Backup Plan:

All You Need To Know About Disaster Recovery

Brought to you by: Colocation America

Safeguarding your digital assets is much easier than you think with a colocation provider. This guide will provide you with the answers you need to formulate an effective disaster recovery plan.

What is Business Continuity?

What does your organization need to do to effectively function during a natural disaster?

Business continuity is a question just as it is a practice. What critical IT resources must you have access to during a service interruption?

What links in the supply chain must be provided to outside vendors for operations to remain un-interrupted?

By making a checklist and defining a clear goal your organization will be able to successfully recover from any un-planned disruption. This "survivalist" mentality is what will carry you through an un-expected event. Business continuity, therefore, is a plan of action.

What is a Disaster Recovery Plan?

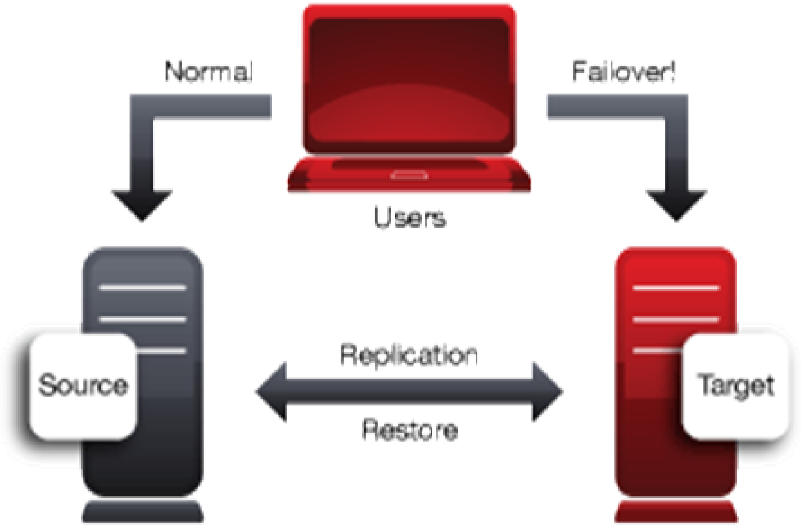
Disaster recovery (DR) is the automatic transfer of data, or other digital assets to a secondary facility. For example, say your server is housed within a data center that gets hit by a hurricane; servers are affected by power outages and the communication line between you and your server is severed momentarily. With a DR plan in place, data backup occurs during a scheduled time each day, week or month. An outage occurs but you are still able to access the back-up data on the remote server; this allows your business to resume normal operations - at least until power is restored to your primary data center.

Protecting The Data That Drives Your Business

Every company, regardless of size needs a disaster recovery plan. The fact is a natural disaster, such as an earthquake or tornado, can quickly cripple a critical IT infrastructure; for companies this means downtown and the inability to access certain online assets that they need to function properly. Unfortunately, many organizations do not have a disaster recovery plan (DR plan) in place, let alone a business continuity plan. The effect this fact has on revenue loss, customer dissatisfaction and/or loss of potential sales, is staggering.

Considering specific factors that may affect or cripple your companies normal day-to-day operations is very important, not to mention a wise investment of capital resources. A simple risk assessment of the IT resources you need to stay up-and-running during a natural disaster is all it takes to formulate an effective "fail-safe" checklist.

The definitions of disaster recovery and business continuity have been simplified to show every IT decision maker that a successful DR plan doesn't' have to be complex, but has to serve a purpose; getting your company back on its feet sooner rather than later.



DR Checklist:

A checklist that provides basic information to employees and steps to follow during a service disruption.

□ Contact information:

Include a list of all pertinent contact numbers from your service provider, emergency services, client and/or vendors as well as employee contact information.

□ Assign Roles:

Everyone should know their role during an emergency. If your primary role is to contact your service provider at the colocation facility make sure you know who that person is, how to reach them as well as what questions to ask.

□ List of Applications:

A list of essential software applications must be complied in order to aid the recovery process, including but not limited to; Application names; technical details; server names; owner contact information;

□ Network Diagram:

depicts the signal path or critical IT infrastructure including switches; network cabling; i/o ports, firewall locations and/or bottleneck routes.

□ Backup Location Address:

Providing the correct address and location of a backup facility is essential, though sometimes overlooked. Never assume employees know the exact route to the disaster recovery location. Provide parking information, contact numbers and any other pertinent info.

□ Supply Resource Numbers:

At times, staff can be tied up at the disaster recovery facility for hours on end. Make sure they have access to essential supplies, whether it is hardware, generator power or something so simple as a pizza delivery number. Sooner or later, they're going to have to replenish supplies. Don't leave your workers hanging during an emergency.

□ Best Practice Protocol:

It is likely you will have to deal with irate customers who cannot access your website (or other online resources). Make sure every employee is up-to-date on best practice protocols. This may include things like what to say and what not to say to a company shareholder or client. Knowing what to say and how to act during an emergency will help maintain company integrity all across the board until you are able to resume normal business operations.

□ Risk Assessment:

identifying any physical or environmental threat that may hinder the disaster recovery process is essential. Proper measures must be taken to avoid potential threats. Doing so will allow employees to focus on DR relief efforts.

Colocation Backup Services:

Colocation backup services are designed to mitigate the loss and risk of losing sensitive business data. Many failsafe’s and protocols are in place in a disaster recovery data center to ensure a maximum level of security.

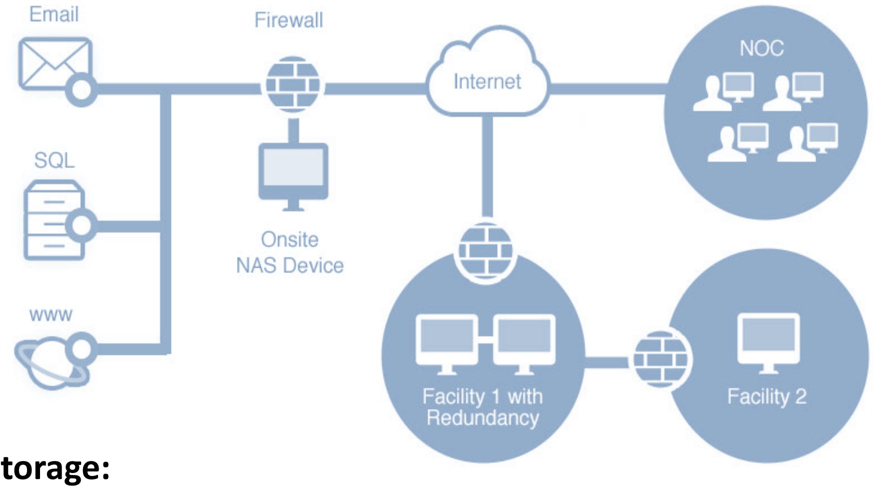
Below is a list of methods commonly used to back up data inside a data center:

Hot Database Backup:

Data backup takes place whenever files are updated or changed. There is less strain on an infrastructure with this data back-up method. A copy of a file is stored in another location and recalled if the primary file is corrupted.

Cold Database Backup:

Continuous or non-stop data backup in a facility is referred to as “cold database backup”.



Online and Offline Storage:

Data stored online is at risk of being tampered with. As a result, many colocation providers offer the option to backup critical data offline - allowing access only to authorized users in times of emergency.

Enterprise Software:

advanced software systems were developed to restore corrupted files, optimize system restore times and eliminate any outside threats to an organization during a disaster.

The Bottom Line:

A successful Disaster recovery plan requires proper testing of procedures beforehand. Business continuity ensures DR (disaster recovery) efforts run smoothly - in such a way that normal business transactions aren't affected and thus remain constant.

Better planning will decrease the risk of organizational failures during times of disaster. Hopefully the business continuity plan your company puts in place will be bulletproof. Even if it's overkill, you will be better off if you prep for the worst.

This PDF was written by James Mulvey on behalf of Colocation America, a leading provider of data center and colocation services. For more information contact James(AT)colocationamerica.com.