

Keeping Your Network Available Through Thick and Thin

The right strategy can make disaster recovery and business continuity succeed in an uncertain world.

Introduction

It's no secret that the 21st century economy is driven by the collective data that resides in servers and systems around the globe. When a disaster occurs or the flow of information is interrupted, private and public companies may find it impossible to conduct essential business.

They may face lost sales, diminished productivity and a litany of regulatory and compliance problems. In a worse-case scenario, they may also endanger public health and safety — or find themselves out of business.

Today, business continuity is a critical concern — particularly for small businesses with limited IT staffing and finite financial resources. The emergence of vast computer networks — often intertwined with partners, customers, employees and others — has changed the dynamics of business in a profound way.

There's an expectation that systems will function effectively and that data will be available almost instantly. Recovery time objectives (RTO) and recovery point objectives (RPO) continue to shrink while the cost of maintaining business continuity system grows.

For IT managers at small businesses, developing an effective business continuity and disaster recovery strategy is essential. Small business must focus on a wide range of factors, including storage and backup systems, mirroring and clustering, ensuring adequate bandwidth, maintaining uninterrupted power, sustaining remote access via mobile devices, overseeing software systems and engaging in adequate planning, including business impact assessment. Only then is it possible to keep information flowing — even during the most adverse conditions.



Disaster Recovery: Experts agree there's a solid understanding of the need for disaster recovery — namely the ability to make some or all data accessible again after a disaster. But they say IT must also begin to focus on the more difficult task of building business continuity.

Business Continuity: Business continuity becomes necessary when not only data is lost, but the underlying application is lost as well. Business continuity is one step beyond disaster recovery. You've backed up not only the directory of data plus images but also the application itself. It's another mirrored image of the primary system.

Data Lost and Found

In an increasingly interconnected world, business continuity and disaster recovery have emerged as key factors in determining whether a business flourishes or flounders. Large companies can lose upwards of \$1 million an hour when systems and data aren't available; small companies can suffer fatal consequences if there's any interruption in the flow of goods or a handful of key customers take their business elsewhere.

Remarkably, only 38 percent of small businesses in the U.S. have any type of emergency preparedness plan, according to the National Federation of Independent Businesses, a small-business advocacy group in Nashville, Tennessee. The remaining 62 percent deal with a crisis when it arises.

Developing a business continuity and disaster recovery plan involves more than tossing an assortment of hardware and software at potential problems. It's essential to integrate and optimize various devices and, in many cases, engineer redundancies into the overall IT framework.

It's also vital to establish policies and procedures for accessing data and maintaining communication during an outage or disaster. Information availability and an always-on mentality must remain the central focus of any initiative.

Although cataclysmic events — such as earthquakes, floods, fires, pandemics and terrorist attacks — are vital considerations, there's also a growing realization that an organization must plan for mundane threats, such as power failures and network outages. In fact, these events account for the vast majority of all incidents and typically lead to the most severe disruptions.

Addressing business continuity challenges is no small issue. Tight budgets and limited resources mean that small business must deploy resources wisely and achieve maximum return on investment. Understanding business requirements and then substantiating them through the right systems is vital.

Unfortunately, business decision makers often put business continuity on a back burner as more pressing problems — or the financial prospects of the organization — take priority. In fact, only about 6 percent of IT budgets are devoted to disaster recovery and business continuity.

Make no mistake, under-funded business continuity and disaster recovery systems are a serious concern. All too often, organizations that cut corners or lack the right IT infrastructure and business policies create substantial risks.

In reality, business continuity operates on a de facto pass-fail system. If, in an emergency, the environment functions correctly, the organization achieves desirable results and success.

If it doesn't meet recovery time and recovery point objectives, the business continuity program fails. Unfortunately, it's only after an incident occurs — and systems do not meet expectations — that business leaders understand the urgency of proper planning.

A successful initiative involves several pieces: excellent technology; the ability to thoroughly test systems; management sponsorship; the right infrastructure and facilities; well-trained employees able to deal with change; the ability to set customer and partner expectations; and ongoing monitoring and enterprise support.

Overcoming these obstacles requires continuous investments, executive buy in and support, and a framework for building well-defined processes. Ultimately, technology only substantiates the business needs and puts the business continuity plan into action.

Devising a Plan

Industry research shows that nearly one-third of businesses suffering a catastrophic event brought on by a prolonged power outage or disaster never reopen their doors and numerous others fail within two years. Often, the greatest losses aren't the result of the immediate event, but ongoing lapses during the recovery phase.

Executives fail to communicate, critical files go missing and customers lose their patience and wind up taking their business elsewhere. Later, sanctions and regulatory/compliance problems may add to the headaches — and the hangover.

The first step in building a reliable architecture is to understand what's required and how to design various systems. This process involves mapping data throughout the business and determining which technologies and solutions fit the organization's requirements.

Understanding RTO and RPO objectives is the foundation on which an effective business continuity solution is built. A few years ago, an organization might establish a two- or three-day window for getting systems back online; today the time frame is usually a few hours.

However, shrinking time windows isn't the only consideration. It's also crucial to identify the point at which systems must be restored — based on data value, cost and business requirements. An organization must ultimately classify data and slot it into tiers based on RTO, RPO and total cost of ownership (TCO).

To be sure, every organization establishes its unique data footprint through RTOs and RPOs. A Web site, e-commerce system or customer database might require instant failover capability while a four-hour lapse in e-mail or multimedia content might prove inconvenient but not fatal.

Not surprisingly, different firms in different industries have drastically different needs. For example, a high-volume online store, bringing in \$25,000 per hour, would require robust failover measures should a single server fail in its infrastructure.

On the other hand, a small computer manufacturer, one that custom configures systems, might get by for a day without its accounts payable system, accounts receivable system and probably its procurement system.

The one constant is that a smaller recovery window puts greater pressure on IT to ensure optimal performance at an acceptable cost. As a result, business and IT leaders must confront a number of issues, including whether to create a standby environment using mirroring or clustering, replicate data within an internal or external data center and whether to replicate data at the application, database or storage level.

Addressing the Details

A business impact assessment can take anywhere from days to weeks, depending on the size of the company and the complexity of its data infrastructure. The team should consist of more than IT managers; it's essential to assemble a cross-functional group of staff who can provide visibility into business needs, risks and long-term costs.

A company must also develop some type of process to rank the importance and urgency of various types of data — customer records, e-mail, financial data, enterprise databases and

more — so that it's possible to create tiers and deploy appropriate and cost-effective solutions.

The business impact assessment team oversees the process of evaluating and prioritizing systems and data; assigning responsibilities; identifying internal and external tools; technologies and solutions; weighing and categorizing potential risks, threats and business impacts; developing crisis communication systems, including phone trees and other emergency notifications systems; informing various departments and groups about the systems that the organization will put into place; and managing interfaces and other administrative systems and tasks.

The end result should be a clearly articulated plan that describes all the various steps — from implementation to testing; drills to system updates — required to build an effective business continuity and disaster recovery model.

The plan should also cover procedures and protocols for managing tasks during a prolonged emergency, and involve a diverse array of challenges, such as temporarily moving facilities, relocating equipment and setting up temporary computer networks.

For some events, such as a pandemic, the plan might also outline telecommuting and remote work options and establish policies for providing equipment to employees — so that they have access to personal computers or PDAs (personal digital assistant), Internet service and other essential business services from home or a remote location. The plan must also specify how the organization will return to normal operations.

This business continuity plan is designed to provide guidance to an emergency response team and executives who oversee operations during an outage, disaster or other interruption. A clear plan that's distributed to key management staff as well as team members makes it possible to move quickly and with tactical precision if an interruption or disaster takes place. It can determine whether a business manages the process deftly or sinks under the weight of poor and uninformed decisions.

Quick Recovery

Here's a checklist of steps that can help an organization manage data business continuity and disaster recovery issues effectively:

1. Analyze requirements and applications. The first step in devising an effective strategy is to understand the organization's business needs. A cross-functional business impact assessment team should examine and rank various types of data so that it's possible to establish the right recovery time objectives and recovery point objectives and understand how cost issues factor into the equation.
2. Match systems to data requirements. When an organization establishes clear recovery time objectives (RTO) and recovery point objectives (RPO), it's possible to match hardware and software with business processes and data recovery needs. In some cases, it's important to have systems back online within minutes; in other cases, hours or days will suffice. A well-designed system is also the key to managing costs and achieving solid ROI.
3. Budget adequately. Under-funded initiatives aren't likely to provide the level of protection that's desired...or required. A business must quantify risks and understand total cost of ownership (TCO) as it relates to business continuity.
4. Develop a response plan. When an incident takes place, it's essential that IT administrators and employees have a clear understanding of how to handle the situation and manage work with minimal disruption. An effective plan spells out tasks, responsibilities and roles — and it covers an array of situations that may demand entirely different responses. It's not enough to ensure that machines are turned on and operating; an organization must establish how employees will access systems and data during an outage or emergency.
5. Designate a recovery team. The sheer unpredictability of a disaster requires an organization to establish a team to lead employees through the recovery process. Armed with phone trees, mobile technology and a clear response plan, these individuals are able to make quick decisions and change course on the fly.
6. Revisit business continuity often. Because business conditions, processes and technology constantly change, it's vital to re-examine business continuity and update a plan on a regular basis. An organization must also test systems periodically — every quarter or at least once a year — to ensure that it hasn't overlooked anything and that the plan works. Finally, it's crucial to update and upgrade systems periodically to fit changing requirements.

Thinking Strategically

One way that many businesses address business continuity and disaster planning is through mirroring and clustering.

Server Clustering: Combining two or more servers — appearing as virtual unified computing resources — to make it possible to operate numerous servers while connecting all of them to a common, mass storage device, usually contained in a network attached storage (NAS) or storage area network (SAN) system. This approach allows an organization to combine servers along with a redundant array of independent disks (RAID) in order to boost overall computing power and system efficiency.

This means that if one server fails, another takes over instantly. Because an application or data resides on multiple servers or storage devices, there's no need to recover data from a backup system when a failure takes place. All the servers in a cluster communicate with one another through a process called polling.

Since the operating system no longer deals with separate servers — it views them as one logical system and constantly polls all the servers in the cluster to determine whether they are operational — the process takes place quickly and transparently. Today, all major operating systems support clustering and it's possible to connect a wide range of devices, including those using a Small Computer System Interface (SCSI) and Fibre Channel.

In the past, organizations used clustering primarily on a local level or limited basis. However, more sophisticated software and systems (such as Symantec's Veritas Cluster Server, which links multiple independent high-availability clusters at multiple sites into a single, highly available disaster recovery framework) have altered the landscape. Increasingly sophisticated software makes it possible to use clustering on a widespread basis — and under multiple environments and operating systems.

Server Mirroring: An important component in effective clustering, mirroring relies on duplicate servers within the same network and typically uses load balancing software to manage resources. While one server handles transactions and processes tasks, another receives duplicate data.

As a result, when a primary server fails, a second device takes over — whether it's located within the same data center, at a separate facility across town or at a remote location operated by the enterprise or under contract with a managed services provider. Hewlett-Packard and IBM are among the leaders in mirroring technology.

While mirroring provides enormous advantages, and is widely used to manage systems that require instantaneous failover capabilities, the downside is that it essentially doubles the need for server space and, in some instances, increases processing demands. This has prompted organizations to use server virtualization in conjunction

with mirroring and other replication techniques. If one virtual system fails, another one takes over instantly and performs the same tasks.

Virtualization: This technology allows multiple computers, operating systems and applications to run side by side within the same physical server. By partitioning a server into several virtual machines that run different operating systems and applications, it's possible to boost resource utilization, improve flexibility and reduce costs.

Still another consideration is the location of a data center that's used for backing up or replicating data. For years, organizations commonly operated two or more data centers within a single geographic region. However, events such as Sept. 11 and Hurricane Katrina have made it clear that the close proximity of data centers can lead to serious problems.

Today, many businesses have turned to inter-regional data centers and instant failover capabilities. This makes it possible to cope with most incidents at a local or regional level but step beyond these facilities when a regional disruption occurs.

Remote Access (to storage): A growing number of organizations rely on mobile remote access to manage various storage systems. Not only does remote access by computer, PDA or smart phone provide access to system status and current network conditions, it allows an IT administrator to make changes as needed — based on operational and security needs. Of course, it's vital to determine who requires remote access features and what specific permissions they need.

All Systems Go

One goal of business continuity is to keep systems running and data available during a blackout or any sort of disaster. But if a server room goes down or equipment is damaged or lost, it's essential to have a backup of the data available.

Once systems are back online, a small business can restore the data and continue operations without major side effects or trauma. Yet, because of cost and performance issues, there's no single approach to backing up.

These days, disaster recovery and business continuity systems include tape backups, tape emulation, disk-based systems such as direct attached storage (DAS), NAS and SAN, and a variety of hybrid systems that use an assortment of tools and technologies to provide an appropriate solution. Here are some of the key components:

Tape Backups: These devices, which use magnetic tape media, have been around since the early 1950s. They're reliable, they're relatively inexpensive and they offer a simple and straightforward way to store data. Additionally, most systems are able to compress

data by a 2:1 ratio. As a result, tape is widely used by many small businesses.

Today, systems range from directly attached devices that back up a single PC to sophisticated tape libraries using autoloaders and vast tape libraries. It's possible to use an array of methods to connect tape drives to systems, including SCSI, Fibre Channel, parallel port, Integrated Drive Electronics (IDE), Universal Serial Bus (USB), FireWire, Enterprise Systems Connection (ESCON) and Fiber Connectivity (FICON).

The tradeoff is that tape is relatively slow because it uses a linear seek method. Thus, it is far better suited to archiving data than backing up files and applications that require immediate access. Numerous vendors — including HP Overland Storage, Tandberg Data and Quantum — offer tape solutions, including more sophisticated autoloader and library systems.

For example, Quantum's CL 400H external tape backup unit uses advanced verification methods to ensure that all data is backed up without errors; it offers advanced cooling; relies on ceramic tape heads to extend the life of media; and a multiple-speed sensor that matches the physical tape speed to the incoming host data rate.

Meanwhile, Tandberg Data's Exabyte VXA-320 Packet Tape Drive Internal offers an automated approach for a single server or PC. It provides 320 gigabytes of storage capacity using full compression and offers a scalable and fast solution; it is able to back up 86GB per hour.

Direct Attached Storage (DAS): The appeal of DAS is that it is possible to directly attach the device to a server or workstation, without a storage network in place. These storage systems have become increasingly popular in recent years because they allow organizations to differentiate SAN and NAS storage from non-networked storage.

Using SCSI, Serial-Attached SCSI (SAS) and Fibre Channel protocols, DAS offers high data bandwidth while extending storage capacity for servers. These systems rely on a Host Bus Adapter (HBA) to provide the interface for the server or workstation.

They offer a high level of fault tolerance, controller redundancy, cooling redundancy and storage fault tolerance. In addition, more sophisticated DAS devices use embedded controllers to off-load management tasks, thus lowering overall costs. They also incorporate basic data sharing.

Although DAS is a fast and effective tool for managing backups and business continuity, its primary disadvantage is that data contained on a device isn't easily shared. Because DAS systems do not normally interconnect to other servers and workstations, it's important to use them for specific situations and applications.

Network Attached Storage (NAS):

What makes a NAS device so powerful is that it connects to the network rather than individual computers or servers. This makes it possible to store disparate forms of data on a common device — even when using different hardware and operating systems, including Windows, Linux, Mac OS X and versions of UNIX.

What's more, NAS units can use more than one hard drive and operate within a redundant array of independent drives (RAID) array, which makes it easy to create secondary backups. If one drive fails, another one holding the same data is available. NAS devices are also easy to install, manage and reconfigure. They require minimal maintenance or upkeep and they're highly scalable.

Once installed, NAS devices become a powerful repository for data across an enterprise. These systems boost availability by making data accessible — even if a server is down.

The disadvantage to NAS is that it offers minimal functionality (most use a scaled-down operating system) and performance can bog down under the weight of too many users or too much demand for its processing power. NAS vendors include: Adaptec Snap Servers, Buffalo, HP StorageWorks, Linksys, SimpleTech and new to market NETGEAR's ReadyNAS.

For instance, Buffalo's LinkStation Pro LS-500GL offers an array of features, including 500GB of storage, Active Directory support, driverless

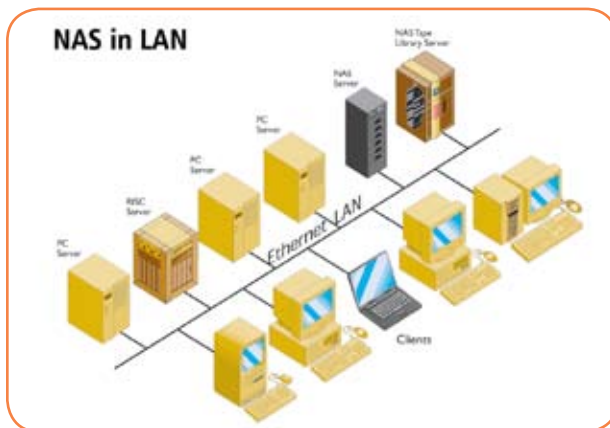
Disaster Recovery — Business Continuity

Main Points to Consider

- Redundant systems — spare hardware that can be set up in the event of a failure
- Backup power — uninterruptible power supply (UPS) hardware in the event of a power outage
- Redundant Internet connections — used for load balancing, or in the event of an outage, will still provide some level of Internet connection
- Hot-spare servers — often used to load-balance servers and provide services in the event of a hardware failure
- Offsite storage of backup media — used to provide a safe location for backup media in the event of a fire or other disaster
- Copies of software needed for installation — in the event of a disaster, install media is necessary to get systems up and running — every quarter or at least once a year — to ensure that it hasn't overlooked anything and that the plan works. Finally, it's crucial to update and upgrade systems periodically to fit changing requirements.

installation, built-in backup software and the ability to add additional drives via a built-in USB port.

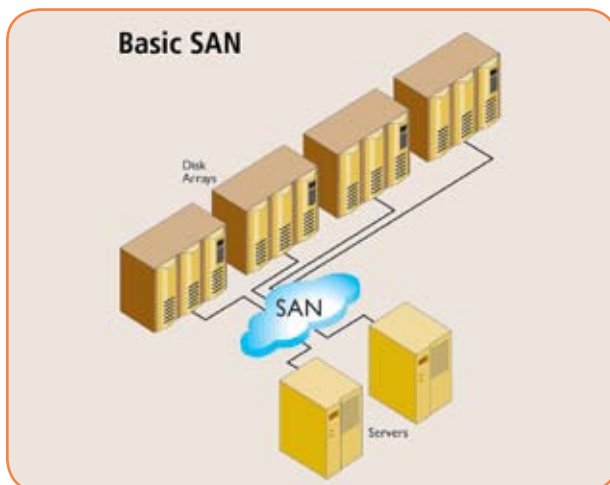
Prices for NAS devices have dropped markedly in recent years. They're now an extremely popular solution for small businesses, including individuals operating from a home office.



Storage Area Network (SAN): Although SANs are typically a tool for larger organizations, some smaller businesses are also turning to these storage systems. A SAN manages disk arrays, tape libraries, DVD and CD disk arrays and other systems, and makes them available to servers across a network.

Simply put, it creates a pool of storage devices that are linked directly to the network rather than a sever. It's a powerful solution that offers unsurpassed flexibility and scalability. For instance, an IT administrator can reconfigure a SAN device from one physical server to another without ever moving or reconnecting anything.

Another strength of SANs is that they utilize storage space in a highly efficient way. That's because SANs allow multiple servers to share the same storage space — and it's possible to use a secondary array that's located in a remote location. After Sept. 11, SAN adoption spiked and its use continues to grow.



Putting a Strategy to Work

Because no two businesses are alike, it's critical to design a solution that offers maximum protection while minimizing time, money and administrative responsibilities. Naturally, a micro-business (typically less than 10 employees) has significantly different requirements than a firm with 100 employees.

For the smallest companies, an external hard drive or NAS device may offer an effective and inexpensive way to replicate data onsite (though it is still necessary to backup data offsite, typically through the use of an online backup service).

Of course, backup and recovery processes become more demanding and sophisticated as a business grows. It may be necessary to step beyond conventional tape-based backups or use a more complex approach than NAS. Tools and technologies include:

Disk-to-disk systems: These devices allow synthetic backups — which typically involve a full backup followed by incremental backups. This approach uses fewer resources and less bandwidth than tape-based methods. Moreover, disks — while susceptible to errors and crashes — are more resilient and less prone to wear and tear that eventually forces an organization to replace tape storage. Finally, if a single cartridge fails during a restore operation, IT can spend hours getting things back on track.

Unlike tape, files stored on disk are accessible instantly, even during a full synthetic backup. EMC, Exabyte, HP, Quantum and Symantec are among the leading providers of disk-based backup and recovery systems.

Disk-to-disk-to tape (D2D2T): This method transfers data from one disk-based system to another on an hourly, daily or weekly basis but eventually transfers the data to a tape system for offsite backup. D2D2T ensures that recent data is accessible and it keeps data sets smaller — thus speeding transfers in either direction. It allows an organization to use dynamic caching and bring information back in near-real time.

Tape emulation: This approach uses hardware or software to make a disk-based system appear like a tape library to backup software. An advantage of this approach is that it's usually "seamless" to deploy and use because it doesn't require any changes to underlying processes. In most cases, tape emulation is easier and less expensive to manage while offering performance improvements over straight backup to disk. That's because it avoids the disk fragmentation that usually occurs in disk-based environments. Another advantage to tape emulation is that it speeds access to production data because it can complete backups more quickly.

Point-in-time copy: Small businesses with extremely tight backup windows and in need of specific restore points benefit

from point-in-time copy. That's because these systems generate a snapshot or mirror of data, which an organization can split up and store on disks as needed. An index keeps track of where the protected data exists on all the various storage arrays. This makes it possible for an IT administrator to roll back a system to a specific point in time — and break recovery points down to four- or six-hour intervals.

Replication-based backup: It also creates a snapshot of an environment but handles backups on an ongoing basis — either synchronously or asynchronously among storage arrays — rather than transferring to tape once or twice a day. This technique drastically reduces the need for tapes and slashes bandwidth and processing requirements. It also provides powerful recovery point and recovery time capabilities, and allows a business to strengthen its disaster recovery strategy by storing the replicated data at a remote site.

Many organizations, particularly those with more complex requirements, rely on a mix of backup and restore methods to manage data. Another approach that is gaining momentum — and can include virtually any backup and availability technology — is colocation.

It allows a company to store data offsite in a facility that is shared with other organizations. Typically, this shared data center offers an advantage of providing state-of-the-art facilities, including storage equipment, telecommunications, etc. — at a cost that's reasonable for a small business.

For many firms, it's a way to adopt a big business approach to backup, disaster avoidance and disaster recovery without the capital outlay. Yet, any foray into colocation must include attention to service level agreements (SLA) in order to ensure that the contract services meet an SMB's specific requirements.

Tiered Storage Strategies

As organizations accumulate more and more data — both structured and unstructured — the need to use the right storage and backup strategies grows. In many cases, it's necessary to map out a method for managing data based on its value and importance at a specific point in time. As a result, tiered storage lands in the spotlight. Using RTOs and RPOs, it offers a way to build a more complete business continuity model.

Tiered storage serves as an umbrella for a number of strategies, including:

Hierarchical Storage Management (HSM): This data management solution moves data between high-cost and high-performance devices and low-cost, lower performance storage media. Vendors in the space include: (Disk) EMC, Emulex, EqualLogic, HP, IBM, LeftHand Networks, Overland and QLogic;

(Tape): ADIC, EMC, HP, IBM, Overland and Quantum; and (Software): IBM and Symantec.

Information Lifecycle Management (ILM): Through the use of technology, policies and practices, it's possible to manage business information in a cost-effective and strategic way throughout its lifecycle — thus streamlining and simplifying business continuity strategy. Vendors in this space include: EMC, HP, Quantum and Symantec.

Continuous Data Protection (CDP): Sometimes referred to as CDP, this approach saves a copy of every change made to data. As a result, a system administrator or user can restore data to a desired RTO or RPO. Solutions providers and products include: EMC RecoverPoint CDP, Microsoft System Center Data Protection Manager and Symantec Backup Exec 11d.

Ultimately, tiered storage may include a mix of tape, optical storage, disk arrays, storage area networks (SAN) and a variety of other systems. It is typically used in conjunction with storage resource management (SRM) software, which helps gauge the value of data, define RTO and RPO objectives, and determine the ideal storage medium.

The most powerful tiered solutions boost the effective capacity of disk bandwidth over a wide area network. Moreover, they are able to accommodate up to 50 times more backup data than conventional systems and use a fast recovery disk — thus increasing available recovery points and improving an organization's ability to restore data to the most ideal point.

Power Plays

One of the most basic but overlooked aspects of business continuity is maintaining electrical power during a blackout or disaster. Small businesses with the most urgent requirements may choose to install a power generator for a crucial data center.

An underlying theme for small firms is that power — its availability and protection — is a vital consideration when building business continuity plans. This is pushing businesses to assign a more strategic value to power technology.

It's wise to use uninterrupted power supply (UPS) devices to keep specific servers and desktop systems running when the power fails. UPS devices typically offer three-to-15 minutes of battery life — thus allowing a computer user to save data and shut the system off normally. There are three main types of UPS systems:

- **Standby or Offline UPS:** It powers IT equipment directly from the Alternating Current (AC) outlet. If a power disturbance occurs, whether it's a blackout, surge or sag, a standby UPS will switch to battery power to protect the technology. A standby UPS is the

BUFFALO

TeraStation® Pro II NAS 1.0 TB

Combining advanced active directory support, fault tolerant data solutions, robust file security and Gigabit Ethernet networking, TeraStation® Pro allows users to deploy a simple, cost-effective data server to their office in minutes without cutting corners on features or expandability.

- Memeo™ Easy Backup software included
- Quick-swap hard drive tray via the front panel for easier maintenance



\$856.99 CDW 1178837

2TB \$1414.99 CDW 1170699



Tandberg Data VXA-320 PacketLoader 1x10

10-cartridge capacity

- Storage capacity: up to 1.6TB native, 3.2TB compressed¹
- Data transfer rate: up to 43GBph native, 86GBph compressed¹
- Bar code reader and rack kit included
- Remote management standard allows monitoring from anywhere in the world
- Allows room to grow with either 40/80, 80/160 or 160/320GB cartridges
- Disaster tested — VXA Packet technology offers reliable tape restoration



\$1899.99 CDW 830263



Symantec Backup Exec™ System Recovery 7.0

New Version

Download free trialware at CDW.com/backupexec

- Captures a recovery point of the entire live Windows® system
- Quickly restores individual Microsoft® Exchange e-mails, folders and mailboxes
- Integrates with Google™ Desktop as well as Backup Exec Retrieve for simple, end-user file recovery that does not require IT intervention



Full version With one-year essential support² \$529.99 CDW 1210359



Exabyte® X23 160GB/320GB Tape Cartridge

Exabyte® X23 offers the scalability of three different cartridge capacities, compatibility with the next-generation drive and the ability to reliably restore data under the most extreme conditions.

\$66.99 CDW 705846

simplest, most affordable UPS and is best for inexpensive or non-critical computers.

- **Line Interactive or Automatic Voltage Regulation (AVR) UPS:** When an overvoltage or undervoltage occurs, a line-interactive UPS corrects the strength of the voltage without the device switching over to battery power. It's a step up from a standby UPS, which automatically switches to battery power for voltage problems. This UPS increases battery life as a result.
- **Double Conversion Online UPS:** This topology provides the most effective power protection and battery backup available and is built for highly critical IT equipment, such as servers and networking gear. It takes the incoming power, converts the AC power to Direct Current (DC), then reconverts it to AC, so it filters out problems, such as electrical line noise, and provides clean, perfect power to IT equipment.
- This UPS is designed so the incoming power flows through the battery, which then powers the IT equipment. If there's an outage, the battery continues to power the equipment until it is drained. With other UPSs, there is a short interruption in service as the device switches from incoming power to the battery.

Manufacturers of UPS hardware and software include: APS, Belkin, Eaton, Liebert and Tripp Lite.

Although UPS systems can provide up to several hours of battery backup, they are not designed to keep a business fully operational during a prolonged power failure; that usually requires a backup generator.

In data center-scale requirements, you need to think about getting off batteries quickly and shift to a generator for your power supply. You also need the generator to run your cooling and air conditioning, which can't run off the battery.

And you can't run without cooling for more than an hour — or even five minutes, if you've got blade servers or other dense racks — before you get hot spots that damage or bring down equipment.

Conclusion

The right strategy and systems can help an organization create effective and powerful disaster-recovery, business-continuity solutions. However, the diversity of data and the complexity of today's hardware and software systems requires a well thought out plan, the right mix of devices and tightly defined policies and procedures.

Small businesses that establish a solid foundation avoid costly downtime and, in the end, achieve a competitive advantage. Make no mistake, disaster recovery and business continuity planning are no longer an option. They are an essential ingredient in operating a successful business.

Both require ongoing attention and a commitment to taking data protection and systems availability to a higher level. Only then can a small business feel confident in its ability to weather any storm.

¹Assumes 2:1 compression

²Essential support includes 24 x 7 technical phone support and upgrade insurance; call your CDW account manager for details

