BUSINESS CONTINUITY PLANNING E-BOOK SERIES

DISASTER RECOVERY

For the Hybrid Cloud Era

3rdelement
CONSULTING
www.3rdelementconsulting.com

Contents

3rdelement
CONSULTING

What is Business Continuity?

Organizations relying on traditional disaster recovery strategies such as secondary data centers for backup sites, pass up additional services and the convenience associated with hybrid cloud-based disaster recovery. The cloud era has been a game changer. Traditional disaster recovery can indeed hold companies back unless they're willing to adopt and adapt.

3rdelement
CONSULTING

Backup is Not Disaster Recovery

It's a common misconception that backup and disaster recovery are the same thing. The two certainly work together, but it's important to understand that backup is not disaster recovery and vice versa. Furthermore, disaster recovery should be an essential part of an organization's IT strategy; even more so as security breaches and network outages increase with the accompanying increase in the cost of downtime. When decision makers are in the infant stages of planning their disaster recovery strategy, they often mistake what constitutes a disaster recovery plan (DRP) with data backup and assume the latter is a sufficient precaution when disaster strikes. Below, we distinguish between backup and disaster recovery and provide a quick definition of each.

Distinguishing backup from disaster recovery

Backup is when your data is "corrupted or lost and you need to restore your data or infrastructure to the original location or a new location". Your data can be situated on and backed up to a tape drive, separate storage in your data center, or even a completely different geographical location.

3rdelement CONSULTING

Disaster recovery entails running your sites, servers, or applications in a secondary datacenter in the event of a catastrophic failure. This entails having a plan and a technical solution to ensure that the core components of your business continue function should a disaster strike.

Technopedia explains that: “Disaster recovery planning is just part of business continuity planning and applied to aspects of an organization that rely on an IT infrastructure to function. The overall idea is to develop a plan that will allow the IT department to recover enough data and system functionality to allow a business or organization to operate – even possibly at a minimal level.”

Why you need more than backup

The purpose of backup is to protect and restore data at a granular level. This means that if, for example, files become corrupted, you can restore these files from the backup. However, if you want to replicate data, configurations, and applications in the event of a disaster, you would need a disaster recovery plan.
Although backup and disaster recovery are related insofar as they both backup and restore data, they serve different purposes. Both services are important as backup keeps your data safe and recoverable and disaster recovery keeps your workloads available when disaster strikes.

3rdelement CONSULTING

Cloud Based - 4 Pitfalls to Avoid

Disaster recovery is crucial to ensure continuity when disaster strikes. However, developing a disaster recovery plan can be difficult, full of pitfalls, and time consuming if done incorrectly. Despite this, many organizations neglect to invest in proper disaster recovery measures citing resources, finances, and time restraints for not implementing a solution. It seems there is a fundamental lack of understanding of the consequences of poor disaster recovery measures and the fact that such consequences more often than not far outweigh the investment.

Here are 4 pitfalls to avoid when planning and implementing cloud based disaster recovery.

Lack of data redundancy

Organizations often neglect to establish a reliable way to recover their data and maintain business continuity when disaster strikes. Implementing data redundancy can accomplish this goal. Data redundancy entails storing

3rdelement CONSULTING

multiple copies of your data in different environments, both online and offline. The general suggestion is to keep at least three copies of your data – two sets of backups in different locations and one offsite. Should you later experience data loss or a network failure, you have multiple backups in multiple locations, and you can recover and restore your data from one of these data environments.

Not focusing on business needs

Organizations often end up spending more time on analyzing technology, data locations, and vendors than on understanding the needs of their business. Organizations (and key stakeholders) should first consider what is most important to them should downtime occur or disaster strike before thinking about the technology that underpins disaster recovery. Important factors include, but are not limited to, access to email, to CRM systems (for sales personnel), to a functional financial management system, etc. Understanding the business needs of your organization will guide you to prioritize and conduct a proper assessment of your disaster recovery plan and disaster recovery technologies.

3rdelement CONSULTING

Underestimating recovery time

Underestimating recovery time is undoubtedly one of the most expensive pitfalls for any organization. It is also one of the pitfalls that most organizations become aware of too late. Organizations often focus their business continuity efforts on protecting and storing backups of critical business data offsite to save money. However, they do not consider the recovery of the stored data under the numerous scenarios that can occur when disaster strikes. Having full knowledge of the recovery time of the business as well as the factors that influence such recovery could lead you to make different choices in regard to technology and service partner.

Inadequate testing

A disaster recovery plan is only useful if it works. It follows that it is crucial to regularly test your plan under simulated disaster conditions. Testing your plan regularly will ensure you have considered all contingencies and can ensure business continuity. However, testing takes time and resources away from daily operations and are often a challenge for IT departments. Although we acknowledge the time and resource constraints, these can be countered by testing over weekends or at night. The bottom line remains: Unless you have a fully tested disaster recovery plan you will not be prepared to weather the challenges when the real disaster strikes. The goal in testing your disaster recovery plan is to embrace finding and eliminating issues so that all stakeholders have confidence in the plan when a real disaster event happens.

3rdelement
CONSULTING

3 Levels of Data Loss and Disaster Recovery Steps Applicable to Each

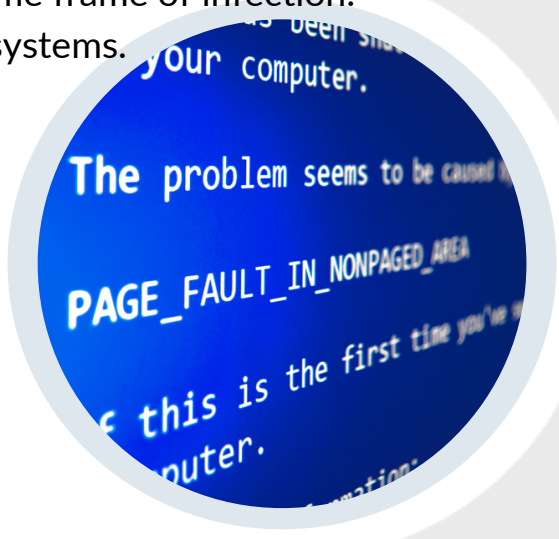
Data loss is a serious problem for businesses of all sizes and even a minor loss can result in lost hours, missed opportunities, and lost revenue. Every business has the potential for data loss. Data loss can occur for various reasons including but not limited to data being deleted accidentally or data becoming corrupted as a result of viruses, physical damage or formatting errors.
You can, however, limit the consequences of potential data loss by understanding the three levels of data loss and the disaster recovery steps to take when each occurs.

Application issues or minor data loss

The first level of data loss refers to application issues or minor data loss that can occur. Minor data loss can include a file or directory accidently being deleted.

What should I do?
Isolate: Identify the source and disconnect from the network.
Identify: Identify all encrypted files and time frame of infection.
Recover: Recover all encrypted files and systems.

3rdelement
CONSULTING



Primary infrastructure

This second level of data loss can include loss of primary storage, loss of a switch or firewall, a breakdown in internet connectivity or loss of public cloud, loss of data center power and failed data, application, or datacenter migration.

What should I do?

Identify: Find your most recent backup.
Rebuild: Rebuild or restore your systems, applications and data.
Restore to Service Level Agreement: Storing backups on disk outside of your primary infrastructure is critical to preventing large scale corruption.

The "crater"

As the name indicates, the data loss associated with “the crater” is the most severe and usually associated with a form of complete and permanent destruction. These include permanent damage (fire, water, etc.), denial of access, an act of God (weather/nature) and the destruction of infrastructure.

What should I do?

Declare: Invoke your Disaster Recovery/Business Continuity Plan.
Setup: Establish your new location.
Restore: Restore all of your applications, systems and data.

It is clear from the three levels of data loss and the disaster recovery techniques applicable to each, that it is essential to have an effective disaster recovery plan. The next chapter outlines how to develop an effective disaster recovery plan.

3rdelement
CONSULTING

How to Develop an Effective Disaster Recovery Plan.

The need for an effective disaster recovery plan to guarantee uptime and minimize data loss when disaster strikes is a necessary part of any organization's risk management strategy. Developing your disaster recovery plan will get you thinking about where your company is potentially exposed and how to find a solution to counter the exposure. The end result is a contingency plan that will have your operations up and running in the shortest amount of time.

Identify the scopes and boundaries of your disaster recovery plan

This means prioritizing your organization's critical disaster recovery systems and assigning a value to those systems if they fail.

Allocate a budget to your disaster recovery plan

When setting the budget, you have to ensure that it is done realistically with a clear understanding of the risks involved.

Develop and deploy the plan

This is the most complex part of the process and should focus on the activities that must occur when disaster strikes. It also entails choosing the necessary tools and technologies to drive your disaster recovery strategy.

3rdelement CONSULTING

Test the plan

An effective disaster recovery plan is a plan that has been thoroughly tested and updated when required.

When disaster strikes, an organization that failed to develop an effective disaster recovery plan will undoubtedly suffer disastrous consequences. These consequences can include operational, financial and reputational damage. Business owners need to realize that no company is secure.

Cloud-based disaster recovery management makes recovery planning easy for business of all sizes. It enables a faster and more streamlined approach and ensures that crucial information is directly available to the people who needs its most in a disaster situation.

To ensure the success of your disaster recovery plan and that you have the best possible support when disaster strikes, you will need a strategic disaster recovery partner, which is the topic of our next chapter.

3rdelement
CONSULTING

5 Tips to Find a Strategic Partner

Choosing the right disaster recovery partner, is critical to limiting your risk and collaborating with a partner you can trust to achieve your objectives. Below we have listed 5 tips to get you started:

Certifications are usually indicative of the platforms that your partner is qualified to support. Determine whether your disaster recovery as a service (DRaaS) partner has the required expertise in the platforms and applications you use.

Geographic diversity. It is an established practice in disaster recovery to have your disaster recovery solution in a different location than your primary business.

A DRaaS partner that can offer multiple solutions are usually able to deliver a more flexible disaster recovery solution.

Synchronous replication is more expensive than asynchronous replication. Operating within your budget means managing costs; ensuring your RPOs and RTOs reflect true business needs is one way to achieve this.

Your disaster recovery partner should offer solutions that allow the testing of DRaaS systems with minimal to no disruption to your business operations.

3rdelement CONSULTING

Conclusion

The focus of this eBook is disaster recovery in the hybrid cloud era. It commenced with highlighting the fact that backup is not disaster recovery and warned businesses of the four pitfalls to avoid when engaging cloud-based disaster recovery. Next it provided a succinct guide to the three levels of data loss and how to leverage disaster recovery to address each. It concluded with the steps to develop an effective disaster recovery plan and to find a strategic disaster recovery partner.

About 3rd Element Consulting

3rd Element Consulting is a woman-owned Managed IT Service Provider. For more than 15 years we've worked with local government, law enforcement and professional service organizations. Their IT has to work; lives can hang in the balance. Our clients are able to simply Consider IT Solved.

BIBLIOGRAPHY
https://adinermie.com/backup-not-disaster-recovery-need-fully-covered/
https://www.techopedia.com/definition/1074/disaster-recovery-plan-drp
http://info.us.ntt.com/rs/nttamericainc/images/WP-Top10DisasterRecoveryPitfalls.pdf
http://www.whitehattechs.com/2019/02/UBAH-Part1.html
https://www.tierpoint.com/the-strategic-guide-to-disaster-recovery-and-draas/

3rdelement CONSULTING
717-763-6800