECOVERY

Can Save Your

BUSINESS

An introductory guide to Disaster Recovery and how it can ultimately keep your company alive.

A Publication of





//

By failing to prepare, you
are preparing to fail.

//

- Benjamin Franklin

Table of Contents

Introduction

Chapter 1: What is Disaster Recovery?

Chapter 2: By the Numbers...

Chapter 3: Standby for (Re)launch

Chapter 4: Make Your Move

Conclusion

How can this eBook help?

This eBook will define disaster recovery for your IT infrastructure and explain how to plan for your specific business needs, including:

Learn the terms:

First, we have to go back to school and identify all the terms that surround disaster recovery and continuity planning.

Review the statistics:

Talk about scare tactics – these notable studies have determined that if you aren't prepared, your business will suffer.

Discover where your business fits in:

Every business is different, so we need to look at the different options available and match them with your organization's unique needs.

Asks questions and seek answers:

Once you've aligned your options with your needs, it's time to start investigating different ways to deploy your recovery plan – this can be done in-house or through a hosting provider.

CHAPTER

1

What is Disaster Recovery?

Disaster Recovery is a critical step in Business Continuity planning. It's an attack or incident that can't be predicted, but it *can* be prepared for.



//

The minute you think
you've got it made, disaster
is just around the corner.

//

- *Joe Paterno*



Having a Disaster Recovery plan doesn't just save your infrastructure; it can also save your job and your organization.

A **Business Continuity Plan** will identify your company strategy for continuing operations after a major incident.

Whether you suffer a natural disaster, an IT hiccup or a malicious attack against your business, you can **prevent serious loss, downtime or potential shutdown** by setting up a disaster recovery plan (or DRP) that allows for the continuation of your technology infrastructure according to your unique business needs.



It starts with establishing two critical times for your business:

Recovery Point Objective (RPO): This is the maximum period of time that your company's IT can be without data that gets lost after a major incident.

Recovery Time Objective (RTO): This is the maximum period of time that it takes for your company to recover the services necessary to resume business after a major incident.

These time intervals should be assessed to identify how long your organization can operate after a major incident without incurring significant risks and losses.

CHAPTER

2

By the Numbers

An attack or incident on your organization may seem far off or unlikely, but recent studies from reputable analyst firms show just how real and unpredictable this can be for businesses like yours.



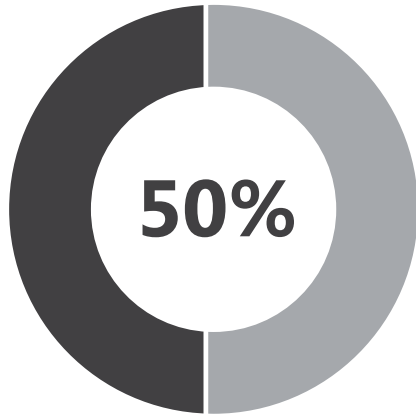
//

Forewarned, forearmed;
to be prepared is half
the victory.

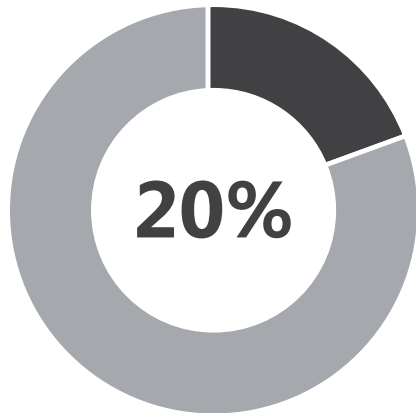
- *Miguel de Cervantes*

//

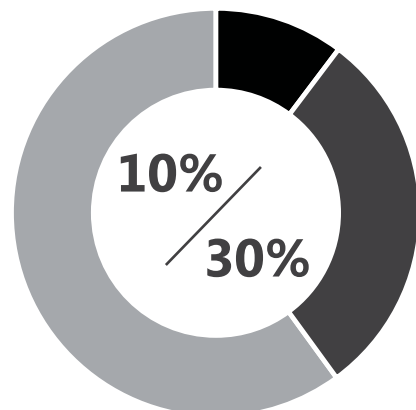
Bad things happen to good companies:



Agility Recovery Solutions reports in the past two years, Over 50% of businesses experienced an unforeseen interruption.



An **Aveco study** estimates that 20% of companies will suffer fire, flood, power failures, terrorism or hardware or software disaster.



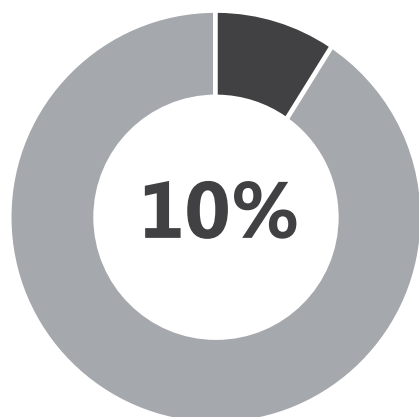
According to a recent **NFIB National Small Business Poll**, man-made disasters affect 10% of small businesses. Natural disasters, however, have impacted more than 30% of all small businesses in the USA.



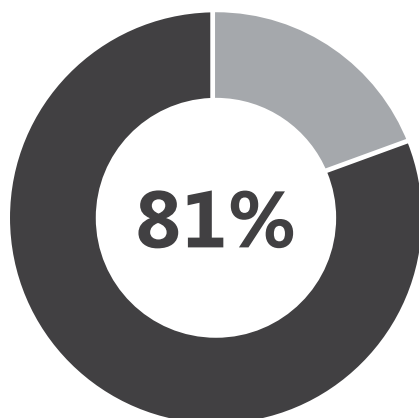
Mozy Online Backup

estimates that every week, 140,000 hard drives crash in the United States.

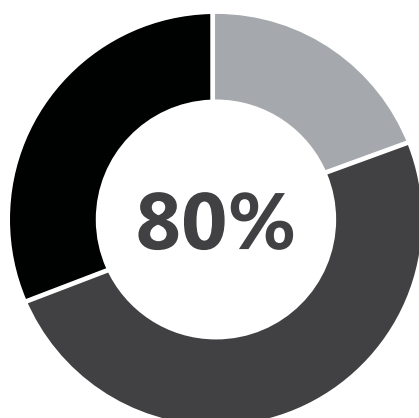
Failure to prepare could mean a “Closed for Business” sign on the door:




A recent **Touche Ross study** puts the survival rate for companies without a DRP at less than 10%!



Agility Recovery Solutions reports the majority of interruptions (81%) caused the business to be **closed one or more days**.



Aveco states that of the businesses without a DRP that suffered an incident, 80% that experience a significant data loss are likely to go out of business **within one month** and 43% of businesses that are not able to resume operations within 10 days of a major incident **will never reopen**.



The cost of downtime is big money per hour:

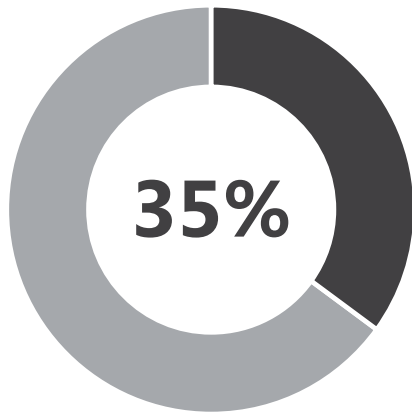
International Data Corp estimates an average loss of \$84,000 for each hour of downtime.

CA Technologies calculated that more than \$26.5 billion in revenue is lost each year from IT downtime, roughly \$150,000 annually for each business.

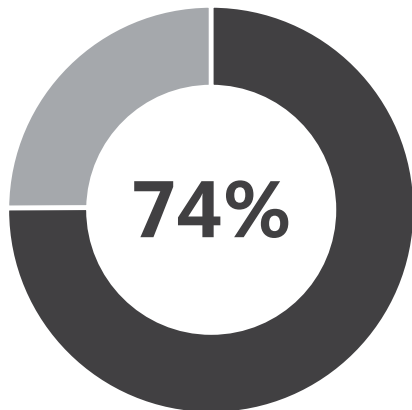
In their survey, **CA Technologies** reported small enterprises lost an average of \$55,000 in revenue due to IT failures each year, while midsize organizations lost more than \$91,000 and large enterprises lost more than \$1,000,000.

A data center outage by itself can cost an average of **\$5,600 per minute.**

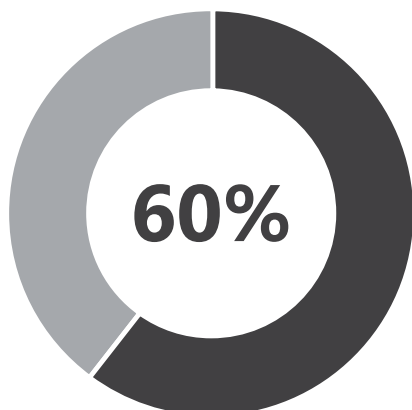
The larger the company, the more ready it is to handle a disaster:



Gartner estimates that only 35% of small and medium businesses have a comprehensive disaster recovery plan in place.



A **Regus** study found that only 51% of small businesses have an IT business continuity plan in place, ensuring IT systems are up and running within 24 hours, compared to 74% of large businesses.



The **Regus** study revealed that about 60% of large businesses have a workspace business continuity plan in place, compared to only 43% of small companies.

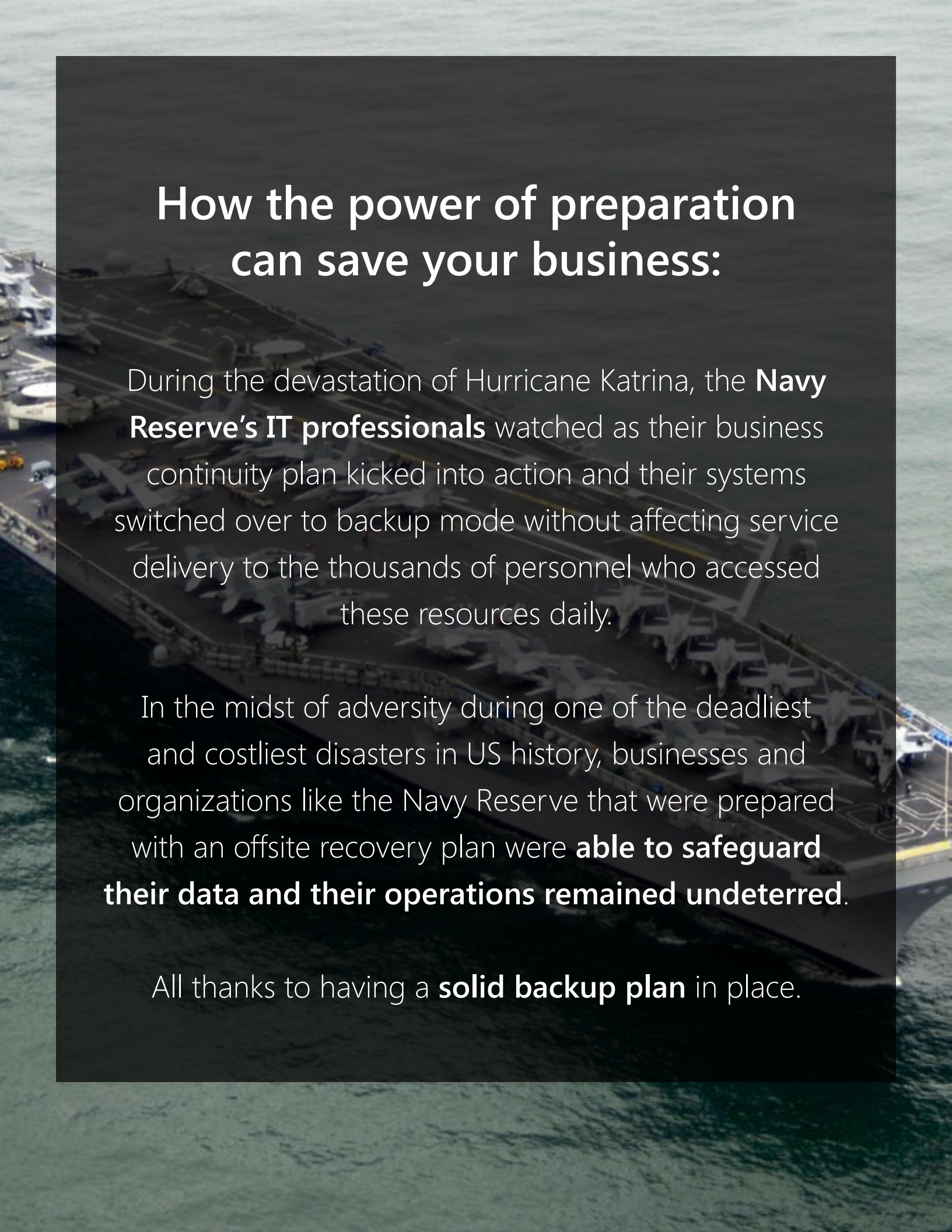
Downtime is often a result of human error:

Vendors offering disaster recovery solutions have stated that between 60 and 70% of all problems that disrupt business are due to **internal malfunctions** of hardware or software, or **human errors** that may lead to fraud.

According to **Timesavers International studies**, the catastrophe most businesses experience is not fire, flood or earthquake, but something much more insidious—**malware**. In 2008, the USA was the top country for overall malicious activity, making up 23% of the total.

VaultIT reports only 26% of downtime occurred because of a fire or explosion and 10% from natural disasters. 60% was a result of human error.

VaultIT also found that only 15% of remote offices are protected because most disaster recovery plans fail to protect your remote office data.



How the power of preparation can save your business:

During the devastation of Hurricane Katrina, the **Navy Reserve's IT professionals** watched as their business continuity plan kicked into action and their systems switched over to backup mode without affecting service delivery to the thousands of personnel who accessed these resources daily.

In the midst of adversity during one of the deadliest and costliest disasters in US history, businesses and organizations like the Navy Reserve that were prepared with an offsite recovery plan were **able to safeguard their data and their operations remained undeterred.**

All thanks to having a **solid backup plan** in place.



Now consider these statistics from a Cloud-centered DRP:

The average length of downtime per major incident for cloud users was **four times shorter** than non-cloud users.

Similarly, cloud users **experienced fewer downtimes** than non-cloud users (via Smart Data Collective).

CHAPTER

3

Standby for (Re)launch

Knowing that you need a backup plan is important, but it's just the start. How do you figure out how to get your data back up and running?

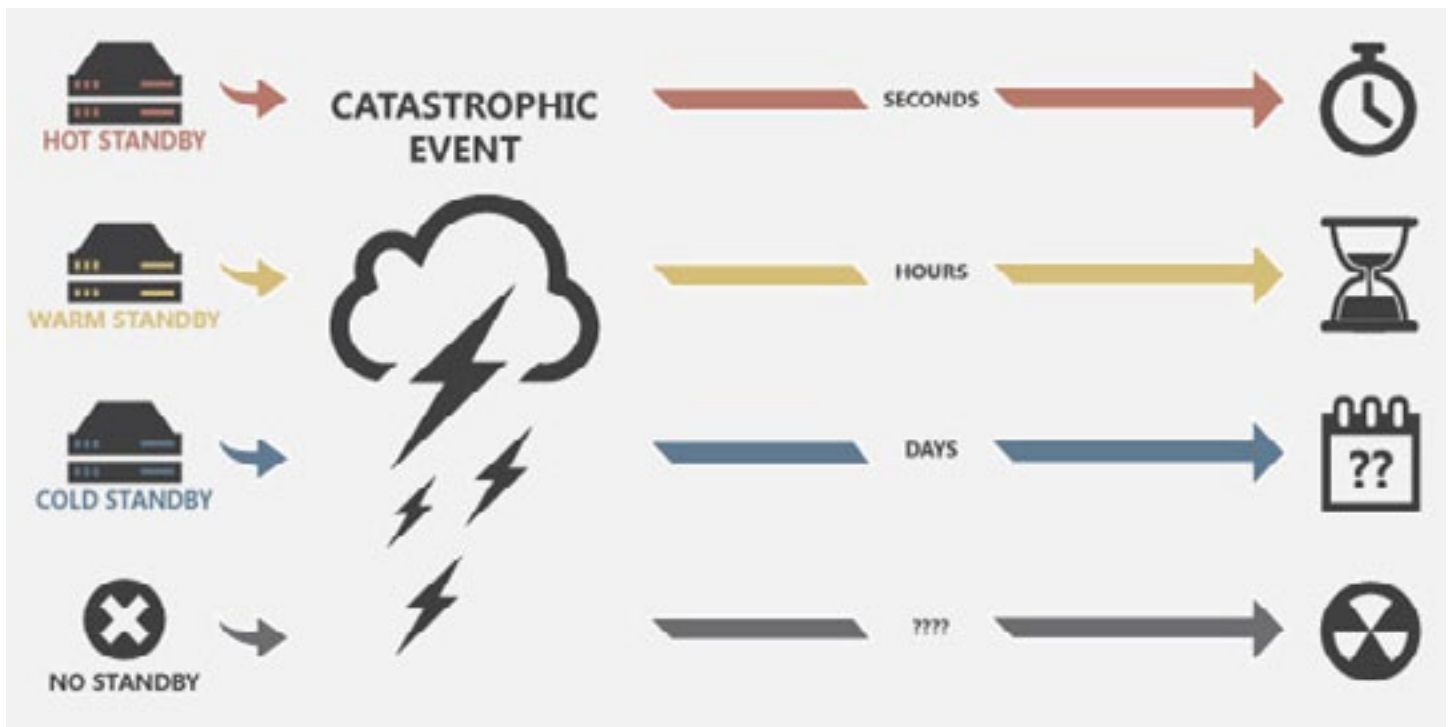


//

Always remember that you
are absolutely unique. Just
like everyone else.

//

- Margaret Mead



Businesses must decide how accessible they want their data to be. There are three redundancy scenarios to choose from:

Cold Standby: A backup system is available if the primary system fails. This is usually used for non-critical information and scheduled backups would be customized by the client. (Availability within hours to days typically)

Warm Standby: A backup system is available and is a close mimic of the primary system. Data is replicated more often than a cold standby, but at the discretion of the client. There can be times when both servers don't contain the same data. (Availability within minutes to hours typically)

Hot Standby: A backup system that runs simultaneously with the primary system. Data is typically replicated in real time and both systems host identical data. (Availability within seconds typically)



The good news is that you have options:

Whatever standby system you adopt (cold, warm, hot), more servers will mean more costs and additional support and maintenance.

The level of **Disaster Recovery** you require will determine the cost.

Of course, that cost is trivial when compared to the cost of losing critical data or even your entire business.

CHAPTER

4

Make Your Move

Once you establish which direction to take with your organization's disaster recovery, the final step involves implementing it.



//

You don't drown by falling
in water. You drown by
staying there.

//

- *Edwin Louis Cole*



Now, you must decide how to deploy your recovery plan:

Hosting providers can manage servers that spin up data as needed and replicate your data from the primary data center to sends to the server farm at your designated off site data center.

You can deploy an **in-house recovery plan** by purchasing the necessary equipment to replicate your data as needed.

Ideally, the backups should be stored in an **off-site location**.



Above all else, ask questions and seek answers!

One thing is certain – this is no little thing.

Make sure you are aware of your organization's unique needs and then actively seek out the best way to implement your plan.

Hosting providers are happy to **answer questions** regarding best practices and recovery options as well as work with you to **identify the best Business Continuity Plan** for your company and set up a Disaster Recovery solution that **satisfies your business needs** so that you can rest easy knowing **your data is secure**.

Please accept this

FREE DISASTER RECOVERY CONSULTATION

from Fpweb.net

One quick phone call can help you identify your failsafe, your 'Plan B'. Take advantage of this opportunity be prepared, because without a recovery plan, there are no second chances.

A Publication of

