eGUIDE

OneNeck® IT SOLUTIONS a TDS® Company

presents

Are you and your DR Plan feelin' lucky?

Surviving a Data Center Disaster Requires More than Luck. It Requires Preparation.

Even though we regularly celebrate Saint Patrick's Day, IT professionals know better than to trust to the luck of the Irish when it comes to disaster recovery. As IT experts know, it's never a matter of if a data center disaster will strike, but when. So top of mind for most IT managers is how they are going to protect business-critical data and what strategies they need to have in place to restore that data when disaster strikes.

According to IDC, 80 percent of small businesses have experienced some kind of data systems failure in the past, at costs ranging from $82,000 to $526,000, or from $137 to $427 per minute. Data is the lifeblood of most businesses, so when the data stops flowing, business stops.

Read more...

FEATURE

Disaster Recovery vs. Business Continuity: What's the Difference?

DR and BC are often confused. In this article we explore the differences and why it's critical you have both.

Page 4

CASE STUDY

City of Minneapolis Succeeding with Managed IT Services

As a trusted partner of the City of Minneapolis, OneNeck hosts and manages their IT infrastructure, ensuring they're always on.

Page 6

FEATURE

DR in the Cloud – Does it make sense for you?

Many organizations are moving to Disaster Recovery-as-a-service (DRaaS). Should you consider it for your organization?

Page 8

FEATURE

DR Options - Which is best for you?

There are lots of options when considering your DR strategy, but which is best for your organization?

Page 10

FEATURE

DR Planning Basics - Where do I start?

Like every business initiative, DR should start with a basic plan and grow from there. But where do you start?

Page 12

Of those IT professionals polled, 64 percent say that data loss is literally a life and death situation for small businesses, and 71 percent say they have to achieve data recovery within 24 hours. That's why 72 percent of businesses are investing in business continuity tools over the next two years, including backup systems.

So if you take the view that a data disaster is not just possible but inevitable, your next step is to determine what types of disaster recovery solutions are best suited to your business needs.

Courting Disaster

There are many causes of data loss, and very few have to do with natural disaster. Most IT professionals (65 percent) feel that technology faults are the leading cause of data disaster, while 60 percent attribute data loss to man-made disasters, and 59 percent attribute security issues. In fact, 65 percent of data disasters are man-made, 29 percent are from technology failures and 22 percent from security breaches.

No matter what the nature of the data loss, there are only limited measures you can take to prevent a disaster. You have to implement safeguards and protocols but with the understanding that things happen, so you need a data recovery strategy as well as data loss prevention protocols.

When planning for disaster recovery, there are two criteria that are most important:

1. having a complete set of business-critical backup data and
2. being able to restore the data quickly.

When it comes to data backup and recovery, most IT professionals consider strategies such as granular file backup and restore, bare metal backup and restore, local failover, hybrid data copies and data encryption, both because they provide complete data sets and can restore data access fast.

One of the primary considerations is whether to store backup data on premise or off premise. Although 91 percent of organizations currently use on-premise backup, an increasing number are looking for off-premise options, including storing data at a location they own (44 percent) or at hosted site (29 percent), with a growing trend toward cloud DR or hybrid data storage.

Cloud Disaster Recovery

More businesses are turning to the cloud for services and data storage. Core business applications such as payroll, email and customer relationship management work well as cloud service solutions, and 80 percent of businesses say they have adopted some form of Software as a Service (SaaS) application.

Disaster Recovery as a Service (DRaaS) is an ideal cloud solution for a number of reasons:

- In the event of a natural disaster, data is archived safely off-premise in the cloud.
- DRaaS has virtually unlimited data storage. Rather than adding more on-site storage, you can add cloud data storage as needed without adding hardware, and storage is elastic and grows with your needs.
- Cloud-based data is accessible any time from any location.
- DRaaS is often more cost-effective, since you buy only the storage you need, without having to invest in more hardware, staff or storage-management tools.
- DRaaS is also highly secure. Data can be encrypted and protected using two-tier authentication and other strategies. It also eliminates the need for physical data security, such as locking the backup disks in a fireproof vault.

Cloud-based data storage also gives you more flexibility so you can adapt your DR plan to suit your business' unique requirements. There are any number of factors that can affect the scope of a disaster recovery solution, such as business hours, e-commerce demands, data criticality and regulatory requirements. Most businesses say they need to have business-critical data restored within four hours. Cloud DR gives you the flexibility to prioritize data access and restore your most critical data assets first.

OneNeck's Managed Services team are experts at disaster recovery and DRaaS. We can work with you to develop a customized DR plan based in your unique requirements. We also can offer various types of services to meet your needs, including DRaaS, colocation with managed services, private cloud services and more. And OneNeck's mission-critical data center facilities are available so you can create your own custom DR site.

So don't leave DR to chance. Disasters will happen, and the right DR partner can make it easier to always be prepared for the worst.

Disaster Recovery vs. Business Continuity: What's the Difference?

When disaster strikes, no one takes the time to worry about words and definitions. Even though the terms Disaster Recovery (DR) and Business Continuity (BC) are often used interchangeably, they have very different meanings. If your company is interchanging them incorrectly, it can leave your organization at significant risk. On the low-end, about $18,000; while on the high-end, we're talking hundreds of millions. According to FEMA, about 40 percent of businesses do not reopen after a disaster.

Whether from a security breach, human error or natural disaster – data loss, downtime or network slowness are costly. Without a plan in place, a comprised network will have lasting implications. A 2015 Verizon DBIR report showed:

- Small data breaches (loss of fewer than 100 records) on average costs businesses $18,120 to $35,730, but can range as high as $555,660.
- Large data breaches (100 million+ records) could cost organizations up to $200 million, though the average is $5-15.6 million.
- In addition to the huge monetary loss, downtime also affects worker productivity and can lead to loss of customers.

Having a plan in place, for DR and BC, is critical. However, both require very different levels of planning. For example:

- DR is Data-Centric: While extremely important in its own right, DR is actually a subset of BC planning. It is concerned with the process of replicating and storing data so that it is quickly recoverable in the event of a disaster. Data must be backed up and stored off-site. It must also be immediately accessible for recovery in the event of a disaster. A major factor is the overall speed of recovery and restoration. In some cases outside of a natural disaster, a local data backup, perhaps at a nearby building or within the corporate campus, will suffice. In situations where a disaster affects an entire city or region (e.g., tornado, flooding), remote backups will be necessary. Because you don't know if a local or regional issue will occur, and depending on your organization's asset criticality, a daily backup may be fine. For others, a fully-mirrored site with hot backup/restore capabilities may make more sense.
- BC is Business-Centric: BC is far larger in scope. Business continuity is focused on the management oversight and planning needed to ensure the entire business can continue to operate with as little disruption as possible – both during and after a disaster. A comprehensive BC plan includes steps for recovering and continuing key business processes, including sales, manufacturing, customer support and billing.

BC is also people-centric. It should ensure employees know where to go and what do in the event of a disaster. Is there an emergency phone

number to call, an alternative office location to go to or a plan for working from home/remotely? Such scenarios must be worked out and communicated in advance – before disaster strikes.

Knowing the Difference & Planning Ahead

The cloud is a useful platform to address both BC and DR, but you must understand the differences for effective planning. Your organization must prioritize your data and systems by importance and determine what is critical to optimize recovery efforts. Another big consideration is to evaluate the cost to your business if an asset is lost or there is significant downtime. To ensure you right-size your efforts, first assess the value of each critical asset and determine a specific plan for each.

A failure to plan ahead can be detrimental to your business. If you don't have a DR and BC plan in place, or if you haven't examined yours for some time, OneNeck IT Solutions is here to help. Our team of experienced professionals is ready to learn about your plans, walk you through the options, and design and deploy a DR and BC plan that ensures your business is adequately protected.

City of Minneapolis

Keeping the City Running with Cloud and Managed IT Services from OneNeck

The Customer

Minneapolis is the largest municipality in Minnesota with more than 400,000 residents, forming half of the Twin Cities with the neighboring state capital, St. Paul. Minneapolis serves as a center of commerce for the region, including support for a large agricultural region with food processing, as well as manufacturing, computing and health services. Running the City's infrastructure requires a complex enterprise network with customized software for each government department and agency.

The Challenge

The City of Minneapolis had been working with their previous IT outsourcing partner for 13 years and desired to find a new managed services and outsourced IT partner to manage the City's IT infrastructure. In addition, the existing network infrastructure was aging, and the City needed an experienced IT services partner to provide cloud and managed services that encompassed server, storage, network, security, database, OS and data protection services. After issuing a comprehensive RFP for outsourced IT services, the City of Minneapolis selected OneNeck out of a field of 18 prospective partners to handle this comprehensive list of services.

The OneNeck® IT Solutions Answer

Because of OneNeck's comprehensive hybrid IT service offerings, OneNeck had all of the resources needed to manage the City of Minneapolis' computing infrastructure. As part of the contract, OneNeck would provide colocation services leveraging OneNeck's national footprint of highly-secure data centers it owns and operates. One data center was to host the City's production application environment, while disaster recovery for mission-critical and business-critical applications would be supported from another OneNeck data center.

OneNeck also was able to bring all the expertise required to maintain enterprise operations, including managed services for networking equipment such as routers, switches and firewalls across 70 locations. Data hosting using OneNeck's' ReliaCloud® infrastructure-as-a-service (IaaS) platform was able to support more than 250 servers with 180 terabytes of data, including dedicated servers for non-virtualized assets.

The OneNeck team also brought the expertise to transition and upgrade critical components the City's PeopleSoft environment to support human resources and finance. Migration included transitioning and supporting hundreds of applications for specific city services, such as waste management, land management, parks and recreation and more.

WATCH

Video

OneNeck's ReliaCloud - Infrastructure as a Service (IaaS)

A cloud solution should enable your IT organization to provide services quickly and cost effectively and be flexible enough to respond to change. Meet ReliaCloud.

Watch Now

Like any IT transformation, there were bumps along the way that the City and OneNeck worked through together. Since the existing contract was still in place when the new contract was signed, the OneNeck team was unable to gain access to the computing environment prior to the hand-off. There was no way to perform an initial assessment. However, when the contract did expire, OneNeck was able to work with the installed systems and initiate the migration without any real problems.

Part of the reason for the success was the ongoing communications between the OneNeck team and the City's IT team. From the first day the contract was signed, the City demonstrated their eagerness to forge a partnership and committed their time and resources to the project. To ensure success, the OneNeck project team and the City's IT group met twice each day to plan and assess progress.

As the OneNeck team moved through each phase of the project, they encountered a few surprises. For example, they discovered that most of the installed enterprise systems were at the end of their lifespan. There was no alternative but to take the outdated systems and make sure they continued to work; letting the system go down was not an option.

The biggest surprise came with the implementation of the Criminal Justice Information System (CJIS). Before work could begin on the CJIS project, the entire OneNeck Operational Support team, more than 100 professionals, had to be screened for security clearance, including fingerprinting and background checks. However, OneNeck worked closely with the City to satisfy all of the City's security and compliance requirements, even though it impacted progress on the overall transition project with the City.

The Benefits

Despite these challenges, the OneNeck team was able to complete Phase 1 of the project on time and within budget. Some of the IT environments were even ahead of schedule.

OneNeck was able to scale the capacity of the ReliaCloud environment quickly to accommodate 70 separate locations and 3,500 users with more than 250 servers and 180 terabytes. Much of the first six months of the project included migrating data and workloads from the existing service provider's data center to ReliaCloud.

As the relationship evolves, the City of Minneapolis will continue to look to OneNeck as a strategic service provider. OneNeck continues to supplement the City's team with diverse expertise, across many technologies, bringing solutions and resources as needed, even outside the originally contracted services.

The City is already seeing on-going benefits as they are more flexible and more responsive to stakeholders needs. City administrators expect to save more than $3 million annually with OneNeck, and as new upgrades and applications are needed as part of organic growth, the City will continue to benefit from OneNeck's versatility and ability to plan and manage a dynamic IT infrastructure.

Disaster Recovery in the Cloud – Does it make sense for you?

The traditional DR method includes purchasing and locating dedicated servers in a remote location and replicating all your mission-critical applications and data to those servers - and then crossing your fingers that you can bring it all back up as planned. Today, as the cloud continues to become more reliable and secure, many organizations are moving to Disaster Recovery-as-a-service (DRaaS).

DRaaS is designed to cater to businesses of every size and need. Organizations can subscribe to full-scale DRaaS, where the service provider manages everything from the replication of a customer's production virtual machines (VMs), and in some cases physical machines, to full-service recovery once a disaster is declared. Others look for an infrastructure-as-a-service (IaaS) model offering in which they handle their own VM replication to the cloud and manage their own recovery, and some organizations simply want backup-as-a-service (BaaS), where the provider manages customer backups from the production site to the cloud.

Whatever flavor they choose, organizations that go the DRaaS route quickly find out that the cloud provides everything most businesses look for in a disaster recovery plan, including:

- Easy, frequent data replication between sites: Since it's

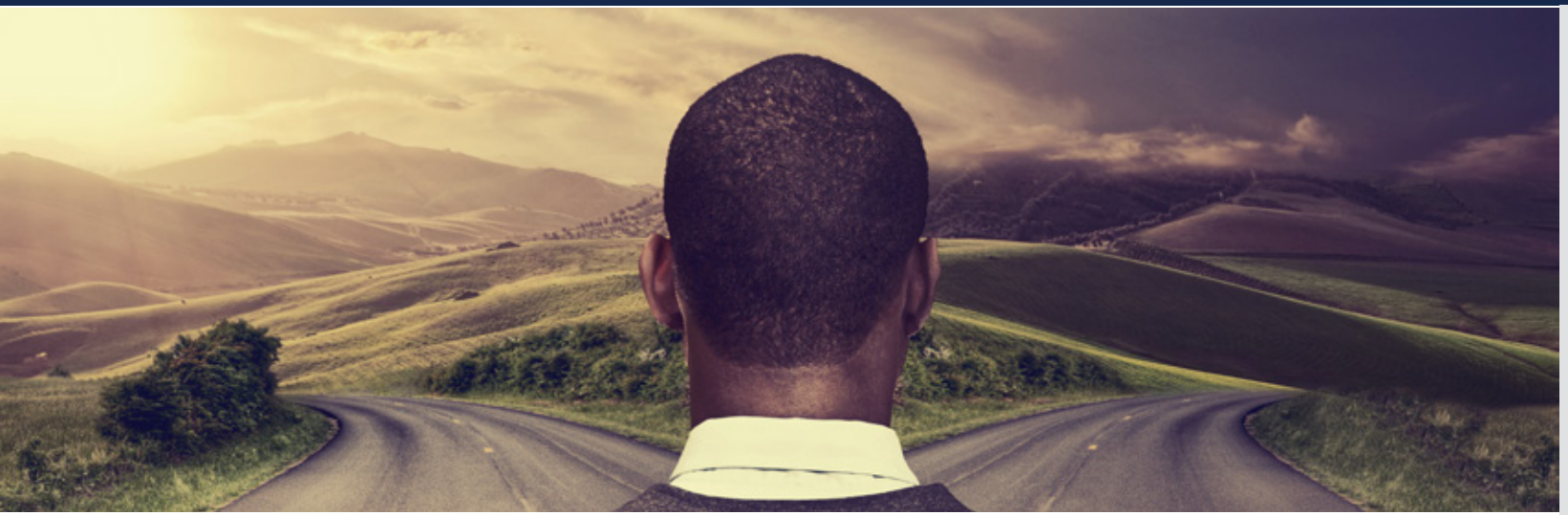
designed to quickly and efficiently move on-premise workloads offsite to well-managed cloud data centers, cloud infrastructure ensures data integrity.

- No wasted infrastructure: Rather than trying to predict and plan for capacity demands that lead to expensive servers, network gear and software sitting idle at a remote DR site, the cloud enables organizations to efficiently backup data without the added overhead.
- Reduced recovery time: Since DRaaS server and storage resources can be accessed on-demand, business applications and services can be brought online far faster than with traditional alternatives.
- Reduced costs: Whether you have your DR hosted in the cloud or have a dedicated server in a collocated facility you have economies of scale that reduce the cost of Disaster Recovery. The overhead and administrative hardware resources are pooled in the cloud so the costs to deliver DRaaS is often a fraction of that associated with traditional DR environments.

Gartner expects that more organizations will be using DRaaS than traditional, syndicated recovery services by 2018, and cloud vendors are fast addressing the opportunity. The best options offer:

- Tailored solutions to fit your needs and budget
- Strong uptime and SLA guarantees, ensuring your data is there when you need it.
- Support for both physical and virtual machines, ensuring every critical service and application can be recovered quickly and effectively.
- State-of-the-art data centers, supporting best practices in redundant power and cooling, physical and cybersecurity, dedicated 24x7 staffing and more.
- Flexibility and scalability, spinning up new compute resources as business needs (and disasters) dictate.

Every business is unique and has its own DR needs. OneNeck takes the time upfront, before implementation, to determine what's critical to your business and your customers to make sure your business can continue operations no matter what. Then, we tailor our solutions to your particular situation.



DR Options - Which is best for you?

Natural disasters, equipment failures and error-induced process interruptions have historically been the primary threats to infrastructure stability. Now, these threats are overshadowed by those originating from malicious intent and overloads on the global infrastructure. These threats to infrastructure stability, together with competitive pressures and market demands, have emphasized the need for effective and thorough risk-based continuity planning, because in most cases, when the information flow stops, so does business.

As such, disaster recovery (DR) planning continues to be a priority initiative for businesses of all types. However, there are a variety of DR options for failing over workloads to an alternate location. It is imperative for IT professionals to understand their options and choose the one that is the best fit for their own organization.

Build Your Own

Building your own DR site is an option for many organizations. By building your own site, you maintain complete control of your infrastructure and data. In addition, you will be able to create a site specific to your exact DR needs.

However, building your own data center is resource-intensive and requires experience. And that's not all—once your data center is built, you also have to manage the upkeep, updating, administration and management of the data center, all of which can be incredibly complicated throughout the life of your data center. An important question to ask yourself is whether you want to be in the business of running a data center. Can you operate a data center facility as well as, or better than, a third-party provider?

Cloud for Disaster Recovery

Today, as the cloud continues to become more reliable and secure, many organizations are moving to Disaster Recovery-as-a-Service (DRaaS). DRaaS is designed to cater to businesses of every size and need. Organizations can subscribe to full-scale DRaaS, where the service provider manages everything from the replication of a customer's production virtual machines (VMs), and in some cases physical machines, to full-service recovery once a disaster is declared. Others look for an Infrastructure-as-a-Service (IaaS) model offering in which they handle their own VM replication to the cloud and manage their own recovery. And some organizations simply want Backup-as-a-Service (BaaS), where the provider manages customer backups from the production site to the cloud.

As with any service, there are cons. Here are the most significant cons of backing up your data in the cloud:

- You can't access your data if you don't have Internet access.
- Bandwidth issues – You need the right amount of bandwidth to back up large chunks of data.
- Large data recovery jobs will use more resources, which could ultimately increase your cost for DRaaS.

Colocation for Disaster Recovery

Colocation is an attractive alternative for organizations who do not want build and maintain their own facility or just aren't ready to place their data in the hands of a cloud provider.

Colocating your disaster recovery IT infrastructure gives you peace of mind in the event of a natural disaster, power outage or other unexpected event that impacts your primary place of business. Colocation can ensure that your offsite infrastructure and applications will remain available and operational if the unexpected happens.

In addition, with colocation, organizations can reduce overhead and increase operating efficiencies by moving their network, servers, data storage and other equipment to a remote location. You'll be paying only for space and, at the same time, maintaining complete control of your equipment. Your valuable IT operations will be protected remotely in a secure data center.

Every business is unique and has its own needs when it comes to DR. It's important to determine what's critical to your business and your customers to make sure you deliver on your commitments no matter what, then select the solution that best suits your particular situation.

OneNeck operates nine state-of-the-art data centers located throughout the US, all of which offer superior security, redundant connectivity and climate-controlled environments ideal for your colocation and DR needs. Our data centers are designed to give you options, help you lower your operating expenses, reduce capital expenditures, deploy solutions faster and scale your requirements as needed.

DR Planning Basis - Where do I start?

DR planning is often considered a component or subset of business continuity planning (BCP). DR generally refers to the processes and a procedures used to recover after a disruptive event and is focused around the critical IT systems in organization. Business continuity planning usually includes the functions that need to continue after a disruption so that your business continues to make money.

At a high level, disaster recovery planning usually involves the following steps:

1. Identify the Scope and Boundaries – This is typically the first step towards completing your DR plan. Identifying the scope involves prioritizing the critical systems for DR and assigning a value to the failures of those systems.
2. Establish the Budget – Budgeting for DR plans can be tricky. Often you will want to do an assessment of the costs to the business via different disaster scenarios. Comparing different options for recovery can vary the costs of the DR plan. Reducing RPO and RTO requirements can soften the financial costs of the DR plan, but be realistic and ensure executive management understands the risks of data loss and system availability being stretched out. Both IT and executive management must agree on the budget, and IT will work within the constraints of the budget that has been established.
3. Develop and Deploy the Plan – Developing and deploying the plan can be the most involved part of this process. Often the plan is actually a 'script' of activities that occur in order and are executed by a recovery team made up of resources from IT. Roles and responsibilities are assigned in the plan as well. Deploying the plan involves choosing the tools and technologies needed to meet the RTO and RPO requirements established in the first step while still working within the constraints of the budget.
4. Test, test, test, test – DR plans are simply not effective if they are not frequently tested. Test the systems you're going to use in recovery regularly to validate that all the pieces work. Always record your test results and update the DR plan to address any shortcomings. As your business environment changes, so should your DR plan.

DOWNLOAD

Booklet

DR Guide - DR in Virtualized Environments

by Zerto

Thorough security and business continuity strategies are crucial for modern businesses, minimizing data loss and downtime. In this booklet, OneNeck partner Zerto provides insights in the challenges, needs, strategies, and available solutions for DR and BC, especially in modern, virtualized environments and the public cloud.

Download Now

(855) ONE-NECK

www.OneNeck.com

OneNeck®
IT SOLUTIONS
a TDS® Company