Rethinking Disaster Recovery Planning in a Virtual World

A Dell White Paper

Dell Enterprise Solutions Group Marketing

THIS WHITE PAPER IS FOR INFORMATIONAL PURPOSES ONLY, AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.

August 2013

Table of Contents

Figures

Introduction

A myriad of threats face the IT systems and confidential data of organizations – public and private, large and small. And horror stories abound:

In July 2010, the crash of a storage device caused the loss of a well-known retailer's online services. In the four days it took to restore online purchasing capability, 12% of the company's total revenues were lost.

Another event in 2010 involved one of the four largest banks in the United States. The bank lost services for its 16 million online customers due to a software bug that corrupted key files in the authentication database. Because both the active and standby data-storage units were corrupted, the bank's only option was to rebuild the database. As a result, online services were not restored for two days and even then, the applications suffered hours of poor performance because of pent-up demand from users.

Many IT professionals read about these types of disasters and shrug their shoulders. There are a number of different reasons why you might discount these painful stories:

- These are just isolated catastrophes.
- My company doesn't have even a fraction of that bank's 16 million customers. Our losses would be far smaller and thus we don't need to take extraordinary precautions.
- Even though I personally think we need to prepare for disasters, we can't afford to spend money to protect our systems and data. Management just won't allow it.

Why should you care?

Let's forget about the size of the mega-bank or the famous retailer and make our discussion more personal. What if you had years of your organization's e-mail, databases and records wiped out by a virus, power outage, system failure or flood?

- What would be the revenue impact of a 4-hour outage on your organization? How about a 24-hour outage?
- How would an outage effect your organization's reputation and customer goodwill?
- How long would it take for your most valued customers to seek competitive alternatives?

In an era where huge percentages of business depend on online services and up-to-date data, it's imperative to have a comprehensive plan for backup and recovery. Take the sobering case of a small company whose "disaster recovery plan" consisted solely of running nightly tape backups. The company was totally caught by surprise when its Microsoft Exchange Server failed at the end of the quarter, costing the company approximately $50,000 in lost orders. Even though the IT department was diligent in backing up data it never performed test restores and hadn't verified that the backups would be recoverable.

In reality, it doesn't matter how big or small your organization is—you need a disaster recovery (DR) plan. A study by The Enterprise Strategy Group in 2012 indicates that 53% of organizations would experience significant revenue loss or other adverse impact if downtime of tier-1 data exceeded more than an hour.[1] And just because others in your organization might choose to ignore the looming problem behind the curtain, it's important for IT professionals to be proactive.

Where do we start? What are we trying to accomplish?

At first pass, DR planning looks like an overwhelming task given the myriad of threats ranging from natural disasters, cyber-attacks, power outages, and software malfunctions to application failures. Where does one start? Compliance? Data security? Establishment of a DR site?

The good news is that thanks to modern technology, a complete DR solution no longer means the establishment of a secondary backup site, although it may be worthwhile to at least scope out the costs of a backup location. The DR/BC planning project should be seen as an opportunity to look at all of your systems/processes and to analyze current needs processes, personnel, systems and vendors.

[1] Enterprise Strategy Group "The Modernization of Data Protection" April 2012

Developing a disaster recovery planning document

This white paper is intended to provide a few high-level insights as to how you can develop and move forward on a disaster recovery plan. It is not a "how-to" guide for developing a DR plan as there are already numerous sources online that can serve as templates for developing a complete disaster recovery plan. Plans vary from the concise free guide from TechTarget to very detailed templates from Texas A&M University and the National Institute of Standards. (See appendix for these three documents)

A DR plan usually includes important strategic components such as a business impact analysis that includes a thorough examination of critical business applications, systems and processes. Other essential elements of the plan are the development of a DR policy statement, the identification of preventative controls and the determination of recovery processes. The DR plan also includes far more mundane yet critical information such as employee contact information, vendor contact information and emergency response procedures. Again, for assistance in developing a plan tailored to your organization we suggest that you refer to the documents and templates included in the appendix.

Disaster recovery solutions range from a simple backup scheme to a fully replicated data center. However even in the seemingly simplest cases, much care needs to be given to contingency planning. Remember our earlier example of the company who had not tested their backup plan and ended up paying the price by losing significant business at the end of the quarter. Any plan should at a minimum cover how the organization brings systems and application back online after an outage to ensure business continuity.

Important considerations when developing your plan

We recommend that you consider these suggestions when developing your DR plan:

1) **Prioritize and rank your most important applications based on value and impact**.

Data value is not one-size-fits-all, nor is the value of data static. Thus a tiered protection/recovery strategy should be developed that balances affordability with risk mitigation. Generally, data and applications can be broken into three categories:

Tier 1: Mission-critical data and applications that needs to be available all the time

Tier 2: Important data and applications that don't require the same availability as mission-critical data

Tier 3: Older or less essential data that still must be retrievable if necessary

After ranking data, service levels can be aligned in relation to the business consequences of losing a particular application or system.

2) **Evaluate, automate and optimize your production and recovery infrastructure**

As mentioned earlier, one benefit of the disaster recover planning project is that it can be an opportunity to simplify your infrastructure and processes with an eye towards business resilience. It's also an opportunity to virtualize applications and systems wherever possible. Investigating the standardization, consolidation and convergence of infrastructure may not only pay dividends in terms of data protection but could also result in lower operating costs.

3) **Address the whole picture–technology, business and people**

A successful disaster recovery plan requires a holistic approach that considers business imperatives, technological choices and human resources. It certainly doesn't make financial sense to have a roomful of telemarketers unable to perform their duties for four hours due to a system failure. Nor does it make financial sense for an administrator to spend hours per week dealing with data backup problems when the process could be automated for a reasonable upfront cost. Thus the planning team's goal should be to implement a comprehensive framework to keep systems and data safe while maximizing productivity.

4) **Understand your recovery point objective and recovery time objective**

One of the most important aspects of disaster recovery planning is establishing recovery time objectives (RTOs) and recovery point objectives (RPOs). These may vary by application within your environment.

The RPO measures how much data loss your organization can tolerate in the event of an outage. Some organizations may be able to withstand losing 24 hours' worth of data and thus may only need to backup data once a day. Other businesses such as financial institutions or healthcare providers may not be willing to tolerate any downtime due to fiduciary concerns or federal regulations and therefore may require more robust protection.

The RTO is the maximum amount of time that a system or application can remain unavailable before there is an adverse effect on the organization. Establishing your RTO usually requires weighing the tradeoffs between risk and cost. If Company A requires a short RTO of 5 minutes they will probably spend much more on disaster recovery than Company B that is willing to wait 8 hours to recover their data.

5) Take an "all risk" approach to protect your organization

There were an astounding 4.6M instances of data loss in the US in 2010[2]. When you consider that on average 1 in 5 recoveries of data fail[3], the amount of time spent on successful and unsuccessful data recoveries is staggering. To reduce the possibility of a catastrophic event, it is important to take an "all risk" approach. After all, it doesn't do much good to have a plan for a hurricane evacuation if you are ignoring other potential risks such as outdated backup procedures. At a minimum, organizations should be prepared for:

- Data center outages–Includes hardware failures of networks, storage: servers and corruption of applications and databases
- Human-caused events–Includes vandalism, riots and terrorist attacks
- Cybercrime–Includes denial of service attacks, computer viruses, and phishing
- Natural disasters–Includes fire, flood, hurricanes, and pandemics
- Internal security breaches–includes outages caused by human error or malicious acts by disgruntled employees

6) Validate, test and practice to ensure preparedness

While many organizations are able to do a credible job developing a DR plan, some IT teams make the mistake of letting the plan sit in a drawer and pray that the plan never needs to be activated. To enhance the value of the plan and to keep your organization protected, periodic infrastructure and integration testing must be performed.

By setting up periodic testing, organizations can validate the integrity of the plan and ensure that recovery procedures are executable. It's also necessary to assess how changes made to hardware, software or application platforms may affect recovery capabilities. Testing is also critical to gauge the capabilities of staff members who will be needed if disaster strikes.

Testing methods can range from round-table reviews to disaster recovery walkthroughs to planned or "surprise" disaster simulations. Results of testing should be carefully documented and appropriate changes to disaster recovery operations should be incorporated to reflect changes in the business or computing environment. The disaster preparation templates provided in the appendix include sections on setting up periodic testing of your organization's disaster recovery systems and procedures.

Get your executives onboard. You'll be surprised how receptive they will be.

Getting started on a DR plan may seem like a daunting challenge particularly if you have limited DR expertise and lack sufficient funding. A traditional comprehensive disaster recovery solution can be very expensive, usually involving a DR site with expensive servers, network equipment, storage and software. In these scenarios, upgrades at the primary site usually require upgrades at the DR site. Operating costs can also be significant because of the need for periodic testing of the DR solution (many organizations won't invest in the resources needed for scheduled testing).

[2] TechWench, All Things Tech, Oct. 13, 2011

[3] Enterprise Strategy Group "The Modernization of Data Protection" April 2012

Low-cost solutions range from tape backup to cloud storage but these choices don't usually constitute a complete protection plan. For example, recovering data from tape can take days or fail entirely. Backing up to the cloud is a non-starter for many organizations concerned about data security. Another concern is that recovering lost data from the cloud can be time-consuming. Thankfully, there are a number of technologies available today that can be combined to provide a complete, integrated solution while controlling expenditures.

Given that there will be upfront and ongoing costs involved, it is imperative to obtain executive sponsorship for development of a plan. Your executives probably recognize the need for DR planning as part of their risk management strategy. However a key reason why top management doesn't approve DR budgets is that there is no perceived return on investment. Executives believe they are spending scarce dollars for something they hope is never used. However you can get your management team to sign on to development of a DR plan by focusing on business-critical factors such as risk mitigation, compliance requirements, increased revenues, better customer support and competitive advantage.

Do not let price get in the way of this exercise–give your executives options. While a second data center with complete redundancy is pricey, that doesn't need to be the only option. Maybe the appropriate solution will be to virtualize the most important applications and take advantage of native virtual protection tools.

Consider bringing in DR professionals to perform the above functions such as risk and vulnerability assessments. There are numerous organizations that specialize in IT disaster recovery strategy development and crisis management planning. For example Dell has certified disaster recovery and business continuity consultants available to perform activities ranging from a gap analysis of your existing environment to program design and implementation.

Once you choose the option that's right for your organization, make sure you have testing procedures and schedules established. And most importantly: make sure you keep management interested/involved in the DR/BC process on an ongoing basis.

Leveraging servers to create a highly available environment

The improvement in reliability of servers has been well documented and is a welcome development for IT professionals. But even the most reliable severs, designed with redundant components can move to the next level of availability through high availability (HA) clustering, i.e., the arrangement of redundant servers in groups to protect against multiple component failures. By removing failure points, higher levels of availability can be achieved and organizations can realize the goal of the five nines (99.999% availability). Correctly designed and implemented, an HA cluster can proactively detect hardware or software problems and automatically restart applications on other systems.

If a disaster recovery site is a necessity you may consider implementing blade servers at the second site. Although the cost may be slightly higher upfront when compared to rack servers, the scale of the blade technology eventually should cost-justify the investment. The blade chassis maximizes efficiency by sharing resources such as power and wiring across all of the blades in the enclosure. Easier to manage than many disparate solutions, blades are frequently called a "data center in a box". And given that the secondary site may not have sufficient trained technical personnel, the level of simplicity afforded by blades will make a great deal of sense for many organizations. In addition to the other benefits, a blade server solution requires less space than conventional rack mounted servers, providing additional cost savings at the secondary site.

So let's talk virtualization

Traditional methods of disaster recovery usually involve backing up data to disk or tape at a second site or utilizing a DR service provider. Organizations that require a more sophisticated approach such as a redundant data center many times have difficulty justifying the cost. Often the business case analysis makes organizations choose which applications to protect while leaving others unprotected.

Server virtualization has proved to be a game changer for IT departments, helping organizations increase efficiency of physical resources while decreasing capital and operating costs. A key benefit of virtualization is the ability to migrate workloads between physical servers, Thus in the event a server needs to be taken offline for maintenance, the server's consolidated workloads can be easily ported to another server or servers, saving administrative time and maintaining business continuity. And, if you are looking at establishing a DR site, virtualization eliminates the need to have a 1:1 server relationship as applications can be backed up to VMs rather than physical machines.

As organizations continue to expand virtualization through their IT environment, backup administrators are learning to utilize native virtualization tools for backup and recovery. The result is that organizations that once were choosing to keep half of their applications unprotected (have the potential to now protect their entire environment for the same cost or less.

It should be noted that while virtualization increases the flexibility of data protection it also makes effective disaster recovery planning a necessity. The fact that more applications are riding on each individual server dictates that the servers be highly available.

Storage systems aren't just for storage

You can leverage a SAN based storage system to protect business-critical applications such as Microsoft® SQL Server® against downtime and disaster. Leading-edge storage systems enable administrators to deploy a robust DR plan that includes replication w with multi-site failover.

Deploying storage based data protection reduces the time and costs associated with traditional DR methods. As discussed earlier, DR infrastructures need to be periodically tested. Leading-edge storage systems address this need, enabling non-disruptive scheduled maintenance, DR testing and workload reallocations. For example, Dell storage systems utilize wizards to set up replication for primary and remote sites, and management is as simple as using a point and click interface.

When evaluating storage solutions, it is important to focus on storage systems that can seamlessly integrate with virtual DR management products. A storage system that tightly integrates with, for example, VMware® vCenter Site Recovery Manager™ (SRM) automates the process of setting up and configuring virtual recovery plans.

The next section of this paper contains three stories of Dell customers using a combination of these strategies to implement disaster recovery. The first two cases demonstrate the advantages of combining virtualization and storage to protect systems and applications. The third case demonstrates some advanced disaster recovery protection capabilities that can be deployed through data protection software. All three of these cases underscore how Dell data protection solutions can make data and system restores a fast single-step process, accelerating typical recovery times from days to an hour or less.

Business Cases

USE CASE I:

Automated DR with Dell Compellent and vCenter Site Recovery Manager

As discussed earlier, organizations that need to protect a large part of their infrastructure can consider virtualizing as many applications as possible in order to benefit from the inherent data protection capabilities afforded by virtualization technology. Our first use case addresses the replication of data to a backup site utilizing VMware's vCenter SRM in conjunction with Dell Compellent Storage Center.

SRM provides an efficient way for enterprises to set up, test and execute effective disaster recovery plans. Dell Compellent tightly integrates with SRM through a storage resource adapter (SRA). Compellent maximizes the value of SRM by automating the disaster recovery process and Compellent Copilot Support provides a single point of contact for efficient and effective resolution of Compellent and VMware-related issues. Compellent integration with VMware SRM enables full non-disruptive validation of recovery plans within an isolated testing environment without disrupting production.

The Dell Compellent SAN replicates highly efficient replays (point-in-time-copies of a volume) between local and remote sites over IP networks, providing SRM-based disaster recovery at a lower cost than other replication solutions. Administrators can manage replications and SRM-based recovery through a single interface, Compellent Enterprise Manager. Compellent also provides fully engineered, end-to-end, virtualization solutions for Microsoft Hyper-V and Citrix.

Compellent integration with SRM helps administrators accelerate the recovery process. Unlike traditional SAN where administrators might need to prepare each storage volume for the VMware environment during the recovery process, Compellent allows administrators to complete the mapping ahead of time, eliminating the tedious work of mapping volumes by hand,. In the event of a problem, administrators using enterprise manager can activate recovery for multiple VMware servers from a remote site with a single click.

Disaster Recovery with VMware SRM and Dell Compellent

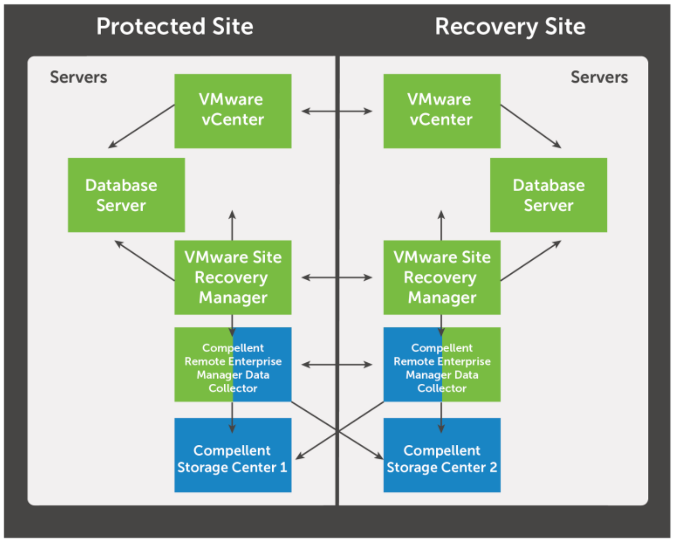

Protected Site
Recovery Site
Servers
Servers
VMware vCenter
VMware vCenter
Database Server
Database Server
VMware Site Recovery Manager
VMware Site Recovery Manager
Compellent Remote Enterprise Manager Data Collector
Compellent Remote Enterprise Manager Data Collector
Compellent Storage Center 1
Compellent Storage Center 2

Figure 1. Dell Compellent's tight integration with VMware Site Recovery Manager maximizes the value of SRM.

Dell Compellent helps protect a cloud service provider's customers

One of many success stories of an integrated Compellent/VMware solution is an implementation for FireHost, a leading provider of secure cloud services for some very large enterprises including 3M and Whole Foods.

The company now runs five SANs in its data centers across North America and Europe in a "secure cloud pod" that hosts more than 5,000 virtual machines. Remote Instant Replay replicates incremental changes in data between the arrays over the wide-area network. The combination of Compellent and VMware allows FireHost to offer two weeks of backup for every secure server they sell. Compellent also enables FireHost to meet aggressive service level agreements (SLAs) and provide recovery times of minutes in most cases.

USE CASE 2:
Comprehensive disaster recovery with Dell EqualLogic Virtual Storage Manager

Organizations that need to replicate data but do not require the level of automation afforded by vCenter SRM may consider implementing VMware with Dell EqualLogic Virtual Storage Manager (VSM).

The EqualLogic VSM is a vCenter plug-in that allows administrators to coordinate data protection and recovery within their vSphere virtual environment. The VSM is a virtual appliance that can be installed into an existing VMware vCenter environment. It should be noted that Dell servers also feature a plug-in for VMware vCenter which simplifies server management while providing smooth integration with Dell Storage. Together, these plug-ins provide administrators the ability to manage both Dell servers and Dell storage through the familiar vCenter interface.

Virtual Storage Manager allows IT professionals to create hypervisor-consistent snapshots, clones and replicas for data protection and disaster recovery. Administrators can select an entire folder of VMs or datastores and create a Smart Copy. Individual Smart Copies are useful for many functions including testing new patches or software builds but the real power from VSM comes from its built-in scheduling function. This provides a layer of automation that simplifies protection of VMs, folders, and datastores.

Instead of deploying a new VM, patching it, installing the applications and backup agent, and then recovering data from the previous known good backup, Smart Copies can be utilized to rapidly roll a failed virtual machine back to a good point-in-time and business can continue with minimal disruption, even in an alternate datacenter.

EqualLogic VSM provides simple data management through a graphical interface that helps administrators simply define data protection policies, create online backups, and quickly recover their data, all with just a few button clicks–increasing uptime, and enabling quicker recoveries in the event of an outage.

Disaster Recovery with Dell EqualLogic VSM

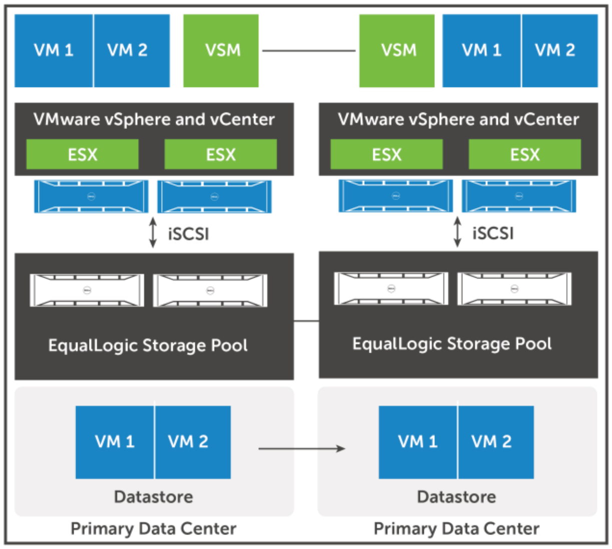


Figure 2. The EqualLogic Virtual Storage Manager is a virtual appliance that can be installed into an existing VMware vCenter environment.

Dell EqualLogic helps protect customer data in hurricane country

Because of its concern about natural disasters and to better manage its compliance requirements, Community Bank & Trust of Florida deployed a VMware solution on Dell™ PowerEdge™ servers and Dell EqualLogic storage

The new platform allows monitoring and reporting of storage information at the volume and VM level, from one central location. Administrators report that storage administration time has been reduced by 75%.

The bank is very satisfied with its highly stable environment. EqualLogic Auto- Snapshot Manager (ASM)/VMware Edition and ASM/Microsoft Edition seamlessly automate SAN-level replication between the bank’s data centers. The virtualized design of EqualLogic has maximized availability- no storage outages have occurred in the three years since installation.

USE CASE 3:
Accelerate backups and recover anywhere with Dell AppAssure

Our final use case explores a solution for organizations that need to upgrade their disaster recovery capabilities but are not looking to replace their existing storage system.

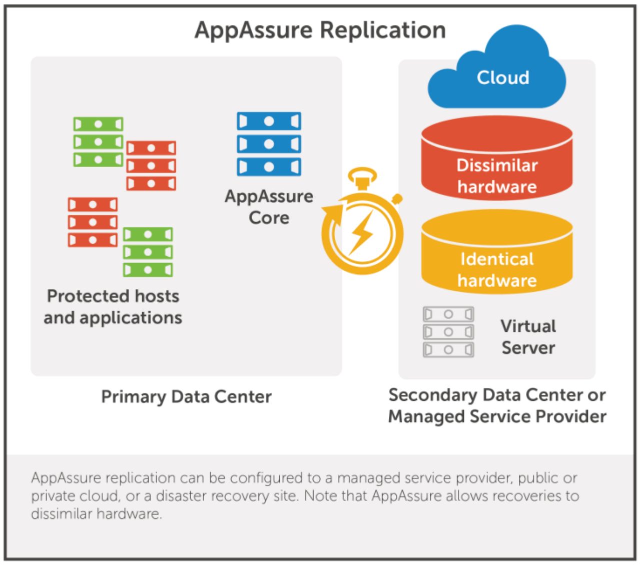
Dell AppAssure provides application-aware backup, replication and recovery for physical, virtual, and hybrid environments. Replication can be configured to an offsite AppAssure core machine, managed service provider, public cloud or private cloud. Customers can choose to install AppAssure as stand-alone software or as part of the AppAssure-powered DL4000 data protection appliance.

A primary reason that some organizations do not move forward with disaster recovery implementations is cost, particularly the charges associated with wide area networks and the cost of deploying identical hardware configurations at the primary and remote sites. AppAssure helps customers cost justify DR projects in several ways. AppAssure WAN-optimized deduplication reduces the amount of data that needs to be replicated resulting in an 80% reduction in bandwidth requirements. AppAssure Universal Recovery™ eliminates the need to restore data and applications to identical machines. With Universal Recovery, administrators can perform cross-platform recoveries from physical to virtual servers (P2V) virtual to virtual (V2V) virtual to physical (V2P), and even physical to physical (P2P) for bare metal restores to dissimilar hardware

The ability to quickly recover after an outage is obviously one of the most important factors in disaster recovery planning. AppAssure Live Recovery™ enables the recovery of data and applications in minutes and even seconds. Rather than waiting for the entire recovery to complete, users can have immediate access to data after an outage occurs, thus ensuring business continuity.

In summary, the revolutionary capabilities of AppAssure can transform disaster recovery operations for an organization either as standalone software, an all-in-one appliance or integrated with Dell Compellent or Dell EqualLogic as part of a total Dell DR solution.

Flexible Disaster Recovery with Dell AppAssure



AppAssure replication can be configured to a managed service provider, public or private cloud, or a disaster recovery site. Note that AppAssure allows recoveries to dissimilar hardware.

Figure 3. Dell AppAssure provides application-aware backup, replication and recovery for physical, virtual, and hybrid environments.

AppAssure protects irreplaceable data for some very important customers

Information Management Services (IMS) provides IT services to a number of prestigious organizations including the National Cancer Institute and the Centers for Disease Control and Prevention. Because of its need to protect the sensitive and irreplaceable customer data, IMS chose AppAssure.

IMS appreciates AppAssure’s nightly consistency checks that ensure the recoverability of important applications and data. The customer no longer ships tapes offsite and instead replicates snapshots in real-time to an alternate site. They are able to easily recover data at any point in time with the click of a mouse and have found that AppAssure provides the granularity necessary to recover even a single email quickly and easily.

.

What can Dell do for you?

In this paper, we have discussed DR solutions ranging from a simple backup scheme to a fully replicated data center. And, hopefully we have made a convincing case that disaster planning is not necessarily an overly burdensome or cost-prohibitive undertaking.

When reviewing your disaster recovery options, a prudent first step might be to contact your Dell account team or Dell channel partner. Dell provides a wide portfolio of solutions that help organizations protect information, enhance application availability, and recover quickly from disasters. We have focused on storage and virtualization technology in our use cases and we sincerely believe that those technologies are the best platform for an effective disaster recovery solution. To conclude our paper let's look at a few other reasons that makes Dell can be a key strategic partner for your disaster recovery implementation.

Dell servers

Virtualization can be deployed on any server, but that doesn't mean all servers are equal for virtualization. Dell designs PowerEdge servers to provide the best possible performance, optimizing for virtualization across the entire portfolio, to meet today's density, flexibility and performance needs, without locking customers into proprietary infrastructures. Dell servers feature a wizard that can automatically update all servers in a cluster without losing workload productivity.

Dell has been deploying virtualization on PowerEdge servers since VMware released its first server hypervisor in 2001. We also provide integrated solutions with partners such as Citrix and Microsoft. Our engineering teams have worked together for years to advance functionality, integration and performance, resulting in servers that are endowed with industry leading reliability, availability, and quality.

VRTX for disaster recovery

Dell VRTX is a new "data center in a box" solution that includes high-performance PowerEdge server nodes, integrated storage, and simplified integrated networking for fast connections and enterprise-class manageability. VRTX has the functionality and raw power associated with sophisticated data centers have, but is easily managed, fits under a desk, and does not require special power or cooling.

VRTX integrates with VMware vSphere and Dell vRanger, a backup and disaster recovery solution specifically designed for VMware environments to provide yet another DR option for multi-site operations.

Dell Professional Services

Dell IT Consulting offers a flexible end-to-end approach to help organizations fulfill their DR requirements Dell professional services consultants employ proven methodologies to deliver disaster recovery expertise that help protect the availability of critical systems and data. Our certified business continuity professionals can help you minimize risk by developing a disaster recovery plan, business impact analysis, IT recovery analysis and emergency response plan. Our services can also include system design, implementation and customer support.

Some of the areas where Dell expertise can make the difference in the success of DR planning are:

- Executive participation in the DR planning process
- Regulatory compliance
- Application recovery requirements and financial impact analysis
- Design of replication and virtualization environments
- DR testing to ensure that systems and staff are ready
- Analysis of test results and implementation of continuous improvement activities

Dell designs its services to be modular in nature, which means that you can apply those services that best fit your requirements. And if IT budgets are a concern, our professional services consultants can design a plan that can be implemented in stages and over years if necessary. What's most important is to put the disaster recovery plan in place.

Summary

In an era where so much depends on online services and up-to-date data, it is crucial to have a comprehensive plan for backup and recovery. A successful disaster recovery plan requires a holistic approach that considers business imperatives, current systems, staffing, procedures and technological choices.

Dell offers our customers the widest possible choice of robust and resilient infrastructure products that can be the foundation of any disaster recovery solution. Dell is dedicated to helping customers meet their critical challenges with solutions that help organizations achieve maximum efficiency, effective disaster recovery, and flexible scalability to meet the needs of the future. The Dell team would welcome the opportunity to come on site to explore your opportunities and challenges and help you define a path forward that will achieve your disaster recovery objectives.

Appendix

Resources

Disaster Recovery Templates

http://searchdisasterrecovery.techtarget.com/feature/IT-disaster-recovery-DR-plan-template-A-free-download-and-guide

http://www.ct.tamus.edu/departments/informationtechnology/extras/ITDisasterRecoveryPlan.pdf

http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf