Business Continuity and Disaster Recovery

A comprehensive business continuity and disaster recovery plan can protect your company from all types of disruptions.

TABLE OF CONTENTS

Executive Summary

A Business Continuity (BC) and Disaster Recovery (DR) plan requires an investment of time and resources. Often, however, while looking for the greatest ROI, IT management may put off business continuity until disaster strikes. This can be a critical mistake.

According to the Symantec 2008 State of the Data Center Report, a survey of 1,600 data center managers released in January, only 35 percent of respondents reported their disaster recovery plan to be above average. At the same time, 27 percent said their plan needed work and 9 percent reported it to be informal or undocumented.

Now is an opportune time to consider the planning, tools and technologies that enable the continuance of operations and reduction in downtime, following a disruption. Cost reducing software, like virtualization, coupled with price reductions in hardware, make implementation easier on strained budgets.

Best of all, if the worst-case scenario becomes front-page news, your business will have a functional and comprehensive business continuity plan. And it will also be prepared with the technology to make it work.

Business Continuity: Tools, Reasons and Reality

Business Continuity and Disaster Recovery Defined

Disaster recovery is the process of making some or all stored data available following a disruptive event. The event might be something massive — like an earthquake, a hurricane or the terrorist attack. However, typically it's something on a smaller scale like a computer virus, power outage, flood, fire or even human error.

Business continuity is considered more of an umbrella term that involves backing up the data directly along with the accompanying application, thereby allowing the business to get back up and running with minimal delay. Business continuity planning suggests a more comprehensive approach to staying in business and continuing to generate revenue.

Plan Components

When it comes to BC/DR planning, certain protocols must be in place. Every good plan employs certain technologies and methodologies to limit the disruptiveness of an outage.

There are studies that show that having the right processes in place can prevent a good 50-to-60 percent of the issues that may crop up following a disruption. These policies and procedures include:

- **BACKUP** — Copying data to a secondary source is essential in today's business climate.
- **ARCHIVING** — This systematic approach to storing and managing e-mail and files meets retention policy needs and e-discovery requirements.
- **OFFSITE STORAGE** — For disaster recovery as well as compliance purposes, it is important to store a copy of your data at another location, preferably outside the city or state your data center resides in.
- **HIGH AVAILABILITY (HA)** — This refers to a strategy which allows for 99.999 percent accessibility of mission-critical systems.
- **VIRTUALIZATION** — Not just used for consolidation and cost reduction, it also allows for quick failover capability in systems to dissimilar hardware.

Business Continuity Objectives

IT managers may ask, "What should my BC/DR objectives look like?" One global manufacturing company used the following criteria:

- Restore mainframes with vital data at a backup site within four-to-six days of disruption
- Obtain a mobile Public Branch Exchange (PBX) unit with 3,000 telephones within two days
- Recover the company's 1,000-plus LANs in order of business need
- Set up a temporary call center for 100 agents at a nearby training facility

Decreasing Cost of BC/DR

The good news is that companies are seeing a decrease in costs for implementing BC/DR planning. Some of the cost reduction is due to the fact that the price for storage has decreased.

From 2008 through 2013, the tech analyst firm IDC is assuming a 30 percent annual decline in the cost per Gigabyte (GB) of external storage. This is seen as a significant factor in reducing data center costs.

Still, the major BC/DR savings has come because of virtualization. It allows operating system(s), application(s) and data to be encapsulated in a set of files. These files can then be transferred to a host in the DR site, regardless of hardware type, offering added convenience and affordability.

The Urgency of Business Continuity

The demands placed upon a firm's information systems are significant. These days, internal and external parties expect operations, services and technologies to be available 24x7 with no exceptions and no excuses.

Nearly every aspect of today's business is expected to be available continuously without interruption. When disaster strikes — whether a natural disaster or technological failure — customers still look for products and services to be available. If they can't find them at your firm, they may move to your competitor.

The Annual Cost of Downtime:

Frequency x Duration x Hourly Cost = Lost Profits

For example, if there were 90 branch outages in an average year each lasting an average of one-and-a-half hours and costing $300/hour, then the cost of branch outages for a year would be in the neighborhood of $40,500. Expressed as an equation:

90 outages x 1.5 hours x $300/hour = $40,500

Source: Iron Mountain

Consequences of Downtime/Outage

Businesses need to place a high value on being prepared for disasters of any kind. The practical ramifications of failing to do so can be very high indeed. These can include:

- **STAYING IN BUSINESS** — Depending upon the source noted, anywhere from 25-to-40 percent of businesses never reopen following a major disaster.
- **LOSS OF CUSTOMERS** — Organizations now span the globe and customers expect 24x7 service.
- **TARNISHED REPUTATION** — A good reputation can be completely erased with just one significant disruption.
- **LEGAL AND GOVERNMENT REGULATIONS** — Compliance can have a major affect on firms that are not diligent about protecting customer data and maintaining business continuity.
- **STAFF CONFIDENCE AND EFFECTIVENESS** — When services or technologies become unavailable, users may suffer productivity losses.
- **COST** — The loss of a single mission-critical service, such as e-mail or order processing, can cost some businesses millions of dollars in direct costs.

Even if firms do have a plan in place, they can still face problems. Often that plan doesn't reflect real-world costs.

Perhaps an organization's management knows a business continuity plan is needed — even required. However, because they believe the probability of a disaster actually occurring is very low, the budget for the disaster plan is woefully under what the costs are to implement a plan that would keep them running.

There is a cost for effective business continuity. And certainly this cost is worth it compared to the alternative: your organization being unable to function.

Strategic Planning

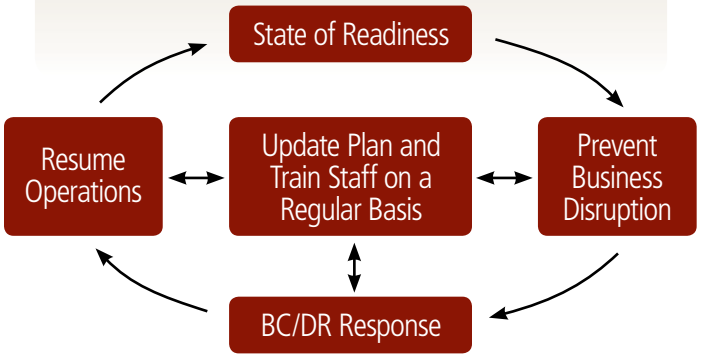
Maintaining disaster preparedness is an ongoing process. It should be considered more of a lifecycle than a process that can be followed end-to-end to completion.

There are five key phases to the business continuity lifecycle:

- **ANALYSIS** — Perhaps the most important component, it is during the Business Impact Analysis (BIA) phase that several examinations will be conducted to determine potential impacts, identify likely threats and develop impact scenarios.
- **SOLUTION DESIGN** — Here the goal is to identify the most cost-effective and technically viable business-continuity solution.
- **IMPLEMENTATION** — This phase includes executing the design elements identified in the solution design phase.
- **TESTING AND ACCEPTANCE** — To be certain that business continuity plans meet the needs of the business, testing is required to ensure process and acceptance.
- **MAINTENANCE** — Once a business continuity plan has been established, regular maintenance of the plan helps to ensure viability. The maintenance phase is the ongoing effort to address technical solution needs, recovery solution needs and organizational changes, and should be repeated often.

In the final analysis, superior preparation and execution allow an enterprise to leverage — and maximize — existing investments. And at the same time, the firm can gain greater functionality and optimize ROI and Total Cost of Ownership (TCO).

Business continuity is not a one-time project. It is a living process, continually updated, fully funded and supported by senior management.



Disaster Recovery: Putting the Moving Parts Together

Determining RPO and RTO

Recovery Point Objective (RPO) and Recovery Time Objective (RTO) are the starting point for mapping costs and benefits. RPO is key for identifying the point at which data is recoverable. For one organization, this might translate into two hours and for another it might mean zero seconds.

RTO, on the other hand, represents the time period required to get systems or applications back in service without a major disruption to the business. The RTO essentially serves as a goal or desired benchmark and is linked to the business processes — and not the actual resources — required to recover missing data.

Developing a successful strategy is no simple task. Business continuity is more than the sum of technology components. It can take many different forms, depending on an organization's RTO and RPO objectives. It touches on many dimensions. It's vital to ask the following:

- What are the risks to the business?
- What's the impact on the business if these risk events take place?
- And then, how does that roll up into costs, both qualitative and quantitative?

Not all services require the same level of protection. So it's key to understand how long of an outage you can tolerate.

Everything ties into RPOs and RTOs. It's the starting point for understanding costs and return on investment.

Rating Application Criticality

The BC/DR process involves reviewing business apps and labeling them as mission critical, business critical or less critical. This is based on the criticality of the application, how quickly those systems need to be recovered and how sensitive the company would be to any data loss from that application.

MISSION-CRITICAL APPLICATIONS: These include applications where the business would be at a complete standstill if the systems were not online. Here's where you would put considerable emphasis on data replication between the production and recovery sites.

BUSINESS-CRITICAL APPLICATIONS: These applications would disrupt business, but not shut it down.

LESS-CRITICAL APPLICATIONS: They don't require 24x7 availability and can be preserved by physical backup to tape and transporting the backup tapes to an offsite location.

Based on these differences, most companies will rely on multiple technologies. It's important to do an impact analysis. Obviously, you don't want to overspend or underspend what's warranted according to the criticality of the systems.

Recovery Site Options

A quick RTO and RPO and fast access to data will mean nothing if your physical location is destroyed and employees cannot work or access that data. Even if your building is intact, basic utilities such as power may be out for an extended period of time in a real disaster.

Therefore, you need backup systems and technology in place that will enable your business to set up shop in a temporary location. It's best to invest in a remote recovery site that mirrors your primary data center. This site could be located in a branch data center, a separate dedicated data center or collocation center.

Companies with multiple locations frequently use their remote data centers as disaster recovery sites. Leveraging existing facilities and infrastructure is a very cost-efficient disaster recovery option.

Note: it's best that your recovery site be located in a different geographic location from your main office or facility. If it's in the same city, or even the same state, it may also be destroyed in a far-reaching disaster like a hurricane.

Also, have a remote access plan so that employees can continue working from home or another location outside the office. One of the biggest concerns for remote access is that information remains secure and in compliance with regulations.

In addition to remote access software, a Virtual Private Network (VPN) is needed so that employees can securely connect to a primary offsite network location. This ensures that staff can communicate with corporate e-mail accounts for an unbroken chain of compliance.

Collocation Sites

Upon completion of a BIA, some firms may find that the benefits of having a separate dedicated data center are worthwhile. These firms feel the advantage of being able to failover in an instant is worth the cost of duplicating most of their production environment.

This kind of setup is somewhat labor intensive and expensive at first. But if built correctly, the labor portion is easily managed or can be contracted out.

On the other hand, many companies find that using a collocation vendor is the optimal way to go. Collocation centers, where companies share data backup space at a highly secure facility offering Uninterrupted Power Supply (UPS) and other network services, can be invaluable should disaster strike.

Here firms lease rack space, cages or rooms. The collocation center also offers fully redundant power, cooling and circuit needs. In addition, space is scalable. If upgrading, you can simply rent more space. And the opposite is true when downsizing.

Firms also save the expense and time of using your own staff to maintain systems. Instead, IT personnel can be used for other projects.

Mirroring, Clustering and Replication

The ability to back up and recover data is an absolutely vital requirement for any kind of disaster recovery and business continuity plan. The overall objective is to increase the paths to data for every application server that needs access, thereby assuring high availability.

If something happens to one of those paths — or the storage device on which that data is stored — there is an alternate way of accessing the data. Failover is the act of transferring that data access from one entity to another. It's a way to protect against hardware and software failures and is most typically a data center activity.

With disk mirroring, at least two drives simultaneously duplicate and store data. Therefore, if one of the disk drive fails, the system can instantly switch to the other without any loss of data or service.

Mirroring provides a high-performance and fault-tolerant solution. It is commonly used in online database systems where it is imperative that data be accessible at all times.

The concept of mirroring is synonymous with the notion of redundancy. That is to say, your remote location "mirrors" that of your local data center. It makes it feasible for an organization to maintain up-to-date copies of data at offsite backup locations.

This allows for uninterrupted access to the data if there is an outage at the local storage. And while it can be asynchronous, mirroring is typically only a synchronous process.

Clustering, on the other hand, refers the use of multiple, interconnected servers. They work together to handle variable workloads or to provide continued operation in the event one fails.

Most commonly, clustering is used for load balancing. It provides for a division of work amongst multiple servers.

This allows for an increase in the work performed, as well as users getting served faster. The simplest way to look at it is that clustering is a way of improving performance and mirroring is as way of improving availability.

Clustering software monitors the health of the database and the servers and makes sure the network and the storage is working properly. Should any of those fail, the failover software or clustering software will start up that application at another site.

Mirroring and clustering are primary ways to achieve replication. Replication comes in a lot of different flavors. Fundamentally, it's creating and maintaining a copy of data at another location. It can be done in server, appliance or storage array.

Synchronous Replication

Used to send copies of data volumes to a secondary storage device, the technology ensures that a remote copy of the data, identical to the primary copy, is created at the time the primary files are updated.

Asynchronous Replication

This technology updates remote storage but with a time lag. Consequently, new writes can be accepted at the primary or local storage site, without having to wait for the secondary or remote site to finish its writes.

BC/DR: Today It's More Cost-Effective

Disk and Tape Technology

Storage is perhaps the most important aspect to disaster recovery. Tape archiving delivers coveted storage space. And it does so with exceptional reliability and without consuming a hefty portion of an IT budget.

Tape has been used for data storage for decades. A data-storage device that reads and writes data onto magnetic tape, tape archiving allows for sequential access to stored information.

Tape is robust, reliable, economical, transportable and suitable for long-term storage. In addition, it boasts a "no-power medium" — using a small amount of power only when the tape is recording or reading data, a welcome benefit to today's "green" data center movement.

As disk technology drops in cost, more and more businesses are opting for hard disk storage or for mirrored disks on a storage network. For short- and medium-term backup and restore needs, disk-based storage has become a highly effective strategy.

Disk storage has two advantages over tape. First, it's a much faster backup method. And while tapes need to be linearly read from the beginning, a hard drive can go directly to the data you need.

Disk-to-Disk-to-Tape (D2D2T) strategies provide two stages of backup. Users copy data regularly from a main disk to a backup disk for speed and accessibility. Then they periodically back up to a tape drive for archival storage.

Deduplication Technology

Disk backup has become more powerful as suppliers have begun pairing it with deduplication technology. This technology stores unique data one time, replacing later instances of identical files or blocks with pointers.

Data deduplication effectively looks for and finds redundancies. It then only transmits unique segments of data.

The data deduplication process allows relatively large backups to be replicated over low bandwidth networks. This helps to facilitate up-to-date copies of data in geographically dispersed locations.

Since backup has a great deal of redundancy, effective deduplication often reduces the disk space needed to store backup by 30-to-40 percent. For many users, that means they can retain backup data on disk for several weeks or months for fast file restores.

By combining deduplication, replication and tape, users can achieve fast backup and restores, disaster-recovery protection and long-term secure retention of data as part of their backup process.

Hierarchical Storage Management

Another approach for long-term retention of archival data is a Hierarchical Storage Management (HSM) solution. It 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.

HSM is policy-based management of file backup and archiving in a way that uses storage devices economically and without the user needing to be aware of when files are being retrieved from backup storage media.

The goal of HSM is to reduce the cost of the storage environment by placing data that is infrequently accessed down the performance curve. While access to data will likely be slower, the storage venue will be less expensive — thereby offering cost efficiencies.

Hierarchical storage management means storing data on the type of media that best meets a number of criteria including:

- The data's criticality to the business
- Your access speed and availability requirements for the data
- The optimal balance between service quality levels and storage media costs

Although HSM can be implemented on a standalone system, it is more frequently used in the distributed network of an enterprise. The hierarchy can also represent various classes of media including RAID, optical storage and tape.

The Role of Virtualization

There are some highly effective business continuity solutions that are empowered via virtualization — especially server virtualization. This is accomplished by combining virtual machines with the replication technology at the heart of disaster recovery.

Virtualization decouples the virtual machine from the underlying infrastructure. Basically, it lets you move a live running virtual machine from one physical server to another. For companies on the leading edge, the next step is virtualizing the disaster recovery site.

Virtualization does two things really well. It allows you to put multiple applications and multiple operating systems on the same physical server. And it allows you to know that they're not going to interfere or interact with each other.

When it comes to disaster recovery, it's a mobility use case. The virtual machine is a file. Therefore, it has the same attributes as a file — it can be easily copied, replicated and moved to a disaster recovery site with dissimilar hardware.

The data and the server files are blocks that can be moved like software. Therefore, moving them from a production site to a recovery site is easy to do over short or long distances. This allows you to eliminate the need to maintain a server at the DR site for each one in your production environment.

Virtualization technology can assist disaster recovery in number of ways including:

- Allowing for dissimilar as well as less hardware at the disaster recovery site
- Facilitating easier failover and recovery
- "Snapshot" technology can be used to capture "point-in-time," making for easier replication
- Replication at the "block level" via Transmission Control Protocol/Internet Protocol (TCP/IP) reduces the time and cost of a replication solution
- Eliminating the need for one-to-one replication of hardware in a disaster-recovery configuration
- Allowing firms to expand the scope of backup to all applications and data and not just those deemed mission critical

Power Protection

Disruptions in power no longer have to bring operations to a halt. Determining how to keep a steady power supply up and running is an essential element of a business continuity plan. One key to keeping the power running is an Uninterruptible Power Supply (UPS).

UPS systems are designed to provide backup power to electronic equipment in the event of a temporary electrical outage. These devices fall into three main categories in roughly ascending order of price and performance.

1. **STANDBY, OR OFFLINE, UPS:** This is the simplest of the devices. When it detects a drop (or a spike) in the electric power coming from the wall outlet, it switches over to its internal battery to power the connected equipment. There's a slight lag in the switchover, but typically not long enough to cause a shutdown or data loss.
2. **LINE-INTERACTIVE UPS:** It adds a transformer that can boost or moderate the incoming voltage to the right level without having to switch over to battery power.
3. **ONLINE UPS:** The unit powers the connected equipment from the internal battery all the time, and uses the incoming AC voltage to keep the battery charged. In the event of a power outage, there's no drop in voltage or switchover to the battery.

   The role of a UPS is to protect equipment from brief outages or spikes. (Most UPS systems also feature surge suppression capabilities.) In the case of an extended power failure, they provide sufficient time to complete tasks in progress and properly shut down systems to prevent data loss or corruption.

Self Generation of Power

For businesses that cannot afford to be without power for any length of time, the only option is self generation. Self generation includes the provisioning of a local generator, its fuel, and necessary switching equipment to handle the organization's equipment load if utility power is discontinued.

If you decide to go in this direction, be sure your backup generator has adequate power for the cooling system. It may seem basic, yet your cooling system is just as critical as your hardware during a power outage. Given the densities of today's computer systems, your data center can heat up quickly when operating without precision cooling.

CDW: A Valued Partner

You need an IT partner you can trust to help maximize performance and minimize costs. This is a firm with in-depth expertise and comprehensive capabilities.

CDW's hosting and managed service offerings are designed to augment your IT strategies at every turn. Whether you seek to enhance disaster recovery, boost availability or more efficiently allocate resources, we can help. From remote hosting to offsite managed data protection, CDW focuses on delivering solutions.

Spectrum of Hosting and Managed-Service Options

Technology comprises the cornerstone of successful business operations. CDW is here to help with a full slate of tech services including:

- Collocation
- Managed Services
- Remote Managed Services
- Disaster Recovery and Business Continuity
- Website Hosting
- Managed Microsoft Exchange
- Managed Cisco Unified Communications
- IT Service Management Consulting

Remote Backup Service

CDW RBS delivers secure, offsite backup/restore as a utility. It offers all the functions, budgetary controls, features and tools of the most sophisticated, dedicated backup systems.

A backup appliance (the RBS node) is installed in your environment. The RBS node connects to the selected servers and workstations, then transfers and encrypts data with your unique key for storage on the RBS node, maintaining the most recent backup of each file locally.

- All data can be encrypted up to AES 256.
- You create and keep your encryption key. CDW, or anyone else, can only decrypt with your key.
- Data is encrypted at the CDW RBS node, before it leaves your network.
- CDW hosts the RBS secure vault in SAS70 Type II audited data centers.

Business Continuity Hosting Services

We design, implement, host and maintain high-availability disaster recovery solutions. Our Enterprise Hosting Centers are designed to be fault-tolerant at all key points of the infrastructure.

HOT-SITE RECOVERY: A popular solution is "hot-site" recovery. This option offers recovery times of less than one hour. We use replication software to replicate the data from the "source" server (located at your location) to the "target" server (a server you own, hosted in one of CDW's data centers).

VIRTUALIZED HOT SERVER: You can elect to subscribe to operating systems hosted in one of our hosting centers and replicate your data there. In a disaster, you move your production load to these virtualized servers and continue production data processing.

Outsourcing to CDW makes it easier and more convenient to create resource efficiencies. We can help you minimize costs, reduce downtime and improve customer satisfaction.

- **CABINET SPACE** — Hosting information in our data center relieves your data center capacity restraints.
- **NETWORK CONNECTIVITY** — We maintain redundant, load-balanced connectivity to multiple tier-one Internet providers.
- **VIRTUALIZED ENVIRONMENT** — You get the security of a dedicated infrastructure with your own virtual firewall, multiple firewall interfaces and security zones, and load balancing.
- **DATA STORAGE AND BACKUP** — Our on-demand storage eliminates investments in underutilized storage. You have complete control of your backup sets and retention periods. And, a copy of the backup data is kept onsite as well as duplicated offsite.

Managed Services

CDW's managed services offerings provide support for your dedicated networks, systems, databases and select applications. Choose advanced monitoring, advanced maintenance and more — at your data center or in our data center.

With our managed services, your organization owns the equipment but we host and manage it. CDW's day-to-day operational management of your network and IT infrastructure enables your staff to focus on mission-ccritical business projects.