tlc SOLUTIONS

DISASTER RECOVERY PLAN

A Guide to Creating Your Own

TABLE OF CONTENTS

Introduction.....3

Disaster Recovery is a Must to Ensure Business Continuity.....3

Building a Disaster Recovery Plan.....5

Different Backup Solutions.....9

Common Backup Techniques.....11

Sample Backup Software and Features.....12

Disaster Reocvery Doesn't Have to be Expensive.....13

Critical Things to Back Up.....15

The Recovery Plan.....17

Elements of an Effective Disaster Recovery Plan.....17

Conclusion.....19

About TLC Solutions.....20

INTRODUCTION

Disasters, natural or due to human error, almost always strike at any time, usually without a moment's notice. Even the largest cities deal with the effects brought about by floods, fires, tornadoes, earthquakes and hurricanes. Japan had experienced a devastating tragedy during the 2011 9.0 magnitude earthquake and tsunami. This has left over 900,000 buildings damaged and halted operations of many large corporations based in Japan. And we can't forget the natural disaster that brought New York City and the American financial district to a standstill – Hurricane Sandy. More than 25% of the US population have been affected.

These tragedies have forced the world to rethink its emergency preparedness programs and emergency alert systems. And this should make you think twice about the security of your business and data. After all, disaster management and business continuity plans are important for maintaining an edge in today's competitive business environment.

DISASTER RECOVERY IS A MUST TO ENSURE BUSINESS CONTINUITY

With disasters comes the risk of losing data that's critical to your business. It should come as no surprise then that some companies that have lost critical data end up going out of business within a year. The recovery of your data is just as important as how secured it is stored. The risk is high and becomes very obvious in the time of need, if creating a disaster recovery plan is overlooked. It affects not only your business operations but also your clients who make use of your products and services.

Talking about downtime costs, IDC research states that we can look at an average cost of about $100,000 per hour, climbing to about $1.6 million per hour for some organizations. Even with disasters not happening, IDC research disclosed that

most organizations still suffer an unplanned downtime of about 10 – 20 hours per year.[1]

The challenge grows as businesses experience influx of big data. This means that there is an equally increasing need for a resilient and robust disaster recovery plan that's strategically aligned it modern approaches to drive better reliability and business continuity.

Businesses are seeing this need and are now actively pursuing a disaster recovery plan that suits their needs. So, congratulations on taking that first step to securing your business data and guaranteeing your successful comeback in the event of a disaster that wipes out your critical data. We hope that the information in this guide will help you in planning a solid Disaster Recovery Plan and ensure the security of all your data!

[1] IDC, Leveraging the Public Cloud for Faster Disaster Recovery at Lower Cost, May 2015

Building a Disaster Recovery Plan

There are five key aspects into implementing a successful Disaster Recovery Plan (DRP) – Network Audit, Business Impact Analysis, Planning, Storage and Recovery.

Network Audit

It is good to start fully knowing and understanding the capabilities and identify the gaps (if there are any) in your network and infrastructure. It would be wise to start the process of creating your own DRP with full knowledge of your systems, to understand which DRP solutions would best fit your network's requirements in order for the DRP to be successful.

If you want further guidance on completing an audit of your network, we offer free network assessments as well. You can give us a call and schedule your no-obligation consultation with us.

Business Impact Analysis

The network audit is a key first step that paves the way for performing a business impact analysis. By now, you should have a list of all the processes that your company uses to deliver your products and services. Partner those processes with the resources (employees, partners, IT infrastructure, and technological assets) they need to power up.

Then start asking yourself these questions:

- How is crisis going to impact your business?
- If you lose a week's or a month's worth of data, would you still be able to operate and deliver your products and services?

- In the event of complete wipe out (fire or complete system failure, etc), how long is your business going to function without your data (your maximum tolerable period of disruption or MTPOD)?
- What are my business' legal liabilities should we fail to deliver the agreed upon products and services to our clients?
- What's the warranty status of all my hardware?
- Do we have a capable support technician on board who could restore my business data as soon as possible?
- Do I have an inventory of all the software and hardware that are critical for my business?
- Does my backup work? When was the last time I checked it?

Be sure to address all these (and more if need be) in order to get a full picture of how your business will survive and how much impact data loss would be should a disaster happen.

Planning

In order for all project implementation to be successful, careful planning should be done – all T's are crossed and all I's are dotted. This shouldn't become as tedious as it could be if you've done your due diligence and done a Network Audit prior. Since you already have the knowledge from your completed audit, you may just fill in the details and as the IT Manager, assign key people in the company with their roles and responsibilities during a disaster recovery scenario. Make sure the communication channel is clear and that people know who their primary, secondary, and alternate contacts are in a crisis or a major IT issue. A strong chain of communication can be the difference between a temporary outage and a big business disaster.

Since you would've known by now your MTPOD, it is time you plan for your Recovery Time Objective (RTO) – the goal you've set for how long a recovery will take. With this goal in mind, start preparing the recovery plans for each team and department of your company.

These plans should include:

- Tasks that need to be done in a crisis
- People assigned for each specific task
- Key contact people for communication
- Hierarchy of priority information to be recovered
- How much data stored in a hard drive or cloud at a time
- Regular backup testing
- Regular network auditing

Basically, a solid Standard Operating Procedure that all of the company employees are aware of, completely understand, and would be able to implement in the event of a crisis.

Storage

Backup and post-disaster storage are of utmost importance as any of the key elements in building your own disaster recovery plan. For this part to be a success, partnering with a trusted and reliable brand or company for your backup and storage method and provider is key. There is no one-size fits all backup storage solution. Each company's needs are different, with regards to how much data is needed to be back full swing after a disruption or compliance regulation.

- Small-scale companies or those with non-specific needs could opt for managed backup providers or go for cloud backup services.
- Large companies with more specific data requirements can choose an in-house solution that's tied in with their existing IT staff.
- Companies that are gradually growing could opt for a backup solutions that's scalable and could grow with their needs without too much hassle on costs and hardware.

So now, what are the key requirements for choosing a backup solution?

- Recovery data should be kept in multiple different physical locations by a significant distance. (e.g redundancy and duplication of stored data in multiple data centres by cloud providers)
- The recovery data should be stored securely in a physical media not located in your office. (e.g HDD stored in a firebox)
- Warranty status of hardware coincides with your RTO (e.g next business day warranty)

Recovery

What makes for a prompt recovery to take in place in the event of a crisis? Great detection and monitoring. This includes having a system in place that keep tracks of and alerts you of disasters – the obvious and especially the non-obvious ones like fire or outage when no one is in the office, physical or cyber intrusion with malicious intent. The faster the detection, the faster you can jump right into your planned recovery process.

Make sure you have created a “survival gear box” that contains the following:

- Business continuity plan documentation
- Team and department recovery plans
- Key information about IT infrastructure
- Product (hardware and software) serial numbers
- Contact information of key personnel during crisis
- Practical items – bottles of water, flashlight, first aid kit, cellphone, laptop, canned food

A good recovery plan should be tried and tested to ensure that it will indeed work in a time of need. Running crisis simulations and practicing test runs should be all you need to do to know the extent of how effective your DRP is. Be consistent in testing your backup – whether it be monthly, quarterly or yearly. Recover data in another computer or laptop and see if it runs smoothly to test out the integrity of the data backup solution.

Different Backup Solutions

Full Backups

This solution allows you to select the folders and files from your drive to backup. Each time this runs, it copies all the selected files and folders in their entirety to your backup storage. It is important to note that this requires a lot of time and may need more storage space than usual.

Differential Backups

Differential backups are usually done partnered with full backups. What it does is it copies only the files and folders that have changed since the last time they were fully backed up. This type of solution overwrites the changed files multiple times. This takes up less time and space but data recovery through this can get complicated as you'd need to do a two-step recovery – backup from most recent full backup and then apply the last differential backup.

Incremental Backup

This is very similar to differential backups that it's also in conjunction with full backups. The only difference is that it copies the files and folders that have since changed from the last backup, no matter the type of backup. This means it

doesn't copy the files that have been changed multiple times, which results in a quicker backup time and smaller storage space needed than differential backups. However, backing up from incremental backup becomes tedious as steps can take as many as how you set up incremental backups. You recover your data by applying the most recent full backup and apply each incremental backup.

System Image Backups

This is a higher level backup solution that backups your files by creating a system image of the drive, copying section by section instead of file by file. It doesn't just include files and folders (like full, differential, and incremental backups), but your entire drive – operating system, programs, drivers, system settings.

IT and support Technicians usually prefer this as this could certainly guarantee full restoration of a computer that's crashed to the state it was when the system image backup was created. This means they won't have to create your entire system from scratch and put the files and folders where they belong. Downside to this is takes quite a long time to backup and requires large storage space – as large as your drive. This method also can't restore just one file (even if that's all you needed), you'd have to re-image the drive and restore all files.

Continuous Data Backups or Versioning

This backup solution backs up data that has changed every time you save. However, they do not overwrite the data, but takes a snapshot of the modified data, and keeps each snapshot taken. This then allows you to restore a file to a version at any particular point in time. You can also pre-set the intervals to create near-continuous data backups and you can restore a file to any version at a particular interval.

Loss of data is minimal in this case but it does take up a lot of bandwidth and resources. This could also prove to be more expensive as it uses continuous data protection (CDP) technology.

Common Backup Techniques

Full and Differential Backup

Sunday – Full Backup
Monday – Differential backup (backup changed files from Sunday)
Tuesday – Differential (backup changed files from Sunday)
Wednesday – Differential (backup changed files from Sunday)
Thursday – Differential (backup changed files from Sunday)
Friday – Differential (backup changed files from Sunday)
Saturday – Differential (backup changed files from Sunday)

Full and Incremental Backup

Sunday – Full Backup
Monday – Incremental back up (backup changed files from Sunday)
Tuesday – Incremental (backup changed files from Monday)
Wednesday – Incremental (backup changed files from Tuesday)
Thursday – Incremental (backup changed files from Wednesday)
Friday – Incremental (backup changed files from Thursday)
Saturday – Incremental (backup changed files from Friday)

System Image Backup

Every two weeks or a month
Continuous Data Backups
Can be pre-set to every hour

Perform backup using the 3-2-1 rule

Storing your backup locally is a first line of defense but it is not sufficient. Data protection experts advise using the 3-2-1 rule (three copies, two types of media, one offsite location) when planning for DR strategy.

Be sure to have two external hard disk drives (HDD) with adequate storage that you can swap every two weeks or every month, depending on the amount of data you'd need to be fully back up from a total data wipeout because of a disaster. Your business impact analysis should be able to tell you this information. Make sure the other one is in a safe location (apart from your office) stored in a secured place (like a firebox, vault). And if finances allow, a duplication or redundancy stored in a cloud service provider.

SAMPLE BACKUP SOFTWARE AND FEATURES

Veeam Backup & Replication 7[2]

Backup Copy Job
This feature gives the backup administrators the power to copy the backup files to a secondary repository – either onsite or offsite. The copied files have the same format as Veeam Backup files and can be used to perform the same restore operations as the original files including Instant VM Recovery, file-level recovery, etc.

[2] A Guide to Business Continuity and Disaster Recovery Planning and Implementation Using Veeam

Moreover, Veeam Backup & Replication offers a built-in WAN Accelerator that helps transfer these files to an offsite location through a connection of any speed – even unstable links. Veeam WAN Acceleration uses both global data deduplication and global data caching, making data transfer across sites up to 50 times faster.

Backup to Tape

Apply best practice by allowing administrators to archive backup files to the Tape Library. In addition to archiving backup files, it can also archive any other files using Windows Tape Format.

Veeam Backup & Replication is able to manage the Tape Library using several methods, including tape barcoding, media pool management and custom retention policy per set.

Disaster Recovery Doesn't Have to Be Expensive

There is a notion that because of the nature of complexity of these backups, it could be quite expensive to implement. But if you know your system requirements and your recovery time objective (RTO), you can opt for one that would give the most bang for your buck.

Balancing your cost against the time to recover (RTO) requires an in-depth understanding of your application's RTI/RPO requirements and the technologies to meet them. Given the advancements in network optimization, data compression, and data deduplication, the expectation that suitable DRP has to be expensive is outdated. This has been further promoted by new developments in cloud-based DR architectures that yield to even more DR cost savings. These technologies have enabled IT departments to build affordable alternatives to expensive replication schemes without sacrificing and even improving RTO and RPO over tape-based disaster recovery. The ultimate goal for nearly any business is to build a recovery service catalog with mid-tier options that scale with changing business requirements.

Below is a table showing recovery catalog that builds on scenarios described earlier and includes two generally accepted approaches for affordable, scalable disaster recovery. These recovery tiers can easily implemented in the cloud to minimize the need for acquiring target recovery assets and data center space, as well as provide a "pay per use" DR procurement strategy. This can be easily valuable for corporate assets that are remote and beyond the reach of a traditional hub and spoke approach.

	Tier 1	Tier 2	Tier 3	Tier 4
Example Technology	Sync/Async, CDR, Application, Replication	LiveSync, Replicated Snapshots	Disk-Based Backups	Restores from Tape
Application Business Continuity	Business Critical Applications	Business Sensitive Applications	Business Sensitive Applications	Non-Critical Applications
Disaster RPO	0-15 Minutes	Snap Freq based 4-24 Hours	Backup Frequency based 6-24 Hours	36 Hours
Disaster RTO	Less than 4 Hours	12-72 Hours	12-72 Hours	Best Effort
Relative Costs	$$$$	$$$	$$	Many Hidden Costs

Table 1 – Representative Recovery Catalog

Tier 1 – Synchronous, asynchronous, and application replication will remain among the most aggressive RPO/RTO capable solutions. This option requires traditional backup for day-to-day recovery purposes.
Tier 2 – Near continuous and replicated snapshots provide a cost effective alternative to sync/async replication, with relatively low recovery time and

minimal data loss. Snapshots can also provide operational recovery capabilities that can integrate with backup processes.
Tier 3 – Replicated, deduplicated, disk base backups (DASH copies) are typically lower cost than technologies in Tier 2, yet can provide the most flexibility and value. This approach can be used for DR between core datacenters as well as for edge-to-core, remote-site-to-core protections, as well as DR to the cloud.
Tier 4 – Tape based backup may be slow to disappear. It still may have a legitimate place in your data protection scheme. However, consider the potential hidden costs and scalability issues compared to alternatives. [3]

Critical Things to Backup

While regular full system backups are ideal for disaster recovery purposes, they are not always cost-practical and doable. If you are limited in terms of funding and time, just be sure to backup these mission critical things daily.

Critical Applications

- Applications critical to operations of your business
- Active Directory (domain)
- Accounting software data
- All backend software data and processes that run the business
- Email Server

Company Data

- Shared folders
- Business contacts (outside vendors, partners, contracts, clients)
- Transaction records (credit card, receipts, invoices, billings)
- Employee data
- Electronic communications (email, text messages)

[3] Balancing Cost, Risk and Complexity in Your DR Strategy, Commvault

Get a really good software that can schedule your large amount of backup data successfully during off-peak hours. Transferring large amounts of data can create all kinds of troubling scenarios – eat up your network bandwidth and affect employee productivity, slow down internet speed, drop VoIP calls, etc. So ensure that the software you will be using is well-equipped with identifying resources failing to back up properly and notify you of and rectify the issue. And schedule nightly backups for less interruptions.

To clarify, applications themselves are not backed up, what's being backed up is the data for these critical applications. In an image level backup, the applications are backed up but would not be restored only from an image, it would have to be the full server/workstation that the image was taken from.

Examples

In Active Directory, the "system state" would be backed up. So when restoring Active Directory, the best practice is to use an image of the Active Directory Server and restore the machine in its entirety. Experts would restore the system state to the most recent backup of the system state.
For software like accounting software, the accounting data from the software would be backed up. In the event that there is an accounting server and images of the server are being taken, then restoring it in its entirety is possible and then continue to restore the data to the last data level backup. Otherwise, if it's just a software, re-installing the software is necessary before you can restore and use the data for that software.

THE RECOVERY PLAN[2]

Performing backup and replication without a recovery action plan is not sufficient.

Backup administrators should deal primarily with the following situations:

Partial Failures

In this situation, some of the services are experiencing an outage. As a first line of defense, the local backups should be used. Compared to the legacy backup solutions, Veeam provides an innovative yet easy and fast way to leverage the backup files taken locally: Instant VM Recovery. This technology allows the hypervisor to start any virtual machine (VM) directly from the backup storage without performing any staging activities, thus allowing normal operations to resume in minutes. In some cases, it would be enough to perform OS file-level recovery or granular Application Item Recovery, which can also be carried out directly from the backup without the need to re-hydrate data or prepare any additional resources.

Total Failures

In this case, the main suite is blacked out because of a hazard. The Disaster Recovery (DR) site will take over the production site until it is brought back online. Veeam replication technology provides a smooth transition using an intelligent Failover mechanism as described above, and similarly when the main production site comes back online through Failback.

ELEMENTS OF AN EFFECTIVE DISASTER RECOVERY PLAN

So now that you've mostly put together your Disaster Recovery Plan, there are just a couple more things to take note of ensure it is effective and when enforced, will truly be a success.

Data Management

This involves having full knowledge of all of your document's lifecycle and their importance. This should lead you to knowing when to destroy a particular document, where to place it to minimize legal risk, their regulatory compliance risk, and the cost of their storage and management.

Since you've already planned for who would be responsible for each team and department, make sure that they know to properly manage the company data that they are responsible for. Accessibility of the data they're handling in the event of a recovery process is important to know. Another important responsibility is the ability to determine the importance of each document and how long their operational and legal lives are. Allotting the necessary virtual and physical space to these documents are dependent on how important they are and understanding when to dispose them is also key to an effective data management.

DRP Audit

The integrity of any Disaster Recovery Plan can only be proved successful if tested and audited on a regular basis. The fact of a disaster is that it happens unexpectedly, and so are changes to data regulations and compliances. This perspective forces you to think twice and use diligence to cover all your bases as disaster is not a matter of "if" it happens but "when" it does. Thus, making sure you have also created an audit process that you commit to regularly is a wise decision. Consult with either an internal or external resource if you will to oversee and review your DRP. This audit will prove useful in ensuring that your strategies and policies are still aligned with your business and are implemented.

CONCLUSION

The survival rate for companies without a Disaster Recovery Plan is less than 10%. With this low of a chance for business survival, it has become imperative for a solid DRP to be put in place. Disasters, due to natural or human error, cause a lot of trouble – major interruption of work, decreased productivity, loss of data, and loss of potential earnings.

Make it an absolute priority to safeguard your intellectual properties and ensure the successful restoration of your business and its operations in the event of a disaster. Start the process of creating a Disaster Recovery Plan your business that's solidly designed for success. And if you have one already in place, have you done due diligence to ensure its effectiveness and success rate?

TLC Solutions and its team of experts have been successfully creating and implementing Disaster Recovery Plans for businesses that are tailored to their specific needs. We have developed best practices throughout the years and have partnered with a variety of world class industry vendors to guarantee a fail-safe plan for all partners for their disaster recovery efforts.

If you want further information with regards to Disaster Recovery Planning, give us a call and schedule your no-obligation consultation. We will even provide you with a free network assessment to make sure all your infrastructure and systems are up to standards, and give you a recommendation of what needs immediate attention to prevent any network issues.

About TLC Solutions

TLC Solutions is a team of motivated, highly qualified IT & Communications Specialists serving businesses throughout Western Canada. We offer managed services, strategic consulting, cloud hosting, network redundancy and disaster recovery. We also provide a full range of communications services including satellite, microwave, and fiber optics. We understand that every business is unique and we ensure the services we provide are specifically tailored to your needs. While we specialize in remote access communications networks for resource-based industries, we excel in all environments – from the hinterlands of northern British Columbia to downtown Vancouver.

Our Backup & Disaster Recovery Partners

Find Us