Beyond Disaster Recovery:
Why Your Backup Plan Won't Work

Centre
TECHNOLOGIES

Contents

Introduction

By default, the world itself is unstable, and disruption and downtime is universal across all organizations. In 2014, FEMA noted 84 emergency declarations throughout the nation, including winter storms, flooding, earthquakes, fires, and hurricanes [2].

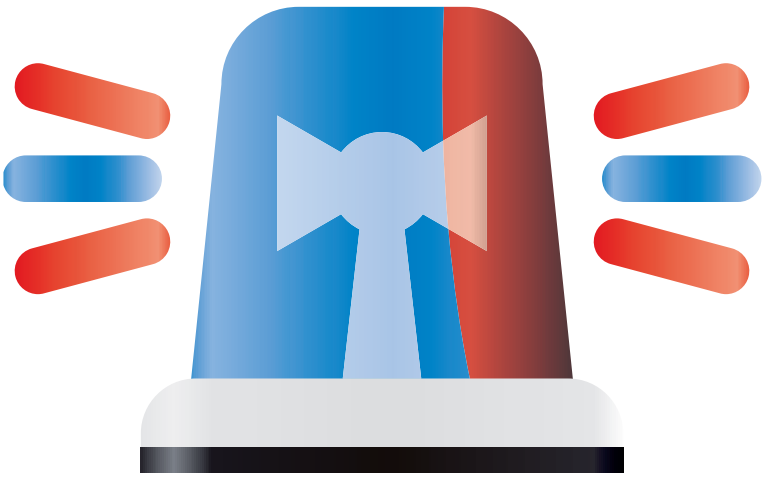
The state of disaster recovery is little short of being a disaster itself. A 2014 study by *the Disaster Preparedness Council* found [3]:

- 3 in 4 companies are failing from a disaster readiness standpoint.
- 20% of businesses reported losses of more than $50,000 to $5 million dollars in downtime.
- More than 65% of organizations fail their own disaster recovery tests.
- 60% of organizations do not even have a fully documented disaster recovery plan.
- 40% of organizations with a DRP claimed that their plan failed to work when they needed it to.

The root of the problem: while many businesses are investing in backup solutions, backup is their only disaster recovery measure. Backup alone is not enough to restore a business, and you need to ensure the protection of your data by extending the scope of your plans beyond *just* disaster recovery.

To take your DR to the next level of efficacy, this report will discuss:

- The pros and cons of the traditional backup model.
- The gaps left by most disaster recovery plans.
- A business continuity solution that can cut your recovery by half.



The Data Backup Model - Upgraded for 2015

For the purposes of this white paper, here are clarifications of the definitions of DR and BC.

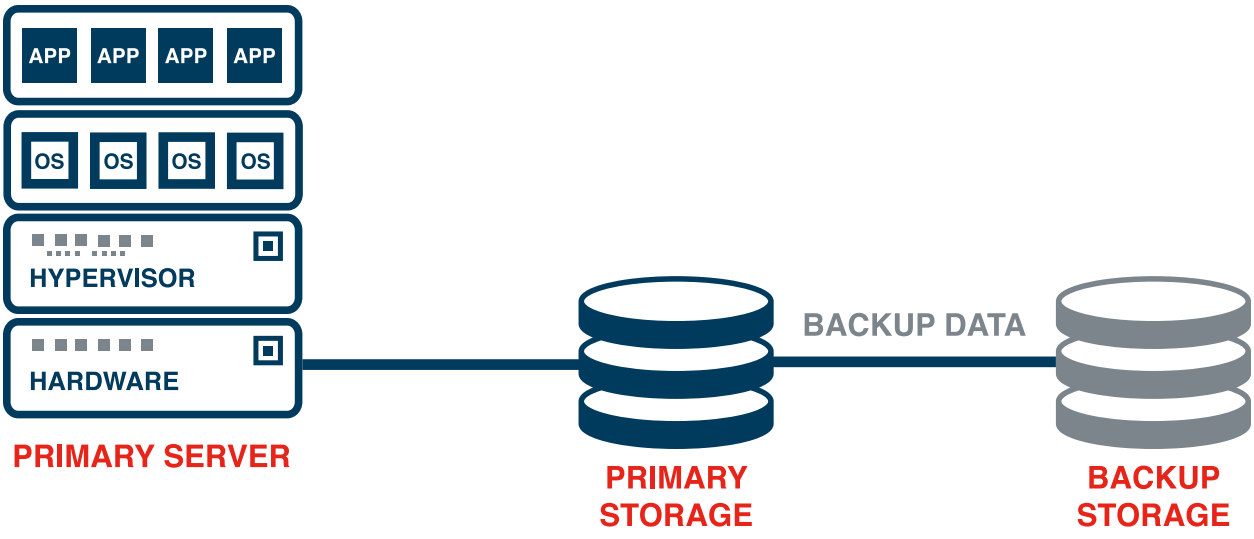
> **Disaster Recovery (DR)** - The process by which you preserve your organization's data in the event of a major or minor disruption (natural and man-made).
>
> **Business Continuity (BC)** – The capability of your organization to continue working after a disruption within an acceptable post-incident time frame.

While the goal for both DR and BC is to preserve an organization's data during a disaster, only ***business continuity*** is focused on the methods and technologies required to decrease your overall downtime. A business continuity plan (BCP) builds the framework to allow employees to continue working after a disaster within a specific recovery-time objective, or RTO.

The modern backup solutions provides, at minimum:

1. Regularly scheduled backup intervals
2. Backup scope includes duplicated data across the infrastructure
3. Data backed up to secondary storage disk array or to the cloud

While the time intervals and the location of the data will vary per provider, a good disaster recovery plan ***must*** meet these minimum requirements. Disaster recovery solutions have come a long way in a few short years, and for a few businesses, this service is *just* enough to rescue their organization from the setbacks of a major disruption.



Why Disaster Recovery Isn't Enough

If your business relies on your digital assets to generate revenue, interact with customers, communicate with your employees, manage files, and run applications, ***DR is not enough***. After a data loss incident, it can take up to ***two days*** to restore a physical server, even if you're just importing data from the cloud.

In short, disaster recovery is nothing more than a copy of your data.

Why?

After a loss incident, you physical server becomes an empty shell, exclusively made from hardware. After a catastrophic data loss incident, your IT department will still have to rebuild your entire network *before* importing your backed up data, provided your physical server is still intact. They will have to build and reconfigure your virtual infrastructure and connectivity before they can move your applications and data back into your infrastructure.

In short, disaster recovery is nothing more than a *copy of your data*. The shortest amount of downtime your business will experience is a minimum of two days, and a maximum of a week depending on your provider's SLA.

The final question is how much downtime you can afford. If your business can survive beyond a longer recovery-time-objective (RTO) of two days or more, the traditional enterprise DR model can work for you.

However, you will still need a ***business continuity plan*** to orchestrate and detail how to restore your business, even from minor disruptions.

Business Consequences with DR-Only Solutions

When you have a DR-only solution, you're at least taking steps in the right direction. You understand the value of your data and the implications of losing it.

Unfortunately, the modern business, and the modern consumer, demands availability. If your network is down, even for just a day, your downtime losses could include:

Consequence	Example
Revenue impact	In 2013, Google lost upwards of $500,000 in a single outage [4].
Loss of reputation and/or loss of customers	NASDAQ suffered a 3 hour long outage which resulted in a memorable trading halt across the USA [5].
Financial, legal, and/or regulatory penalties	HIPAA could fine your business for data loss and lack of appropriate safeguards, with a maximum fine of $50,000 per violation [1].
Productivity losses	Google's 2013 outage cost them 40% of their traffic [4].
Employee moral	If your RPO window is too wide, your employees could lose some of their most valuable recent data.

Table 1 Consequences of DR-only solutions

The core of a good business continuity strategy is to create a balance between cost-efficacy, staying within acceptable RTO's, and recovering data that is as "young" as possible. Additionally, implement a business continuity solution that allows your organization to restore your data via ***bare metal recovery***.

How to Create the Ideal Business Continuity Plan

Business continuity is a way to maintain or quickly resume business functions in the event of a major disruption, whether caused by a fire, flood, blackout, or a malicious attack on your network.

Realistically, while any business can expect *some* downtime after a loss incident, the ideal business continuity model is responsible for reducing your RTO's with suitable RPO's.

Step 1: Establish Metrics and Identify Key Business Functions

Without knowing what assets you are protecting (and what you're protecting it from), you cannot develop a plan to protect them. Determine and document:

- RTO's
- RPO's
- Compliance
- Threats and threat levels

Conduct a ***Business Impact Analysis***, or BIA, to identify the key functions of your business. The final result of your initial planning phase should be a document similar to this:

Mission/Business Process	Maximum Tolerable Downtime	Recovery Time Objective	Recovery Point Objective
Description of process i.e. Pay Customer Invoice	*72 hours*	*48 hours*	*1 hours*

Table 2 Sample BIA (Source: NIST Computer Security Division [6])

Step 2: Centralize Your Data

Data needs to be stored in a centralized primary enterprise storage system, such as a ***Dell Compellent or Tegile Storage***. Scattered storage is a different disaster waiting to happen, but in the context of a DRP/BCP, you cannot efficiently back up data which is not kept in primary storage.

Step 3: Utilize an Offsite Secondary Datacenter

The lifeblood and key to faster RTO's is your secondary offsite data center. If your current DRP has a secondary datacenter onsite, it will be exposed to the same conditions as your primary datacenter.

There are two ways to ensure the availability of your data via bare metal recovery with a secondary datacenter:

Select holistic technology solutions that enable reliable cost-effective bare metal recovery.

Option #1: Invest in secondary storage that is compatible to your primary storage system (ex. Dell Storage to Dell Storage or Tegile to Tegile).

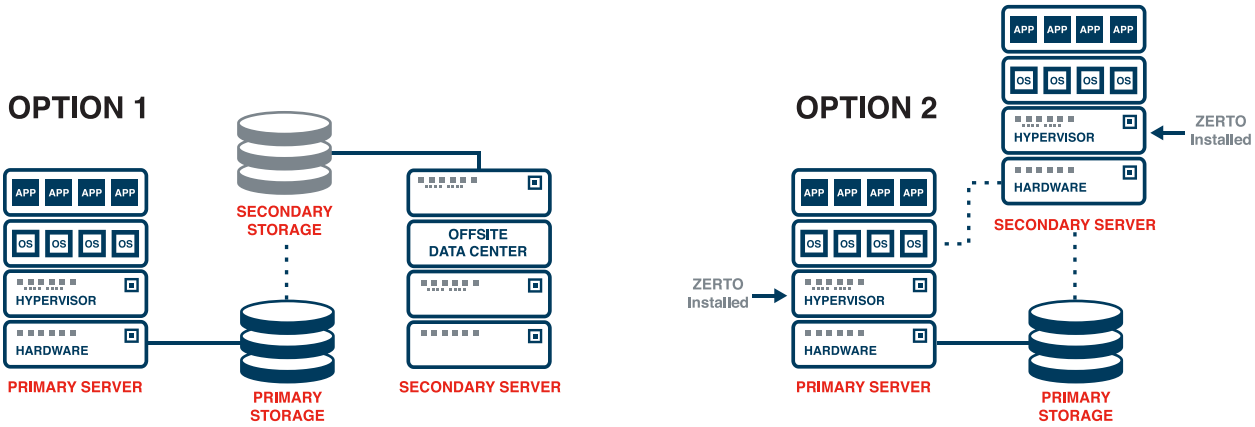
Option #2: If you do not have compatible secondary datacenter storage, take advantage of enterprise replication software that replicates your data from the hypervisor layer (like Zerto virtual replication software).

Configure your secondary storage to be an exact replica of your primary storage. If a disruption incapacitates your primary datacenter in any form, the secondary datacenter should be able to take over and carry the load.

In short, investing in a secondary datacenter ensures that you can:

1. Backup and replicate your digital assets across the infrastructure.
2. Enable easy recovery of your backup data via bare metal recovery.
3. Operate from your secondary datacenter until your primary systems are back.

Even if your employees have to work remotely as a result of displacement, they can still have secure access to important company assets via the offsite secondary datacenter.



Step 4: Comprehensively Test Your BCP

This is the most ignored step in DR planning. Without regularly scheduled, comprehensive testing, you might be missing several key factors in your recovery plan.

- Are you backing up data from all required resources?
- Are you utilizing your storage space efficiently with technology that offers deduplication?
- Are you able to effectively access your secondary datacenter once your primary fails?
- Is your plan updated to cover multiple data loss situations?
- Have you tested each different business process in the BIA?
- Do you have a way to communicate to your disaster response team after a catastrophic incident?
- Are you confident that each member your response team knows each of their roles?
- Have you tested multiple major and minor disruption scenarios?
- Are you documenting the results of your tests to make future improvements?

Keep a print and digital copy of your DRP/BCP document, and ensure that it is available throughout the organization.

40% of organizations in 2014 stated that their plans didn't work when they needed them to.

Conclusion

If you have a basic disaster recovery plan, your business is already ahead of the curve. However, the demands of the modern enterprise go beyond surviving a disruption, and are almost entirely focused on thriving regardless of circumstance.

Downtime, especially in the event of a natural disaster, is unavoidable, and striving to reach 100% uptime is not cost effective. That is what a comprehensive business continuity plan is for: to allow your organization to resume and continue normal operations after a loss incident within the shortest time.

Recommendations and Next Steps

1. Avoid being part of the 40% statistic: Establish whether or not your current disaster recovery plan will work in the event of an incident.
2. Establish whether your current disaster recovery plan will cover your business's post-incident needs.
3. Establish if you current business continuity plan meets acceptable RTO's and RPO's across every level of the organization.
4. Establish whether or not your current (if any) secondary datacenter can support your business if your primary datacenter is incapacitated.
5. Find a cost-effective DR/BC solution provider that offers a solution that can meet your specific recovery goals.
6. Work with a full-service IT solutions provider, instead of working with a DR/BC software manufacturer.

As opposed to searching for and contracting directly with the DR or BC software provider, a technology consulting firm will help you develop a comprehensive continuity solution.

Instead of only implementing a single recovery measure, an IT solutions provide will help you develop a holistic DR/BC solution which includes all of the safeguards mentioned in this report with the added value of preliminary and ongoing support.

About Centre Technologies

Centre Technologies is a privately-owned, leading IT company that provides IT solutions for businesses of all sizes in Texas and Louisiana. Since 2006, Centre Technologies has combined technology with business insight to create a customized set of services as unique as the organizations they were created for. Their approach to enhancing businesses with IT operates under the principle that, “Technology is the Centre of every business.”

Contact us directly to explore the value Centre’s mobility solutions can bring to your business.

Phone: 281-506-2480
Address: 480 N. Sam Houston Parkway E. Suite 100, Houston, TX 77060
Website: www.centretechnologies.com

Bibliography

[1] A. M. Association, “HIPAA Violations and Enforcement,” 2015. [Online]. Available: http://www.ama-assn.org/ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/hipaahealth-insurance-portability-accountability-act/hipaa-violations-enforcement.page?. [Accessed 9 April 2015].

[2] FEMA, “Protecting Your Business,” 23 September 2014. [Online]. Available: https://www.fema.gov/protecting-your-businesses. [Accessed 30 March 2015].

[3] E. D. Council, “Business Continuity Planning for Business,” 28 November 2014. [Online]. Available: http://www.eden.gov.uk/business-and-the-economy/economic-development/business-support-and-advice/business-continuity-planning/. [Accessed 30 March 2015].

[4] R. Dines, “Quantifying The Impact Of Downtime: What We Can Learn From Recent New York Times, Google, And Amazon Outages,” Forrester, 19 August 2013. [Online]. Available: http://blogs.forrester.com/rachel_dines/13-08-19-quantifying_the_impact_of_downtime_what_we_can_learn_from_recent_new_york_times_google_and_amazon_out. [Accessed 9 April 2015].

[5] I. B. Edge, “Downtime Report: Top Ten Outages in 2013,” 2014. [Online]. Available: http://www.itbusinessedge.com/slideshows/downtime-report-top-ten-outages-in-2013-05.html. [Accessed 9 April 2015].

[6] N. C. S. Division, “Sample BIA Template,” 26 November 2013. [Online]. Available: http://csrc.nist.gov/. [Accessed 9 April 2015].