*Managing the information that drives the enterprise*

# STORAGE*

SEARCHSTORAGE.CO.UK

*essential guide

# DISASTER RECOVERY

**With the technologies that are available to help speed, simplify and lower the cost of disaster recovery protection, your excuses for not having a plan are falling away.**

## inside



TechTarget

editorial * antony adshead

# Technology options are removing obstacles to disaster recovery protection

**Server virtualisation and the cloud are making the task of disaster recovery protection considerably easier than in the not-too-distant past and removing excuses for not doing it.**



**DISASTER RECOVERY HAS** assumed a heightened profile over the past few years. So much so that looking back to only five years ago seems like the Dark Ages from here. It was common to come across many businesses without disaster recovery plans or provision. I'm sure it still is, but with the mushrooming of disaster recovery technology in the past few years, there's no excuse nowadays.

On the one hand, there have been strong push factors impelling organisations towards effective disaster recovery planning.

This can take the form of legal and regulatory compliance. Financial services players, for example, have prescribed levels

of disaster recovery in place. Regulations such as Basel II, MiFID and those of the UK Financial Services Authority dictate the standard of disaster recovery expected, the minimum distance of secondary sites, etc.

Good business sense is also a driver. Again, in the financial services sector, for example, the need for rapid failover to a secondary site is not only driven by regulation but also by the bottom line. In algorithmic trading, milliseconds are worth millions every year, and the financial services company that doesn't resume trading again within seconds of an outage will lose money hand over fist.

**The good news is that there are some very attractive pull factors that make disaster recovery potentially easier, less costly and less of a management headache than it has ever been.**

Damage to reputation and future ability to trade are the bottom lines that disaster recovery must protect against. There are chilling statistics about the number of businesses that never recover from an IT disaster, and those that do—but too slowly—are likely to suffer a hemorrhage of customers and a slower but inexorable death.

But enough of the doom and gloom. While there are compelling push factors driving the need for a sound disaster recovery strategy, the good news is that there are some very attractive pull factors that make disaster recovery potentially easier, less costly and less of a management headache than it has ever been.

First of these is server virtualisation. Once upon a time, an effective disaster recovery strategy meant that your secondary IT setup needed to be a carbon copy of your primary data

centre. This was because applications—OS, updates, patches and all—were tied to one physical server.

Server virtualisation broke this link. The hypervisor now sits between applications and the physical device, and where once apps and data could be restored only to identical servers, now bare-metal restore on any device is possible. In fact, mirroring in real time or near real time can enable failover to the secondary server estate in minutes or seconds.

Now, it's true that in even the organisations that are most advanced in IT terms, not all servers are virtualised. But the fact that many—probably a majority in most IT departments—are, will make disaster recovery an easier task, with only a few servers needing to remain entirely physical. For many SMBs, however, chances are their entire server estate can be virtualised and disaster recovery made entirely independent of specific physical devices.

The cloud takes that theme to further logical conclusions. The provision of compute and storage facilities remotely by a service provider has been the buzz phrase in IT for the past couple of years. It's potentially a game changer in many areas, not least of which is disaster recovery.

Cloud disaster recovery offers remote resources to which your replicate data; then, should an outage occur, your company's employees can work from the cloud while your physical IT facilities are restored. It's early days, but at some point—security and bandwidth permitting—this could be the standard by which all work.

Having said all that, there is one area of disaster recovery that hasn't necessarily gotten any easier. And that is the need to analyse risk, develop detailed plans, and test and train and continuously update them. In this Essential Guide, you will find pointers towards achieving these tasks. ⊙

**Antony Adshead** is bureau chief of SearchStorage.co.UK.

# How to write a disaster recovery plan and define disaster recovery strategies

## Learn how to develop disaster recovery strategies as well as how to write a disaster recovery plan with these step-by-step instructions.

BY PAUL KIRVAN



**FORMULATING A DETAILED** recovery plan is the main aim of the entire IT disaster recovery planning project. It is in these plans that you will set out the detailed steps needed to recover your IT systems to a state in which they can support the business after a disaster.

But before you can generate that detailed recovery plan, you'll need to perform a risk assessment (RA) and/or business impact analysis (BIA) to identify the IT services that support the organisation's critical business activities. Then, you'll need to establish recovery time objectives (RTOs) and recovery point objectives (RPOs).

Once this work is out of the way, you're ready to move on to developing disaster recovery strategies, followed by the actual plans. Here we'll explain how to write a disaster recovery plan as well as how to develop disaster recovery strategies.

## DEVELOPING DR STRATEGIES

Regarding disaster recovery strategies, ISO/IEC 27031, the global standard for IT disaster recovery, states, "Strategies should define the approaches to implement the required resilience so that the principles of incident prevention, detection, response, recovery and restoration are put in place." Strategies define what you plan to do when responding to an incident, while plans describe how you will do it.

Once you have identified your critical systems, RTOs, RPOs, etc, create a table, as shown below, to help you formulate the disaster recovery strategies you will use to protect them.

You'll want to consider issues such as budgets, management's position with regard to risks, the availability of re-

browse

The state of disaster recovery

Writing the DR plan

Virtual DR

Cloud DR

WAN optmisation

SMB best practices

Table 1: **Determining DR strategies**

| Critical system | RTO/RPO (in hours) | Threat | Prevention strategy | Response strategy | Recovery strategy |
|---|---|---|---|---|---|
| Accounts payable | 4/2 | Server failure | Secure equipment room and backup server; install UPS | Switch over to backup server; validate that UPS is running | Fix/replace primary server; fail back to primary server |
| Manufacturing | 8/4 | Loss of manufacturing systems | Set up failure alerts and conduct regular inspections; install UPS | Run manufacturing on alternate system | Fix primary manufacturing system; return to normal operations |
| Building security | 2/2 | Security system destroyed | Locate system in secure area; install protective enclosures around sensor units; install UPS | Deploy guards at strategic points | Obtain/install replacement unit(s), sensor(s) |

sources, costs versus benefits, human constraints, technological constraints and regulatory obligations.

Let's examine some additional factors in strategy definition.

**People.** This involves availability of staff/contractors, training needs of staff/contractors, duplication of critical skills so there can be a primary and at least one backup person, available documentation to be used by staff, and follow-up to ensure staff and contractor retention of knowledge.

**Physical facilities.** Areas to look at are availability of alternate work areas within the same site, at a different company location, at a third-party-provided location, at employees' homes or at a transportable work facility. Then consider site security, staff access procedures, ID badges and the location of the alternate space relative to the primary site.

**Technology.** You'll need to consider access to equipment space that is properly configured for IT systems, with raised floors, for example; suitable heating, ventilation and air conditioning (HVAC) for IT systems; sufficient primary electrical power; suitable voice and data infrastructure; the distance of the alternate technology area from the primary site; provision for staffing at an alternate technology site; availability of failover (to a backup system) and failback (return to normal operations) technologies to facilitate recovery; support for legacy systems; and physical and information security capabilities at the alternate site.

**Data.** Areas to look at include timely backup of critical data to a secure storage area in accordance with RTO/RPO requirements, method(s) of data storage (disk, tape, optical, etc), connectivity and bandwidth requirements to ensure all critical data can be backed up in accordance with RTO/RPO time scales, data protection capabilities at the alternate storage site, and availability of technical support from qualified third-party service providers.

browse

The state of disaster recovery

Writing the DR plan

Virtual DR

Cloud DR

WAN optmisation

SMB best practices

**Suppliers.** You'll need to identify and contract with primary and alternate suppliers for all critical systems and processes, and even the sourcing of people. Key areas where alternate suppliers will be important include hardware (such as servers, racks, etc), power (such as batteries, universal power supplies, power protection, etc), networks (voice and data network services), repair and replacement of components, and multiple delivery firms (FedEx, UPS, etc).

**Policies and procedures.** Define policies for IT disaster recovery and have them approved by senior management. Then define step-by-step procedures to, for example, initiate data backup to secure alternate locations, relocate operations to an alternate space, recover systems and data at the alternate sites, and resume operations at either the original site or at a new location.

Finally, be sure to obtain management sign-off for your strategies. Be prepared to demonstrate that your strategies align with the organisation's business goals and business continuity strategies.



## TRANSLATING DISASTER RECOVERY STRATEGIES INTO DR PLANS

Once your disaster recovery strategies have been developed, you're ready to translate them into disaster recovery plans. Let's take Table 1 and recast it into Table 2, on p. 9. Here we can see the critical system and associated threat, the response strategy and (new) response action steps, as well as the recovery strategy and (new) recovery action steps. This approach can help you quickly drill down and define high-level action steps.

From Table 2 you can expand the high-level steps into more detailed step-by-step procedures, as you deem necessary. Be sure they are linked in the proper sequence.

## Table 2: **Using strategies to create plan**

| Critical system | Threat | Response strategy | Response action steps | Recovery strategy | Recovery action steps |
|---|---|---|---|---|---|
| Accounts payable | Server failure | Switch over to backup server; validate that UPS is running | Verify server is down; verify data has been backed up and is safe; test backup server; start switchover to alternate server | Fix/replace primary server; fail back to primary server | Verify cause of server outage; obtain, test and install new server; fail systems back to new server |
| Manufacturing | Loss of manufacturing systems | Run manufacturing on alternate system | Verify manufacturing system is down; verify data has been backed up and is safe; test alternate system; start switchover to alternate manufacturing system | Fix primary manufacturing system; return to normal operations | Verify cause of manufacturing system outage; contact repair resources; fix and test manufacturing system; fail manufacturing system back to repaired system |
| Building security | Security system destroyed | Deploy guards at strategic points | Verify security system is down; verify security data has been backed up and is safe; contact guard agencies to source on-site guards; define guard duties; brief guards on duties; provide communications devices for guards | Obtain/ install replacement unit(s), sensor(s) | Verify cause of security system outage; contact supplier to get replacement; test replacement system; restart security system |

browse

The state of disaster recovery

Writing the DR plan

Virtual DR

Cloud DR

WAN optmisation

SMB best practices

## DEVELOPING DR PLANS

DR plans provide a step-by-step process for responding to a disruptive event. Procedures should ensure an easy-to-use and repeatable process for recovering damaged IT assets and returning them to normal operation as quickly as possible. If staff relocation to a third-party hot site or other alternate space is necessary, procedures must be developed for those activities.

When developing your IT DR plans, be sure to review the global standards ISO/IEC 24762 for disaster recovery and ISO/IEC 27035 (formerly ISO 18044) for incident response activities.

## INCIDENT RESPONSE

In addition to using the strategies previously developed, IT disaster recovery plans should form part of an incident response process that addresses the initial stages of the incident and the steps to be taken. This process can be seen as a timeline, such as in "Disaster timeline" (below), in which incident response actions precede disaster recovery actions.

## THE DR PLAN STRUCTURE

The following section details the elements in a DR plan in the sequence defined by ISO 27031 and ISO 24762.


*Note: We have included emergency management, as it represents activities that may be needed to address situations where humans are injured or situations such as fires that must be addressed by local fire brigades and other first responders.*

*Important: Best-in-class DR plans should begin with a few pages that summarise key action steps (such as where to assemble employees if forced to evacuate the building) and lists of key contacts and their contact information for ease of authorising and launching the plan.*

1. **Introduction.** Following the initial emergency pages, DR plans have an introduction that includes the purpose and scope of the plan. This section should specify who has approved the plan, who is authorised to activate it and a list of linkages to other relevant plans and documents.

2. **Roles and responsibilities.** The next section should define roles and responsibilities of DR recovery team members, their contact details, spending limits (for example, if equipment has to be purchased) and the limits of their authority in a disaster situation.

3. **Incident response.** During the incident response process, we typically become aware of an out-of-normal situation (such as being alerted by various system-level alarms), quickly assess the situation (and any damage) to make an early determination of its severity, attempt to contain the incident and bring it under control, and notify management and other key stakeholders.

4. **Plan activation.** Based on the findings from incident response activities, the next step is to determine if disaster recovery plans should be launched, and which ones in particular should be invoked. If DR plans are to be invoked, incident response activities can be scaled back or terminated, depending on the incident, allowing for launch of the DR plans. This section defines the criteria for launching the plan, what data is needed and who makes the determination. Included within this part of the plan should be assembly areas for staff (primary and alternates), procedures for notifying and activating DR team members, and procedures for standing

down the plan if management determines the DR plan response is not needed.

5. **Document history.** A section on plan document dates and revisions is essential and should include dates of revisions, what was revised and who approved the revisions. This can be located at the front of the plan document.

6. **Procedures.** Once the plan has been launched, DR teams take the materials assigned to them and proceed with response and recovery activities as specified in the plans. The more detailed the plan is, the more likely the affected IT asset will be recovered and returned to normal operation. Technology DR plans can be enhanced with relevant recovery information and procedures obtained from system vendors. Check with your vendors while developing your DR plans to see what they have in terms of emergency recovery documentation.

7. **Appendixes.** Located at the end of the plan, these can include systems inventories, application inventories, network asset inventories, contracts and service-level agreements, supplier contact data, and any additional documentation that will facilitate recovery.



## FURTHER ACTIVITIES

Once your DR plans have been completed, they are ready to be exercised. This process will determine whether they will recover and restore IT assets as planned.

In parallel to these activities are three additional ones: creating employee awareness, training and records management. These are essential in that they ensure employees are fully aware of DR plans and their responsibilities in a disaster, and DR team members have been trained in their roles and responsibilities as defined in the plans. And since DR planning generates a significant amount of documentation, records

management (and change management) activities should also be initiated. If your organisation already has records management and change management programmes, use them in your DR planning. ⊙

**Paul Kirvan**, CISA, FBCVI, CBCP, has more than 20 years of experience in business continuity management as a consultant, author and educator.

browse

The state of disaster recovery

Writing the DR plan

Virtual DR

Cloud DR

WAN optmisation

SMB best practices

# Virtual disaster recovery

## Storage and server virtualisation make many of the most onerous disaster recovery tasks relatively easy to execute, while helping to cut overall DR costs.

BY LAUREN WHITEHOUSE

**IF YOUR COMPANY** still lacks a viable disaster recovery (DR) strategy, it might be time to start thinking virtualisation. The initial drivers behind server virtualisation adoption have been improving resource utilisation and lowering costs through consolidation, but next-wave adopters have realised that virtualisation can also improve availability.

Virtualisation turns physical devices into sets of resource pools that are independent of the physical assets they run on. With server virtualisation, decoupling operating systems, applications and data from specific physical assets eliminates the economic and operational issues of infrastructure silos—one of the key ingredients to affordable disaster recovery.

Storage virtualisation takes those very same benefits and extends them from servers to the underlying storage domain, bringing IT organisations one step closer to the ideal of a virtualised IT infrastructure. By harnessing the power of virtualisation, at both the server and storage level, IT organisations can become more agile in disaster recovery.

## REDUCE THE RISK

Improving disaster recovery and business continuity are perennial top-10 IT priorities because companies want to reduce the risk of losing access to systems and data. While most shops have daily data protection plans in place, fewer of them focus their efforts on true disasters, which would include any event that interrupts service at the primary production location. An event can be one of many different things, including power failures, fires, floods, other weather-related outages, natural disasters, pandemics or terrorism. Regardless of the cause, unplanned downtime in the data centre can wreak havoc on IT's ability to maintain business operations.

The goal of a DR process is to re-create all necessary systems at a second location as quickly and reliably as possible. Unfortunately, for many firms, DR strategies are often cobbled together because there's nothing or no one mandating them, they're too costly or complex, or there's a false belief that existing backup processes are adequate for disaster recovery.

Backup technologies and processes will take you only so far when it comes to a disaster. Tier 1 data (the most critical stuff) makes up approximately 50% of an organisation's total primary data. When the Enterprise Strategy Group (ESG) surveyed IT professionals responsible for data protection, 53% said their organisation could tolerate one hour or less of downtime before their business suffered revenue loss or some other type of adverse business impact; nearly three-quarters (74%) fell into the less-than-three-hour range. (The results of this survey were published in the ESG research report, *2010 Data Protection Trends*, April 2010.) When relying on backup for DR, under the best conditions, the time it takes to acquire replacement hardware, reinstall operating systems and applications, and recover data—even from a disk-based

copy—will likely exceed a recovery time objective (RTO) of one to three hours.

Recovery from a mirror copy of a system is faster than recovering with traditional backup methods, but it's also more expensive and complex. Maintaining identical systems in two locations and synchronising configuration settings and data copies can be a challenge. This often forces companies to prioritise or "triage" their data, providing greater protection to some tiers than others. ESG research found that Tier 2 data comprises 28% of all primary data, and nearly half (47%) of IT organisations we surveyed noted three hours or less of downtime tolerance for Tier 2 data. Therefore, if costs force a company to apply a different strategy or a no-protection strategy for "critical" (Tier 1) vs. "important" (Tier 2), some risks may be introduced.

browse

The state of disaster recovery

Writing the DR plan

Virtual DR

Cloud DR

WAN optmisation

SMB best practices

## BENEFITS OF SERVER VIRTUALISATION FOR DR

Virtualisation has become a major catalyst for change in x86 environments because it provides new opportunities for more cost-effective DR. When looking at the reasons behind server virtualisation initiatives on the horizon, ESG research found that making use of virtual machine replication to facilitate disaster recovery ranked second behind consolidating more physical servers onto virtualisation platforms. (See the ESG research report, *2011 IT Spending Intentions*, published in January 2011, for details of the survey results.)

Because server virtualisation abstracts from the physical hardware layer, it eliminates the need for identical hardware configurations at production and recovery data centres, which provides several benefits. And since virtualisation is often a catalyst to refresh the underlying infrastructure, there's usually retired hardware on hand. For some organisations that might not have been able to secure the CapEx to

outfit a DR configuration, there may be an opportunity to take advantage of hand-me-down hardware. Also, by consolidating multiple applications on a single physical server at the recovery data centre, the amount of physical recovery infrastructure required is reduced. This, in turn, minimises expensive raised floor space costs, as well as additional power and cooling requirements.

Leveraging the encapsulation and portability features of virtual servers aids in DR enablement. Encapsulating the virtual machine into a single file enables mobility and allows multiple copies of the virtual machine to be created and more easily transferred within and between sites for business resilience and DR purposes—a dramatic improvement over backing up data to portable media such as tape and rotating media at a cold standby site. In addition, protecting virtual machine images and capturing the system state of the virtual machine are new concepts that weren't available in the physical world. In a recovery situation, there's no need to reassemble the operating system, reset configuration settings and restore data. Activating a virtual machine image is a lot faster than starting from a bare-metal recovery.

**Leveraging the encapsulation and portability features of virtual servers aids in DR enablement.**

Flexibility is another difference. Virtualisation eliminates the aforementioned need for a one-to-one physical mirror of a system for disaster recovery. IT has the choice of establishing physical-to-virtual (P2V) and virtual-to-virtual (V2V) failover configurations—locally and/or remotely—to enable rapid recovery without incurring the additional expense of purchasing and maintaining identical hardware. Virtualisation also offers

flexibility in configuring active-active scenarios (for example, a remote or branch office acts as the recovery site for the production site and vice versa) or active-passive (for example, a corporate-owned or third-party hosting site acts as the recovery site, remaining dormant until needed).

Finally, virtualisation delivers flexibility in the form of DR testing. To fully test a disaster recovery plan requires disabling the primary data centre and attempting to fail over to the secondary. A virtualised infrastructure makes it significantly easier to conduct frequent non-disruptive tests to ensure the DR process is correct and the organisation's staff is practiced in executing it consistently and correctly, including during peak hours of operation.

**With server virtualisation, a greater degree of DR agility can be achieved.**

With server virtualisation, a greater degree of DR agility can be achieved. IT's ability to respond to service interruptions can be greatly improved, especially with new automation techniques, such as those available for VMware virtualisation technology and Microsoft System Center Virtual Machine Manager, which offers tools to determine which applications and services to restore in which order. Recovery can be quicker and the skills required by operations staff to recover virtualised applications are less stringent.



## USING STORAGE VIRTUALISATION IN A DR PLAN

As organisations become more comfortable with one form of virtualisation, they don't have to make great intellectual or operational leaps to grasp the concept of virtualising other data centre domains. Often, IT organisations undertaking

complete data centre refresh initiatives position virtualisation as a key part of the makeover and look to extract all possible efficiencies in one fell swoop by deploying virtualisation in multiple technology areas. So it's not uncommon to see server virtualisation combined with storage virtualisation.

Like server virtualisation, storage virtualisation untethers data from dedicated devices. Storage virtualisation takes multiple storage systems and treats those devices as a single, centrally managed pool of storage, enabling management from one console. It also enables data movement among different storage systems transparently, providing capacity and load balancing. In addition to lowering costs, improving resource utilisation, increasing availability, simplifying upgrades and enabling scalability, the expected benefit of storage virtualisation is easier and more cost-effective DR.

**In a DR scenario, storage virtualisation improves resource utilisation, allowing organisations to do more with less capacity on hand.**

In a DR scenario, storage virtualisation improves resource utilisation, allowing organisations to do more with less capacity on hand. IT is likely to purchase and deploy far less physical storage with thin, just-in-time provisioning of multiple tiers of storage. By improving capacity utilisation, organisations can reduce the amount of additional capacity purchases and more easily scale environments.

Virtualisation allows storage configurations to vary between the primary and the DR site. Flexibility in configuring dissimilar systems at the production and recovery sites can introduce cost savings (by allowing existing storage systems

to be reclaimed and reused), without introducing complexity. It also allows IT to mirror primary storage to more affordable solutions at a remote site, if desired.

Native data replication that integrates with the virtualised storage environment can provide improved functionality for virtual disaster recovery. Remote mirroring between heterogeneous storage systems (that is, more expensive at the primary site and less costly at the recovery site) contributes to lower costs.

## FINAL WORD ON VIRTUALISATION

Whether used singly or combined, server virtualisation and storage virtualisation are making an impact on IT's ability to deliver DR and to deliver it cost effectively. If your company has been on the sidelines, crossing its collective fingers and hoping a disaster never strikes, it might be time to investigate virtualisation. And if you have virtualisation in place, you should have the basic elements for an effective and cost-efficient DR environment. It's time to take the next steps. ⊙

**Lauren Whitehouse** is a senior analyst focusing on backup and recovery software and replication solutions at Enterprise Strategy Group.

# Blueprint for cloud-based disaster recovery

## Cloud storage and computing services offer a number of alternatives for cloud-based DR depending on the recovery time and recovery point objectives a company requires.

BY JACOB GSOEDL



**CLOUD COMPUTING**, along with mobile and tablet devices, accounts for much of the high-tech buzz these days. But when it comes to hype, the cloud seems to absorb more than its fair share, which has had the unintended consequence of sometimes overshadowing its real utility.

Although the concept—and some of the products and services—of cloud-based disaster recovery (DR) is still nascent, some companies, especially smaller organisations, are discovering and starting to leverage cloud services for DR.

It can be an attractive alternative for companies that may be strapped for IT resources because the usage-based cost of cloud services is well suited for DR where the secondary infrastructure is parked and idling most of the time.

Having DR sites in the cloud reduces the need for data centre space, IT infrastructure and IT resources, which leads to significant cost reductions, enabling smaller companies to deploy disaster recovery options that were previously only found in larger enterprises. “Cloud-based DR moves the discussion from data centre space and

hardware to one about cloud capacity planning," said Lauren Whitehouse, senior analyst at Enterprise Strategy Group (ESG).

But cloud-based disaster recovery isn't a perfect solution, and its shortcomings and challenges need to be clearly understood before a firm ventures into it. Security usually tops the list of concerns. Questions to consider:

- Is data securely transferred and stored in the cloud?
- How are users authenticated?
- Are passwords the only option or does the cloud provider offer some type of two-factor authentication?
- Does the cloud provider meet regulatory requirements?

And because clouds are accessed via the Internet, bandwidth requirements also need to be clearly understood. There's a risk of only planning for bandwidth requirements to move data into the cloud without sufficient analysis of how to make the data accessible when a disaster strikes. Questions to consider:

- Do you have the bandwidth and network capacity to redirect all users to the cloud?
- If you plan to restore from the cloud to on-premises infrastructure, how long will that restore take?

"If you use cloud-based backups as part of your DR, you need to design your backup sets for recovery," said Chander Kant, CEO and founder at Zmanda, an open-source backup app vendor.

Reliability of the cloud provider, its availability and its ability to serve your users while a disaster is in progress are other key considerations. The choice of a cloud service provider or managed service provider (MSP) that can deliver service within the agreed terms is essential, and while making a wrong choice may not land you in IT hell, it can easily put you in the doghouse or even get you fired.

## DEVISING A DISASTER RECOVERY BLUEPRINT

Just as with traditional DR, there isn't a single blueprint for cloud-based disaster recovery. Every company is unique in the applications it runs and the relevance of the applications to its business and the industry it's in. Therefore, a cloud disaster recovery plan (aka cloud DR blueprint) is very specific and distinctive for each organisation.

Triage is the overarching principle used to derive traditional as well as cloud-based DR plans. The process of devising a DR plan starts with identifying and prioritising applications, services and data, and determining for each one the amount of downtime that's acceptable before there's a significant business impact. Priority and required recovery time objectives (RTOs) will then determine the disaster recovery approach.

**Triage is the overarching principle used to derive traditional as well as cloud-based DR plans.**

Identifying critical resources and recovery methods is the most relevant aspect during this process, since you need to ensure that all critical apps and data are included in your blueprint. By the same token, to control costs and to ensure speedy and focused recovery when the plan needs to be executed, you want to make sure to leave out irrelevant applications and data. The more focused a DR plan is, the more likely you'll be able to test it periodically and execute it within the defined objectives.

With applications identified and prioritised and RTOs defined, you can then determine the best and most cost-effective methods of achieving the RTOs, which needs to be done by application and service. In the rarest of cases, you'll have a single DR method for all your applications and data; more

likely you'll end up with several methods that protect clusters of applications and data with similar RTOs. "A combination of cost and recovery objectives drive different levels of disaster recovery," said Seth Goodling, virtualisation practice manager at backup app vendor Acronis.

## CLOUD-BASED DISASTER RECOVERY OPTIONS

**Managed applications and managed DR.** An increasingly popular option is to put both primary production and disaster recovery instances into the cloud and have both handled by an MSP. By doing this you're reaping all the benefits of cloud computing, from usage-based cost to eliminating on-premises infrastructure. Instead of doing it yourself, you're deferring DR to the cloud or MSP. The choice of service provider and the process of negotiating appropriate service-level agreements (SLAs) are of utmost importance. By handing over control to the service provider, you need to be absolutely certain it's able to deliver uninterrupted service within the defined SLAs for both primary and DR instances. "The relevance of service-level agreements with a cloud provider cannot be overstated; with SLAs you're negotiating access to your applications," said Greg Schulz, founder and senior analyst at the StorageIO Group.

> **"The relevance of service-level agreements with a cloud provider cannot be overstated; with SLAs you're negotiating access to your applications."**
>
> —GREG SCHULZ, founder and senior analyst, StorageIO Group

A pure cloud play is becoming increasingly popular for email and some other business applications, such as customer

relationship management (CRM), where Salesforce.com has been a pioneer and is now leading the cloud-based CRM market.

**Back up to and restore from the cloud.** Applications and data remain on-premises in this approach, with data being backed up into the cloud and restored onto on-premises hardware when a disaster occurs. In other words, the backup in the cloud becomes a substitute for tape-based off-site backups.

When contemplating cloud-based backup and restore, it's crucial to clearly understand both the backup and the more problematic restore aspects. Backing up into the cloud is relatively straightforward, and backup application vendors have been extending their backup suites with options to directly back up to popular cloud service providers such as AT&T, Amazon, Microsoft, Nirvanix and Rackspace.

"Our cloud connector moves data deduped, compressed and encrypted into the cloud and allows setting retention times of data in the cloud."

—DAVID NGO, director of engineering alliances, CommVault Systems

"Our cloud connector moves data deduped, compressed and encrypted into the cloud and allows setting retention times of data in the cloud," said David Ngo, director of engineering alliances at CommVault Systems, who aptly summarised features you should look for in products that move data into the cloud.

Likewise, cloud gateways, such as the F5 ARX Cloud Extender, Nasuni Filer, Riverbed Whitewater and TwinStrata CloudArray, can be used to move data into the cloud. They straddle on-premises and cloud storage and keep both on-premises data and data in the cloud in sync.

The challenging aspect of using cloud-based backups for

disaster recovery is the recovery. With bandwidth limited and possibly terabytes of data to be recovered, getting data restored back on-premises within defined RTOs can be challenging. Some cloud backup service providers offer an option to restore data to disks, which are then sent to the customer for local on-premises recovery. Another option is a large on-premises cache of recent backups that can be used for local restores.

"I firmly believe that backups need to be local and from there sent into the cloud; in other words, the backup in the cloud becomes your secondary off-site backup," said Jim Avazpour, president at OS33's infrastructure division.

On the other hand, depending on the data to be restored,

browse

The state of disaster recovery

Writing the DR plan

Virtual DR

Cloud DR

WAN optmisation

SMB best practices

**Cloud-based DR approaches side-by-side**

| | Managed primary and DR instances | Cloud-based backup and restore | Replication in the cloud |
|---|---|---|---|
| Instances | • Salesforce.com CRM<br>• Email in the cloud | • On-premises into the cloud<br>• Cloud to cloud | • On-premises into the cloud<br>• Cloud to cloud |
| Merits | • Fully managed DR<br>• 100% usage based<br>• Least complex | • Only requires cloud storage; cloud virtual machines are optional<br>• Usually less complex than replication | • Best recovery time objectives (RTOs) and recovery point objectives (RPOs)<br>• More likely to support application-consistent recovery |
| Caution | Service-level agreements define access to production and DR instances | Less favorable RTOs and RPOs than replication | Higher degree of complexity |
| Implemented via . . . | N/A | Backup applications and appliances | • Replication software<br>• Cloud gateways<br>• Cloud storage software such as EMC Atmos and Hitachi HCP |

features like compression and, more importantly, data dedupe can make restores from data in the cloud to on-premises infrastructure a viable option.

**Back up to and restore to the cloud.** In this approach, data isn't restored back to on-premises infrastructure; instead, it's restored to virtual machines in the cloud. This requires both cloud storage and cloud compute resources, such as Amazon's Elastic Compute Cloud (EC2). The restore can be done when a disaster is declared or on a continuous basis (pre-staged). Pre-staging DR VMs and keeping them relatively up-to-date through scheduled restores is crucial in cases where aggressive RTOs need to be met. Some cloud service providers facilitate bringing up cloud virtual machines as part of their DR offering. "Several cloud service providers use our products for secure deduped replication and to bring servers up virtually in the cloud," said Chris Poelker, vice president of enterprise solutions at FalconStor Software.

**Replication to virtual machines in the cloud.** For applications that require aggressive RTOs and recovery point objectives (RPOs), as well as application awareness, replication is the data movement option of choice. Replication to cloud virtual machines can be used to protect both cloud and on-premises production instances.

In other words, replication is suitable for both cloud-VM-to-cloud-VM and on-premises-to-cloud-VM data protection. Replication products are based on continuous data protection (CDP), such as with CommVault Continuous Data Replicator, snapshots or object-based cloud storage such as with EMC Atmos or the Hitachi Content Platform (HCP). "Cloud service provider Peak Web Hosting enables on-premises HCP instances to replicate to a Peak Web HCP instance instead of another on-premises HCP instance," said Robert Primmer, senior technologist and senior director content services, Hitachi Data Systems.

browse

The state of disaster recovery

Writing the DR plan

Virtual DR

Cloud DR

WAN optmisation

SMB best practices

## NEW OPTIONS, OLD FUNDAMENTALS

The cloud greatly extends disaster recovery options, yields significant cost savings and enables DR methods in small- and medium-sized businesses (SMBs) that were previously only possible in larger organisations. It does not, however, change the DR fundamentals of having to devise a solid disaster recovery plan, testing it periodically and having users trained and prepared appropriately. ⊙

**Jacob Gsoedl** is a freelance writer and a corporate director for business systems. He can be reached at jgsoedl@yahoo.com.

browse

The state of disaster recovery

Writing the DR plan

Virtual DR

Cloud DR

WAN optmisation

SMB best practices

# Unshackling disaster recovery with WAN optimisation products

**WAN optimisation can have a huge impact on data movement processes, especially for disaster recovery (DR). Learn about WAN optimisation products specifically aimed at improving DR, and what you need to have in place before you deploy WAN optimisation.** BY JEFF BOLES



**TRADITIONAL DR HAS** often revolved around tape just because DR has required so much data to be moved. But WAN optimisation can mean the difference between DR over the wire being possible or not, and in the age of the cloud, there's an over-the-wire data movement choice for nearly any system you can think of. This is proving a panacea to the more than 85% of organisations that have too much of their data unprotected in the face of a potential disaster.

In contrast with tape-based practices, DR over the wire is easier and requires less expense in manpower, transportation and physical media. Moving data over the wire also yields much better recovery points and recovery times than tape. Moreover, DR over the wire reduces the possibility of media errors or lost shipments that can often make tape the biggest question mark in a DR plan, and nearly impossible to test with enough rigour. For up-to-the-moment recovery, or avoiding the loss of a day or

more of data, over-the-wire DR may be the only way to go.

Certainly, achieving over-the-wire DR takes some serious technologies in the data centre. Identifying and moving the right data and executing application failovers are not simple tasks and require either significant manual support or good integration of tools like VMware's vCenter Site Recovery Manager or agent-based technologies such as Vision Solutions' Double-Take software. But the technology that may make or break over-the-wire DR may well be WAN optimisation.

Why is this? When Taneja Group examined WAN optimisation vendors' claims around what they can do with transmitted traffic, the cutting-edge vendors lay claim to serious transmitted data reduction (often as much as 95%) and lowered latency from the way they reduce traffic chattiness over the wire. Those two factors can create a magnitude of differences in how up-to-date your data is and how quickly you can be ready to spin up the environment in the event of a disaster. Moreover, WAN optimisation products can open the doors on where and how you do DR and can make it practical to provision a DR location nearly anywhere—from your own facility where you don't want to pay for a high-speed private line, to the numerous service providers that are coming to market with cloud disaster recovery offerings.

**The technology that may make or break over-the-wire DR may well be WAN optimisation.**



## WHAT TO LOOK FOR IN A WAN OPTIMISATION PRODUCT

With an eye towards drastically reducing DR data transmission and achieving these speed and ease-of-use benefits of

DR over the wire, here's a short list of what you should look for in a WAN optimisation product:

- **Designed for DR data:** Ask your vendor about its credentials for optimising your DR data stream, with an eye on the tool sets that you are using to move your DR data. There may be a world of difference between moving file data and moving the bits on the wire that make up EMC's SRDF. Either examine, or take a guess at, what your data footprint will be over the wire, and the priority of that different traffic. Then evaluate how well a given vendor can optimise your mission-critical data alongside your less important data. Moreover, if your mission-critical data is something very specific, like EMC's SRDF, then make sure your vendor has EMC's blessing and is a supported solution.
- **Designed for your DR site:** Make sure your vendor's product can be integrated into your DR site. If it is privately owned and operated, this may be easy, but many solutions built today are carrying data to a service provider or a hosted facility of some type, even if those facilities are from a provider like Iron Mountain or SunGard. Optimisation at two ends of the wire will be many times better than optimisation at only one end of the wire.
- **Designed for the right workloads:** Make sure your vendor of choice has a portfolio of products that can be applied to where your DR data movement needs are today and where they might be tomorrow. With the idea of the cloud rapidly shifting how businesses are thinking about IT, your workloads might move or be very different than anticipated when tomorrow arrives.
- **Designed to give you control:** Finally, with a solution designed to work in the network, you should expect that WAN optimisation products can provide control of that network. The age of the cloud will create rapidly changing utilisation

patterns that can cause interference with mission-critical workloads like DR. The right insight, along with sufficient control, can mean the difference between keeping your solution optimised under these rapidly changing demands, or running into issues that you can't address with anything short of a forklift upgrade. WAN optimisation devices are ideally placed to provide visibility into the network and are ideally equipped to shape network use.

With your eye on this short list, you can turn to examining the vendors on the market today, a few of which include Blue Coat Systems, Certeon, Cisco Systems, Citrix Systems, F5 Networks, Riverbed Technology and Silver Peak Systems.

Obviously, on top of these products, you must still have data replication, tools for coordinating what happens in the event of a disaster and, most important of all, processes and technologies for testing your plan and making sure your plan stays in step with the perpetual changes occurring in any IT environment. But with WAN optimisation in tow, you can finally put some of those technologies to work in pursuit of real business continuity. ⊙

**Jeff Boles** is a senior analyst and the director of Taneja Group's hands-on Technology Validation Services, focused on validating vendor solutions in real-world use cases. Jeff's background also includes more than 20 years of senior management and hands-on infrastructure engineering in the trenches of operational IT.

browse

The state of disaster recovery

Writing the DR plan

Virtual DR

Cloud DR

WAN optmisation

SMB best practices

# SMB disaster recovery best practices

**This technical tip outlines the essentials of disaster recovery and business continuity planning for SMBs. Learn about best practices for SMB DR planning and the basic steps that are required to put an effective disaster recovery plan in place.** BY PIERRE DORION



**DISASTER RECOVERY** isn't always easy, but following some key disaster recovery best practices is a good start.

It is possible for IT managers at SMBs to feel that they can easily recover from an outage because they have smaller IT environments and employ smart IT people. Conversely, there are instances where managers don't know how to build a disaster recovery strategy. In either case, this often leads to no disaster recovery planning at all. If an SMB intends to build a DR plan, it needs to follow the essentials for disaster recovery planning.

## DETERMINING IMPACT

The most important—and difficult—step in disaster recovery planning is to understand how an unplanned outage would affect an organisation. This step is referred to as a business impact analysis (BIA). Without the ability to determine the impact of an unplanned outage in a meaningful way, it be-

comes very difficult to determine the type of disaster recovery strategy is needed.

An “unplanned outage” refers to any unforeseen event that interrupts normal business activity for a period of time, such as an IT systems failure, fire, power outage or a natural disaster. Depending on the nature of the interruption, this can cause an organisation to lose revenue, have problems with customer satisfaction, lose opportunities or possibly go out of business.

That impact is determined by identifying the most critical business activities or functions, and then predicting what would happen if those processes stopped. This is where many inexperienced planners make a mistake: They are tempted to skip a few steps and go to solution mode.

DR planners should not assume there is a workaround or contingency available when a highly critical function goes offline.

The intention is to set a recovery time objective (RTO), which refers to how long can a process be down, and a recovery point objective (RPO), which refers to how much data can be lost, for critical functions and IT infrastructure.

Businesses must determine:

1. A financial value for a critical function, based on how much money is lost when the revenue stream is interrupted. An organisation’s accountant can usually help with this process.

2. How critical each function is for the organisation, based on how a function affects the revenue stream using a rating system—for example, one to five, where one is the most critical and five the least critical

3. How long a business function can be interrupted before it starts affecting revenue stream

4. How much client or business transaction information can be lost or re-created without seriously affecting the business

5. The IT infrastructure and systems upon which the business functions depend

## UNDERSTANDING RISK

The next step is the risk assessment, which complements the impact analysis. The impact of an outage and the anticipated risk that may exist will indicate the need to develop a recovery strategy.

Assessing risk is another area where planners can get bogged down. Do not attempt to calculate risk on the chance it could happen, or try to calculate annualised loss expectancy (which are both complex tasks). Keep it simple and be realistic about the kinds of risks your organisation could face, including specific threats tied to an organisation's geographic location. A risk exists for an organisation if there's nothing in place to maintain or quickly recover a critical function.

On the other hand, if a system identified as critical is found to have adequate redundancies and protection, you can move on to the next systems and applications.



## DEVELOPING A RECOVERY STRATEGY

Once critical functions and the supporting IT infrastructure have been identified and the impact of an outage is quantified using a monetary value or rating, a recovery strategy can be developed to help prevent or mitigate losses.

This is also when we need to start considering any existing contingencies or redundancies already in place. For example, if a critical application is hosted by a service provider and under a service-level agreement, it is probably safe to say that little to no recovery strategy is required for that application. However, a recovery strategy is required for applications that support critical functions but lack provisions to keep those applications operational.

A specific recovery strategy is determined by an organisation's anticipated financial losses if critical functions are unavailable, as well as the time needed to recover necessary applications.

An application with an RTO of within five days may do just fine with a tape backup process, but an application that needs to be up within an eight-hour business day might require remote data replication and/or standby IT systems at a recovery site. Outsourcing disaster recovery is also a viable strategy: Companies that cannot afford the cost of developing their own recovery strategy may consider paying for DR availability services or a "DR as a service" subscription.

The key is to always remember that the total cost of a recovery strategy should never exceed the losses it is designed to prevent.

browse

The state of disaster recovery

Writing the DR plan

Virtual DR

Cloud DR

WAN optmisation

SMB best practices

## DOCUMENTING THE RECOVERY PLAN

The next step is to document the recovery strategy and procedure, which forms the foundation for a disaster recovery plan. Keep it simple: Smaller businesses should not attempt to develop an enterprise-class DR plan. Very detailed disaster recovery plans take time to develop and are hard to maintain. At a high level, the disaster recovery plan should outline the priorities for system recovery, the RTO, recovery procedures, as well as the location of data backups and the contact info for key recovery personnel.

Testing the plan frequently will help identify what elements are missing and need to be added, instead of discovering problems with the plan during a disaster event. Every time a recovery procedure is tested, gaps and improvements are identified and this is how plan maturity is eventually achieved. ⊙

**Pierre Dorion** is data centre practice director and a senior consultant with Long View Systems in Phoenix, Arizona, specialising in business continuity and DR planning services and corporate data protection.

***Essential Guide to Disaster Recovery*** **is a SearchStorage.Co.UK.com e-product.**

EDITORIAL DIRECTOR
**Rich Castagna**

UK BUREAU CHIEF
**Antony Adshead**

SENIOR SITE EDITOR
**Sue Troy**

ASSISTANT SITE EDITOR
**Francesca Sales**

CREATIVE DIRECTOR
**Maureen Joyce**

VICE PRESIDENT/GROUP PUBLISHER
**Mike Kelly**
mkelly@techtarget.com

SENIOR VICE PRESIDENT, INTERNATIONAL
**Bill Crowley**
bcrowley@techtarget.com

**TechTarget**
275 Grove Street, Newton, MA 02466
www.techtarget.com



**About TechTarget:** TechTarget publishes media for information technology professionals. More than 100 focused Web sites enable quick access to a deep store of news, advice and analysis about the technologies, products and processes crucial to your job. Our live and virtual events give you direct access to independent expert commentary and advice. At IT Knowledge Exchange, our social community, you can get advice and share solutions with peers and experts.

browse