



Disaster Recovery and Continuity of Operations Planning

Keeping your organization operating at its best while preparing for the worst

TABLE OF CONTENTS

- 2** Network Management
- 3** Data Storage Solutions
- 3** Unified Communications
- 4** Recovering Servers
- 5** Client Access
- 6** Power Management
- 6** Security and Disaster Recovery
- 7** Manufacturer Options

Executive Summary

For any government organization or educational institution to fulfill its mission, it's important for data to be continually secure and available. Numerous events over the past few years have led to a heightened awareness of the need to be prepared for the worst.

IT departments are now faced with the pressing concerns of growing demand for and reliance on access to information, along with ensuring continuous operation during a disaster.

These concerns are forcing organizations to bring a renewed focus to disaster recovery (DR) and have a comprehensive continuity of operations plan (COOP) in place. Having a thought-out, detailed strategy for disaster recover and continuity of operations puts organizations in a position to keep their systems running when problems occur.

Most organizations need to place a high value on being prepared for disasters of any kind because the ramifications of failing to do so can be very costly, and could result in a loss of public confidence, putting public safety at risk, reduced staff morale and effectiveness, and downtime that can cost organizations a great deal of money.

A plan that helps operations get up and running quickly or keeps them up and running with a minimal loss of data, information and productivity is now a necessity. This white paper will benefit organizations by informing and helping them plan out their strategies for DR and COOP.



Network Management

In disaster situations, networks can be managed remotely, whether from across the room or from another building, city, state or even country. Organizations can choose to manage the network themselves or outsource this task.

In-house management requires a sizable investment in people, processes and technology. It requires properly trained staff available around the clock; a strong set of standard operating procedures defined to handle various events; and a fault-tolerant infrastructure to monitor and generate alerts based on pre-established parameters.

Organizations can find management solutions that offer varying levels of visibility, control and application. At the console of a management device, managers can literally see what is transpiring on the network by viewing the screen and/or panel and lights on the device itself.

But with this kind of insight available, where an organization has visibility into network conditions remotely in an actionable way, it becomes impractical to devote human resources to these mundane tasks. This opens the possibility of outsourcing network management to a managed service provider. Many organizations reach this conclusion.

Two key considerations for outsourcing your network management are price and contractual obligations. If terms can be defined and agreed to, outsourcing can be far more effective and efficient (as well as less costly) compared to an in-house management strategy.

Organizations utilize hosted managed services (HMS), which are usually based on service level agreements. SLAs allow the organization to determine the degree of outsourced management that best suits it. This model scales well and ultimately proves more cost effective than self-maintaining the environment 24x7.

Network Load Balancing

Network load balancing is the process of spreading the work or balancing the workload between two or more servers, network links or other devices. Load balancing also increases resiliency within the network by potentially eliminating single points of failure and by providing seamless continuity should a network link, server or other device fail.

Choosing an HMS provider

Before signing a contract, it is important to investigate how an HMS provider runs its network operations center (NOC). Only in doing so can you responsibly select a provider to monitor and manage your network.

For example, find out what certifications the provider has and what is its overall reputation is in the marketplace. How well is its NOC staffed? What kind of service level agreements does the provider offer, and will any of them aptly fit your needs?

You may want to inquire as to what green energy measures the facility has implemented. And it's critical to know what the service will truly cost.

Network load balancing can be accomplished within the network using software (such as certain operating systems) or through purpose-built hardware. When properly deployed, load balancing can add critical elements to an organization's disaster recovery plan or COOP.

WAN Acceleration

Consolidating an organization's data to a data center as well as a disaster recovery site can lead to problems when attempting to access vital information quickly. Wide area network (WAN) optimization resolves this issue by accelerating protocols, compressing traffic and caching files. It speeds up applications such as Exchange, Citrix and web applications.

Acceleration statistics vary by manufacturer, but backup and recovery of Windows data processes can be accelerated up to three times their normal speed, while bandwidth utilization can be decreased by more than 60 percent, according to some manufacturer claims. WAN acceleration should be considered essential to your DR plan.

Data Storage Solutions

Disaster recovery plans and COOP tend to focus heavily on technology, while neglecting the enormous investment in paper-based resources. A document management system that transfers those paper-based resources into a space-saving, more-manageable electronic format is a critical component of any plan.

A management system begins with document capture, which involves making digital copies of the original paper documents. This is typically done with a scanner or multifunction device. Once the content is in an electronic format, it is indexed and stored in a central repository.

Being able to quickly and easily locate important documents in the aftermath of a disaster makes a document capture and management system invaluable to a DR plan.

Disk-based Storage

Disaster recovery can utilize many storage solutions. Direct-attached storage (DAS) is one option. DAS offers two varieties of storage: mirrored disk and the various redundant array of independent disks (RAID) solutions. Both options protect from the most common form of system interruption, a drive failure.

Disk-based storage offers advanced features helpful to DR such as cloning, snap shooting and continuous data protection (CDP).

- **CLONING:** This technology automatically copies production LUNs (logical unit numbers) to another location on the system so that if the production copy failed or corrupted, the cloned copy could be brought into action for nearly immediate recovery.
- **SNAP SHOOTING:** This technology copies file changes to a disk from a particular point in time forward. So a file can be recovered from the point in time where it is deleted or changed.
- **CDP:** This technology monitors an organization's files and as a file is changed or "auto saved," a copy of the changed bytes/blocks is replicated to either a local directory or remote location.

Tape Archiving

Another storage option for disaster recovery is tape. Tape is a data storage device that reads and writes data onto magnetic tape. It is typically used for archiving and allows for access to data sequentially rather than randomly.

Tape is portable (unlike disks, tape can be removed from a drive and taken to another location for recovery or storage), green (tape requires no power other than the read/write drives), dense and very fast. Many organizations have turned to a combination of disk and tape storage for preserving their archives.

When using either disk or tape, an advanced technology known as data deduplication can provide valuable storage benefits. Data deduplication reduces storage needs by eliminating redundant data. Only one unique instance of the data is retained on the storage media.

Hierarchical Storage Management

Another approach for long-term retention of archival data is a hierarchical storage management (HSM) solution, which involves migrating data from its production location to a lower cost/tier of storage while leaving a "stub" file behind.

The stub file allows applications or file searches to see the file in its normal location, but when accessed, recall the file from its lower-cost location. This lower-cost location can be either a slower disk such as SATA, or even a backup solution such as tape.

Unified Communications

The adoption of "one-wire" infrastructures has combined e-mail, voicemail, cell phones and public address systems onto one data and voice IP network, and the use of wireless technology has further extended the network beyond the four walls of a building. The disaster recovery challenge is adapting the network for mass communication and emergency notification.

In recent years, emergency notification has taken on a new meaning: sending out messages to entire office buildings or an entire campus of buildings. IP phones, sitting on the desks of every staffer, have become more than just phones.

They can also be used to display a text message and play audio broadcasts from the handset speaker. In a matter of seconds, a public safety official can log onto an internal website and send out a prerecorded and pretyped emergency message to any building within the organization.

IP-addressable speakers can be deployed throughout a building or across a campus. These IP speakers are Power over Ethernet (PoE) devices that can be plugged into any CAT 5 jack on the network, turning a voice and data network into a public address system. For remote outdoor locations, IP speakers can also be deployed with wireless radios to extend the network.

Non-IP Network Options

A desktop notification system (DNS) can be deployed throughout an organization where IP phones or IP speakers are not yet in use. This small desktop client sits in the system tray of workstations until an emergency notification is sent. Once activated, the DNS displays a text message about the alert while playing an audio broadcast via desktop computer speakers if available.

Recovering Servers

Developing a comprehensive and cost-effective recovery strategy for servers is challenging. Server consolidation, with the goal of reducing data center cost and complexity, should be explored before developing a recovery plan. The goal of server consolidation is to reduce the number of servers, as well as make the environment simpler to administer and maintain — and easier to recover.

The four most common forms of server consolidation carried out today are:

- **PHYSICAL CONSOLIDATION**, which involves consolidating multiple file, print and database servers onto fewer, larger, clustered servers;
- **VIRTUAL CONSOLIDATION**, which involves migrating multiple physical servers onto fewer servers through virtualization;
- **DATA CENTER CONSOLIDATION**, which allows organizations with multiple data centers and remote sites to consolidate servers and storage devices to a centralized data center;
- **APPLICATION SERVER CONSOLIDATION**, which allows for the consolidation of multiple application servers onto fewer physical or virtual systems.

Disaster Recovery Lifecycle

Maintaining a disaster recovery plan or COOP is an ongoing process, a lifecycle rather than a once-a-year checklist. There are five key phases to a disaster recovery lifecycle:

- **ANALYSIS:** In this phase organizations determine potential impacts, identify likely threats and develop impact scenarios.
- **SOLUTION DESIGN:** With this phase, the goal is to identify the most cost-effective and technically viable solution.
- **IMPLEMENTATION:** This phase consists solely of the execution of the design elements identified in the solution design phase.
- **TESTING AND ACCEPTANCE:** To be certain that disaster recovery plans and COOP meet the needs of the organization, testing is required to assure process and acceptance.
- **MAINTENANCE:** Once a disaster recovery plan or COOP is established, regular maintenance of the plan helps ensure viability.

Physical and Virtual Server Options

Although data centers are clearly going virtual, on average only 80 percent of a data center can be virtualized, so solutions are still needed for the replication and failover of the physical servers. Physical server arrays have several options for recovery:

- **SERVERS DEPLOYED WITH LOCAL STORAGE OR DIRECT-ATTACHED DISK:** Recovery options include restoration from tape media to similar hardware, restoration from tape media to dissimilar hardware, host-based replication and physical to virtual (P2V).
- **SERVERS DEPLOYED WITH A COMBINATION OF LOCAL AND REMOTE STORAGE:** Recovery options include either storage-based replication or geographically dispersed clusters.
- **SERVERS DEPLOYED WITH NO LOCAL STORAGE:** This situation, with both the operating system and data drives stored on remote storage, can utilize all of the previously mentioned options.

Because of their isolation and encapsulation capabilities, virtualized servers can be moved and restored between different physical servers and storage hardware, with no need for any kind of migration. Virtual server environments also have several options for recovery:

- **SERVERS DEPLOYED WITH LOCAL STORAGE OR DIRECT-ATTACHED DISK:** Recovery options include restoration from tape media to any hardware, host-based replication and guest-based replication.
- **SERVERS DEPLOYED WITH A COMBINATION OF LOCAL AND REMOTE STORAGE:** Recovery options include utilizing the previously mentioned options, as well as storage-based replication.
- **SERVERS DEPLOYED WITH NO LOCAL STORAGE:** This situation, with both the operating system and data drives stored on remote storage, can utilize any of the previously mentioned options.

Should You Virtualize?

Server virtualization is now the leading technology used for disaster recovery. Organizations virtualize not only because of its immediate cost savings, but also because of its flexibility.

Data center design can become very simple once all areas (storage, server, desktop, application and network) are virtualized. Starting in the production site, multiple shared storage subsystems can be used with storage virtualization in front of them.

This allows servers to be moved on demand between different storage devices. All servers and desktops can be completely virtualized, which allows all instances to be replicated into the recovery facility and brought online in minutes.

The end-user experience is almost identical when accessing applications in either site. In many instances, users can be redirected to the recovery site automatically.

Virtualization removes hardware dependencies. This enables completely different servers and storage subsystems to be used in the recovery site. And this allows organizations to reuse existing hardware for their recovery sites.

Client Access

Many organizations put a tremendous amount of time and effort into developing a disaster recovery plan but overlook developing a client access plan. With little or no strategy as to how end users actually connect to the systems in the disaster recovery site, a good plan can quickly be rendered ineffective.

A client access recovery plan should be formed around the applications needed to run the organization. Once these applications

are identified and the server, storage and network infrastructure are replicated, the last piece is how an end user will access those key applications.

Client access is the method used to present applications to end users. The most common form of access is assigning physical desktops and notebook computers to end users. Unfortunately, it proves extremely difficult to duplicate these application delivery environments in a disaster.

An alternative gaining popularity is utilizing thin clients — small, inexpensive devices with no moving parts that run a light operating system and connect to a remote operating system and applications, thereby only sending mouse clicks and keyboard information back and forth.

When preparing your organization for disaster or continuity of operations, it is essential to plan for desktop, notebook and thin client replacement. Depending on the situation, many work staff may lose their smartphones as well. Given our dependence on these mobile devices, a strategy needs to be put in place to replace them as well.

Terminal Services

Once your organization has decided on a client access device, it can decide on a method for delivering client access. Both Citrix Presentation Server and Microsoft Terminal Services produce similar products that can host an end user's desktop as well as their applications. Whether your organization decides to deliver a published desktop or a published application is completely dependent on the user's needs.

There are several methods for accessing the published application. For example, an end user can access a published application using a browser on a home computer. A client can also be loaded directly onto the operating system so that application icons can be readily available on the actual desktop and only a single click away.

Server virtualization is now in widespread use. As a result, using the same technology to host desktops is quickly becoming the norm. Virtual desktops involve an end user accessing a desktop operating system with a thin or thick client device using remote desktop protocol (RDP).

Power Management

A disaster recovery or backup technology is going to need power. The best way to ensure that your equipment is receiving consistent, clean and reliable power is to back it up with an uninterruptible power supply (UPS).

A UPS is a device that provides backup power via battery to electronic equipment. Not all UPS products are the same. There are different types of UPS solutions that offer varying types of protection and various additional features. Choosing the right UPS can mean the difference between seamless operation and outright system failure during a power emergency.

STANDBY UPS: This is the most basic level of protection. When the UPS detects a drop or spike in voltage or the complete loss of power, it switches over to its internal battery. The standby UPS solutions is designed to protect desktop and workstation systems that require just basic protection for a period of time long enough to safely save open applications and shut down the equipment.

LINE-INTERACTIVE UPS: This setup offers midlevel protection. In addition to the battery backup, the line-interactive UPS also contains a transformer that can regulate the incoming voltage, bringing it up or down to an acceptable range rather than failing over to the battery at the first sign of trouble.

ONLINE OR DOUBLE-CONVERSION UPS: This is recommended for the highest level of protection. This technology takes the battery backup and voltage regulation of the line-interactive UPS and adds power conditioning via rectifiers and inverters that convert the incoming power to its purest form before releasing it out to the load.

When looking for a UPS solution, there are several factors to take into consideration. Most important, you want to determine the amount of power the organization's devices consume, determine how much future expansion the organization anticipates and select the UPS that will support the capacity needed.

Next, consider how much runtime (or battery uptime) you will need. Runtime is the amount of time the UPS will continue to provide backup battery power to your devices. On average, most organizations are looking for 15 to 30 minutes of runtime.

Other Power Considerations

Here are some other important things to consider when deciding on a power solution:

- **REDUNDANCY:** Similar to a RAID set with hard drives, having a mirrored (or 2N) UPS solution will provide the organization with additional availability in the event the primary UPS fails.
- **FORM FACTOR AND PHYSICAL SIZE/SPACE AVAILABILITY:** Determine how much room you have for the UPS unit. There are both rack-mount and freestanding UPS solutions.
- **EXTERNAL BYPASS:** This feature will allow you to disengage power from the UPS while maintaining power to your equipment.
- **POWER DISTRIBUTION:** UPS units can provide output power in two ways: outlets on the back of the UPS or a direct connection to an electrical panel via conduit.
- **SERVICES:** Regular maintenance on the UPS unit is important. UPS manufacturers provide startup services to inspect the wiring, boot up the unit, run diagnostics and ensure the system is functioning properly.

Security and Disaster Recovery

Disaster recovery involves making sure that information assets remain reliable and available if trouble strikes. Security has two primary concerns with respect to disaster recovery planning: minimizing the likelihood of disasters and minimizing their severity.

Disaster Prevention

When an organization adopts disaster prevention as a security goal, there are three basic focuses:

- **ELIMINATE THREATS:** Though not always feasible, many organizations attempt to make themselves less likely targets. For example, they will move critical data centers to areas not plagued by severe weather.
- **ELIMINATE VULNERABILITIES:** Again, while an organization can't eliminate all existing vulnerabilities, it can make an effort to eliminate critical ones.

- **MAKE VULNERABILITIES UNEXPLOITABLE:** This approach interposes a safeguard that prevents a threat from triggering a vulnerability.

Focusing on the various options for preventing disasters is an important part of disaster recovery. Thinking through the prevention strategy is a critical exercise because it provides insight into what combinations of threats and vulnerabilities currently remain uncountered.

Disaster Mitigation

Like disasters, risk has more than one component. The following equation is a simple and common formulation of risk, expressed as an annualized loss expectancy.

RISK = FREQUENCY X IMPACT

Risk is expressed as a figure in dollars per year. That figure represents the product of the number of incidents per year and the average loss expectancy associated with an incident. In the case of disaster-scale incidents, frequency should remain low even though the impact is high.

Although most organizations devote the bulk of their security dollars to minimizing the frequency of incidents, other measures can lessen the impact of incidents when they do occur. User education is an example. If users know how to respond to signs of trouble (such as a worm outbreak), a potentially serious incident can be nipped in the bud before it mutates into a full-fledged disaster.

Likewise, compartmentalization of information and assets helps contain incidents within manageable boundaries instead of allowing them to spread across the enterprise. Investments in fault tolerance, redundancy and capacity are equally investments in system availability.

Disaster Strikes

Within IT, a "disaster" can be many things. By broad definition, a disaster is an adverse, unfortunate and unforeseen event. There are three common types of disasters:

- Natural (fire, flood, wind, earthquake)
- Malicious intent (viruses, burglary, vandalism)
- Accidental (outages of power, telecom, hardware or software systems)

Finally, a proper incident response plan includes the preservation of key information about the incident. Keeping detailed and accurate records of what went wrong doesn't lessen the severity of a disaster, but it can help greatly when an organization goes to recover costs either through insurance claims or litigation.

Manufacturer Options

Disaster recovery and continuity of operations planning cover a wide swath of technologies. Because there is so much that falls into this category, what follows here is a "best of" covering some of the solutions that are indispensable for organizations when setting strategy for recovery and operations continuity.

NETAPP is a manufacturer of storage solutions that can help keep an organization's data flowing and highly available. One of its premiere products is the S550, a storage solution that can scale from 1TB to 12TBs and can combine NAS, iSCSI SAN and Fibre Channel SAN. Utilizing StoreVault software, this solution can back up a complete multi-terabyte Microsoft SQL Server database in seconds — and recovery is just as fast.

EMC is a manufacturer that specializes in storage and content management solutions. One of its top offerings is the CLARiiON AX4, a scaleable network storage product that can facilitate your organization's storage consolidation and provide you with highly available information management.

It can consolidate and share storage for up to 64 servers and is compatible with VMware virtualization software. The AX4 can also mix and match SATA and SAS drives for varying application requirements.

VMWARE is the market leader in virtualization software. VMware ESX Server is virtual infrastructure software that is used by organizations for partitioning, consolidating and managing their systems in mission-critical environments.

This solution provides a highly scalable virtual machine platform with advanced resource management capabilities, which can be managed by the VMware VirtualCenter. This solution will lower the TCO on your organization's computing infrastructure.

MCAFFEE is a software and computer security solutions manufacturer. One of McAfee's leading products is Total Protection. This software suite delivers an integrated security system with built-in, automatic protection against viruses, spyware, hackers and identity thieves.

It also provides e-mail protection against spam, phishing, inappropriate content and viruses. This software is compatible with McAfee SecurityCenter, a web-based management and reporting console with tons of security features.

SYMANTEC specializes in security and backup solutions. Its most well-known product is probably its Ghost software. Symantec Ghost Solution Suite is an imaging, deployment and system management solution.

It facilitates recovery and operations continuity by securing images of your organization's staff computers. In an emergency where access to computers is lost, your IT team will be able to call up operating systems and settings for users' computers and reinstall them on new access devices.

HEWLETT-PACKARD'S forays into disaster recovery and operations continuity revolve around servers, storage and thin client solutions. HP offers the ProLiant DL360 G5 server with two quad-core Xeon processors. This server is optimized for space-constrained installations, has redundant power and fans, and Lights-Out remote management.

HP's StorageWorks 2000 Smart Array family of SAN devices assist in storage consolidation. And HP's Compaq Thin Client t5730, with an AMD processor, high-end graphics, HP Sygate Security Agent and local application support, can facilitate remote access for your users.

WYSE TECHNOLOGY manufactures thin client solutions. One of Wyse's premiere thin client products is the V90L model. This is a midrange thin client with an Eden 800MHz processor that delivers Windows XPe performance; supports dual-video; and has serial, parallel and USB ports. Wyse has partnered with Planar to create the fully integrated ND1750 LCD monitor. This device has a 17" display and is a good fit for virtual desktop computing.

CISCO'S forays into disaster recovery and operations continuity are built around networking solutions. One of its key recovery and operations offerings is the 7942G Unified IP phone. This phone runs over the network and is designed for wideband audio. Its graphic capabilities allow users to take advantage of XML applications.

Another helpful Cisco product is its Unified Communications software. This software helps facilitate the kind of enterprise-wide communication that needs to happen during a disaster situation via its messaging applications.

Making the Case for Your DR Plan

Finding out the true cost of downtime for an organization can be a very difficult process, which is why most organizations outsource their risk analysis to outside consultants. This process can take quite a long time, but its results are invaluable. Once your organization determines the cost of downtime, it will be easier for the IT department to make a case for a disaster recovery plan.

BROCADE is a communications systems manufacturer that offers storage network products. It offers the ServerIron GT CGx2 SSL load-balancing device, which can help organizations keep servers running smoothly. This product has a 2-port Gigabit line module and a WSM6-SSL-1 management module.

The management module's processors perform application switching, traffic management, SSL acceleration and web optimization, as well as dedicated and reliable device management.