DISASTER RECOVERY 101

3 Steps You Need to Take (Before It's Too Late)

Centre
TECHNOLOGIES

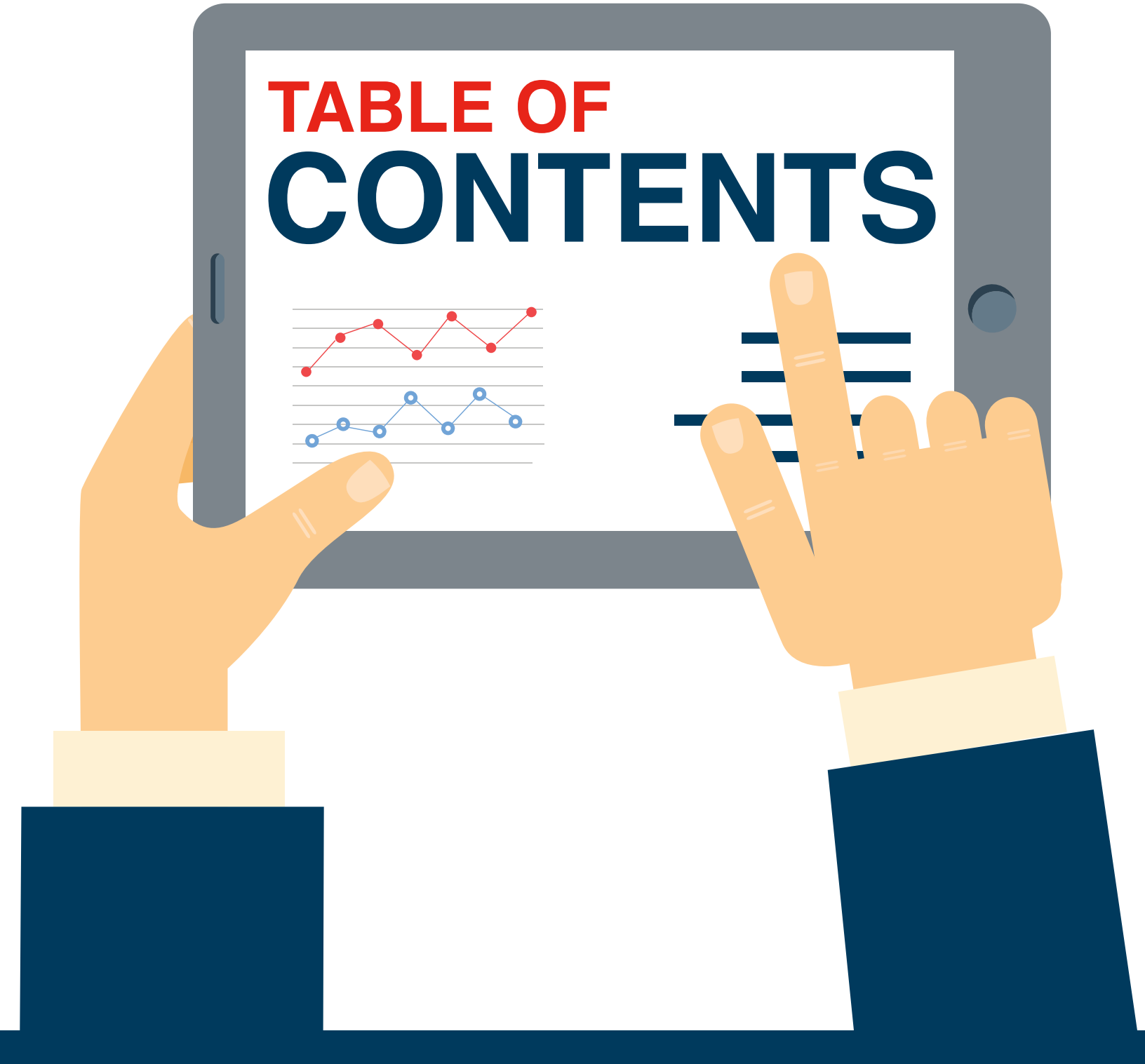
TABLE OF
CONTENTS

Introduction

In the world of IT disaster recovery, what exactly is, “too late?” Have a look at these statistics:

- According to FEMA, 40% of businesses never re-open after a disaster [1].
- 90% of businesses that lose data as a result of a disaster will close within 18 months [2].
- Over 70% of businesses who suffer from a major fire do not re-open or will close within 3 years [3].
- In 2014, 43% of companies experienced data breaches which crippled their ability to work [4].

Disaster comes in many forms, with the operative (and somewhat euphemistic) word being, “disruption.” Any incident that causes data loss is considered a disruption, including events as simple as a power outage, to events as major as a fire or hurricane.

“Too late,” for the modern enterprise, means being unable to recover after a disruption. Your ability to recover from even the worst of nature’s tantrums can make, or irreparably break, your business. It is time for a very straightforward discussion about disaster recovery and business continuity.

Disaster Recovery vs. Business Continuity

To clarify the difference between the two terms:

1. Disaster Recovery (DR): a plan for duplicating your critical business data with measures like automatic backup to an offsite datacenter.

2. Business Continuity (BC): a plan to resume business after a disaster with minimal data loss and downtime.

DR and BC are used together in context so often that many people think the terms are interchangeable. However, the two are fundamentally and functionally different, even if they have similar end-goals in mind.

From a DR standpoint, the only goal is to have a copy of the data somewhere safe, away from the disaster site. After a disaster, if a business only has a copy of their data, it could still take weeks for them to recover.

Business continuity, on the other hand, is a solution focused on restoring the business within a specific, pre-designated time-frame. BC focuses on the longevity and health of the business by putting measures in place to reduce downtime.

Why You Need to Read this eBook

When hurricane season comes, you buy extra canned foods, bottled water, and prepare your family to weather the storm. During wildfire season, you clear the debris around your home and take measures to control the spread unexpected fires. On a daily basis, you lock the door to your home and business to protect the important things inside. You store your important identity and financial documents in a safe place, hoping to protect them from damage or theft.

Why wouldn't you do the same for your data?

You need to read this eBook to protect your business's most important asset, your data, in the event of an unforeseeable disruption. After reading this book, you'll be able to:

- Identify the risks of neglecting a disaster recovery plan.
- Identify your data's critical enemies.
- Learn about technologies that can help you recover after a disaster
- Learn about the steps you need to take to safeguard your business's data.

This eBook offers a step-by-step formula to help guide you from risk assessment to solution implementation.

Chapter 1: The Risks (aka, The "Too Late" Scenario)

What is "too late?" The quickest answer is this:

Too late is AFTER you lose your critical data.

It is as simple as that. From an IT perspective, "too late" is called, "catastrophic data loss."

As residents in states that are at the mercy of the Gulf Coast, you don't have to be reminded of the devastation hurricanes can cause. The combination of wind and water damage is enough to render most businesses in a hurricane's war path completely helpless.

However, hurricanes are not the only things that can cause "too late" scenarios.

The Four Great Causes of Data Loss

Data loss causes can be broken down into four main categories:

- Human error and technical failure
- Criminal activity
- Power source issues
- Natural disasters

While each type of disruption poses unique challenges for your organization, the result – catastrophic data loss- remains the same.

Human Error and Technical Failure • Human error • Computer failure • Data corruption • Network failure • Software errors **Criminal Activity** • Hacking • Malware • Internal sabotage • Terrorism	**Power Source Issues** • Blackout/Brownout • Power surge • Power grid failure **Natural Disasters** • Hurricane • Fire • Flooding • Earthquake • Winter storm • Tornadoes

Table 1: Four Great Causes of Data Loss

Road to (Data) Recovery

You owe it to yourself and the health of your business to develop a strong and comprehensive disaster recovery and business continuity plan. If your business falls victim to a data loss incident, and you do not have a disaster recovery plan, there is a strong chance your business will join the 90% statistic [2].

Your business's only chance of surviving after a data loss incident – manmade, natural, or otherwise – is to take five steps on the road to recovery… before a disaster happens.

- Step 1: Evaluate risks and determine recovery thresholds.
- Step 2: Evaluate DR and BC technologies.
- Step 3: Test and maintain your DRP.

Chapter 2: First Steps - Creating Your Plan

How long can your business afford to be down? What resources do you need to function as a business? What digital assets are required to keep the trust of your clients and employees?

You cannot start planning your disaster recovery and business continuity strategies without first identifying what you need to run your business.

Step 1: Identity the Processes Critical to Your Business

These include the business processes that must be restored ASAP after a disruption. The Disaster Recovery Journal defines critical business processes as, "Business activities or information that could not be interrupted or unavailable for several business days without significantly jeopardizing operation of the organization" [5]. Depending on your industry, you critical activities could include:

- Giving nurses the resources to care for patients in a hospital
- Keeping the IT department functional to restore business to the rest of the organization
- Ensuring the encryption of your bank clients' financial information

Identifying your critical processes, ultimately, protects your assets, meets your critical business needs, and keeps your organization compliant with regulations.

Step 2: Document Dependencies

Outline the applications your critical processes depend on, and then diagnose each application's maximum acceptable downtime accordingly. This includes client financial records, security and encryption applications, the operating system, etc. Document which vital applications meet your dependencies.

In this phase, you should also determine which disaster personnel will be required to carry out the restoration of your vital applications.

Step 3: Perform a Business Impact Analysis, or BIA

At this point, you need to crunch some numbers. Conducting a business impact analysis will allow you to measure the impact downtime will have on different areas of your business. In a single document, you can determine availability requirements, estimate the cost of downtime (including revenue loss), and identify legal and compliance risks.

Step 4: Determine your RPO's

RPO, recovery point objective, is the point in time at which you can successfully recover your data. Modern enterprise backup solutions offer RPO's within anywhere from one day to one hour. The best solutions, paired with other technologies, can even bring your RPO's down to less than 15 minutes. In other words, your data is being backed up every 15 minutes. After a disruption, you need to know how "old" your backup data is. Define an acceptable RPO to share with your backup provider. Keep in mind: a lower RPO requires enhanced performance and resources to achieve, and it will increase your costs. That said, your RPO is dependent on your discovery in Step 1. In other words, your RPO is what your business needs it to be.

Step 5: Determine your RTO's

RTO, recovery time objective, is the span of time between a disruption and full restoration. Use your BIA to assess your business's maximum tolerable downtime, and use it to determine your desired RTO.

Step 6: Determine your MTD

MTD, maximum tolerable downtime, is literally the maximum duration of time your business can afford to be without the critical business processes you identified in Step 1 before causing irreparable harm to your bottom line.

You should only start looking into the appropriate business continuity and disaster recovery technology after you have completed your initial planning and risk assessment. This next chapter will give you an overview of the technologies available for your DR/BC plans.

Chapter 3: Next Steps – Finding the Right Technology

There are many players in the field of disaster recovery and business continuity. While it might be tempting to opt for bare minimum protection, choose a holistic DR solution that offers the full coverage you need based on your assessment in the previous chapter.

Key Features of an Effective DR Solution

With DR, your end goal is to optimize your resources to ensure the lowest TCO with the highest levels of protection for your business's digital assets.

- **Automatic Backup:**

Can you really remember to back up your data at regular intervals? Invest in a software solution that automatically backs up your data within scheduled intervals. Choose your software based on your required RPO's (sub 15 minutes, 1 hour, 1 day, etc.).

- **Replication:**

Replication differs from backup in that it copies and moves data between company sites, Replication creates operational copies of your data that can be used for business continuity.

- **Deduplication:**

Your backup solution should have built-in deduplication. This solution recognizes data that is a duplicate of another piece of data (ex: older versions of the same email thread). Deduplication allows for leaner storage of your backup data, lowering your storage costs.

- **WAN Optimization:**

Whether built into your backup solution or a separate investment, WAN optimization streamlines packet delivery for your backup data to the secondary data center and back. With WAN optimization, you can accelerate the pace and efficiency at which you transfer your information to and from the datacenter, cutting down your RPO's and RTO's significantly.

- **Bare Metal Recovery:**

The new standard of excellence in modern disaster recovery and business continuity solutions is the ability to deliver bare metal recovery. This means that the DR solution is able to recover data to the original environment without any previously installed operating system configurations. Bare metal recovery offers seamless revival to the environment after a disaster within the agreed upon RPO.

- **Environment Monitoring:**

You need visibility into your DR replication environment, and a DR/BC solution should offer visibility and some control. You should be able to see what data is being replicated, how it is being stored, and be able to access information about its configuration. Environmental monitoring gives you the power to proactively monitor the environment for signs of trouble long before a loss incident.

- **Secondary Datacenter or Cloud Repository:**

The most important feature in an effective DR solution is an offsite repository for your data. It makes no sense to have your secondary datacenter/storage on premise. If you do not want to invest in a secondary datacenter, you can opt for a secure, encrypted cloud repository solution with your local IT services provider.

An internet search will reveal hundreds of hits for local and national DR/BC providers, and your final solution may involve more than one product to ensure the most protection for the most value.

The mind boggling list of backup, restore, replication, and cloud providers can make it impossible for you to positively identify the right solution for your organization. Use your research and metrics to communicate your requirements to your prospective solution providers, and analyze the technologies they offer.

Chapter 4: Last Step – Maintaining Your Disaster Recovery Plan

Your disaster recovery and business continuity plans are not "fix-it-and-forget-it" arrangements. The most overlooked step in the process of implementing your plans is ***testing***.

The best practice for DR testing lies with the "test to fail" methodology.

Instead of creating scenarios and developing plans to see if your DRP succeeds, take steps to understand under which circumstances your plan will ***fail***, and only then will your organization find the real vulnerabilities in your DRP.

Ways to Test Your Disaster Recovery Plan

Walkthrough Tests

Walkthroughs are a "quick and dirty" way to test your DRP. Each member of the disaster team will verbally rehearse each step of the plan, starting with initial incident response. They will verbally cover each component of the plan until the point where normal operations resume. A walkthrough is useful for identifying large gaps and vulnerabilities in new plans and systems.

Checklist Tests

One of the most cost-effective routine DR tests is a checklist test. This covers vulnerabilities with daily, monthly, quarterly, or yearly maintenance tests to ensure the availability of critical hardware and software. For example, the checklist can include daily assessments on:

- Fuel levels for the backup generator.
- Up-to-date licensing on your DR software.
- Correct storage for generator fuels.
- Backups have been sent per protocol to the secondary site.

Simulation Tests

Simulation tests are "talking" tests that let DRP key-players rehearse their roles during an actual emergency. Your entire operation can run normally while your disaster recovery team rehearses notification procedures, interim operating procedures, and backup and recovery operations. During sim tests, the team should test all critical software, hardware, and human assets involved, as well as the stability of your communications. Sim tests can comprehensively provide the most flexibility with the least amount of disruption.

Failover/Failback Testing

Some providers offer the ability to partially or fully mirror your infrastructure through real-time replication to an alternate site. This gives you the ability to Failover your processing environment to the alternate site, drastically reducing or eliminating downtime. Periodic testing of either a partial or full Failover/Failback will provide the business continuity assurance you need.

The “Turn It All Off” Test

Also known as a full interruption test, this costly and disruptive form of DR testing mimics the conditions of the disasters your business has a high likelihood of facing. Ideally, you would schedule this type of testing to occur after hours or at a time period with the least amount of disruption to other employees and customers. Within this test, your team would create a controlled disruption event (power outage, DDoS attack, etc.) and take the steps needed to restore the system using the current DRP. Someone on the team should take notes on shortcomings, successes, and gaps in the plan. The test ends when all systems are back up to normal operations.

Conclusion

Throughout this eBook, we discussed the steps businesses need to take before the proverbial “too late” scenario.

- Step 1: Conduct risk assessments to determine your recovery objectives.
- Step 2: Develop a plan with proven enterprise backup technologies.
- Step 3: Continue to test your plan for vulnerabilities and efficacy.

Fortunately, you do not have to take these steps to protect your organization alone.

Centre Technologies is an enterprise IT solutions provider serving businesses throughout Texas and Louisiana. We understand the unique threats inherent in our geography, as well as man-made threats like human error and malware attacks.

Why Centre Technologies?

1. Centre is an IT solutions industry leader that never stops innovating and never stops investigating new ways to mitigate new threats.
2. Our proven methodologies ensure the ultimate safety and performance for your network.
3. Our solutions guarantee the security and availability of automatically backed up data.
4. We address common misconceptions about DR/BC solutions and establish a partnership based on business value.
5. We work closely with our clients to help them reach their business goals.
6. We provide local, enterprise-class support to businesses throughout Texas and Louisiana.
7. We pass the value of working with our best-of-breed partners to you and your business.
8. Our certified and experienced IT professionals consistently meet and exceed our contractual SLA's.
9. Our services combine the capabilities of an enterprise class service with the personalized attention of a local provider; the only IT solutions partner in Texas that can provide the best of both.
10. We offer multiple network operation centers and redundant tools from two separate geographic l locations to ensure 24/7/365 support.

Contact Centre Technologies

Let the disaster recovery experts at Centre Technologies take the steps necessary to protect your data and your business. Contact us directly for more information about our disaster recovery solutions.

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

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."

Bibliography

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

[2] C. Mullen, “Chamber 101,” 2015. [Online]. Available: http://www.chamber101.com/2programs_committee/natural_disasters/disasterpreparedness/Forty.htm. [Accessed 15 May 2015].

[3] C. Central, “Business Continuity Statistics: Where Myth Meets Fact,” 2009. [Online]. Available: http://www.continuitycentral.com/feature0660.html. [Accessed 15 May 2015].

[4] E. Weise, “43% of companies had a data breach in the past year,” 24 September 2014. [Online]. Available: http://www.usatoday.com/story/tech/2014/09/24/data-breach-companies-60/16106197/. [Accessed 15 May 2015].

[5] D. R. P. Council, “The State of Global Disaster Recovery Preparedness Annual Report 2014,” 2014. [Online]. Available: http://drbenchmark.org/wp-content/uploads/2014/02/ANNUAL_REPORT-DRPBenchmark_Survey_Results_2014_report.pdf. [Accessed 15 May 2015].