

Traditional Backups Vs. Backup and Disaster Recovery and Continuity (BDR-c)



Purpose of backing things up

When you stop and think about it for just a few seconds the question isn't "Do we have good backups?" or "How are we backing things up?" The question is "How do we plan to stay in business if we lose our data or server for any real length of time or forever?" Simply having your data stored on some media in the event of a disk failure or server failure is ok

If you have been in business for 15 or more years think back to how important your data and technology was in 1995. In that year, most of-fice had some kind of computer/s and maybe a Windows NT server but if the data were permanently lost or the server crashed, we could pretty much go back to doing business the "old-fashioned way" for a while until we got back on track. Now in 2011 we live in a very different world. The server/s and data needs to be available all the time from many places no matter what. In 1995 your technology rated at a 1 or 2 on a scale of 5, 5 being absolutely critical. In 2011 your technology is a 6! Sadly, many business owners don't start making their technology a 6 when it comes to supporting it until there is a crisis. Perhaps this is why over 70% of businesses who permanently lose their critical data are out of business within 18 months of the event.



Cybernut Solutions provides outsourced IT support from a wealth of knowledgeable technicians and system administrators certified in their respective fields. We are committed to providing you with technology solutions that help you achieve your business goals by improving productivity, profitability and efficiency across the board. Discover what a strategic IT solution and the support you need to back it up can do for your organization today!

Traditional Backups

Until just a few years ago it was acceptable to have a server with a tape drive in it that ran backups daily and could be used to restore data in the event of data loss. This was in use because until more recently, it was simply the only means to back anything up. Usually, employees were told to save their most important data on the server or network drive (G: drive) for example or else it wasn't being backed up. Later, redirecting users' documents folders became a popular strategy.

Administrators would redirect users' documents folders to a network share on the server and the tape backup would include that folder. To the user, it appeared seamless. The documents folder looked like a local folder but it was really on the server.

Usually once a week a designated employee would take a tape offsite for safe-keeping at home. There are many problems with this type of backup. The biggest is RECOVERY!

What can go wrong?

Tape did not come without problems. Users with a lot of big files could slow down your network. Server drive space would become an issue as users would use the high-speed connection to download music and other large files to their documents folder (server share). Tapes would quickly run out of space and backup jobs would fail. In fact, tape backup jobs are notorious for failure. If you work in an office that uses a tape drive, go into the software and look at some reports of backup jobs and I'll bet you will note that there are more failures than successes. More often than not, business would realize that their tape backups were not working until they needed them. Then the stark reality that your data is truly gone forever would hit. Tempers flare, fingers get pointed, people get fired and business go down.

Newer options emerge

Because of businesses beginning to realize that their data was not as recoverable as we would like...or at all, the market opened up with newer and better ways to ensure data recoverability.

BDR Devices

This is clearly the way to go. Having a Backup and Disaster Recovery devices on the network that can backup all your critical data on all your computers and server, replicate a downed server and synchronize all that data to a secure, offsite location automatically minimized your business's chances of having a data disaster or massive amounts of server downtime. Imaging your employees working normally while your server on a bench being worked on by technicians for a few days.

What can go wrong?

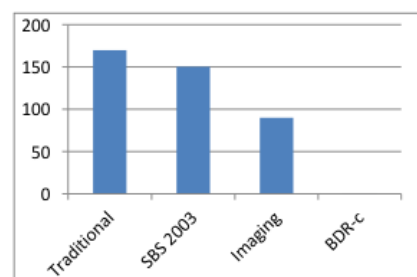
It would take an apocalyptic event to wipe out your data if you have properly employed a BDR-c device. The only thing that can realistically go wrong is that the device fails to run backups and nobody is notified. Most of these devices are programmed to send an email alert to an administrator in the event of a failed backup job.

How is BDR-c different from traditional recovery strategies?

When you first turn on your computer it goes through what is known as the “Boot process.” This is when the computer wakes up, discovers what kind of hardware it has, where the Windows operating system resides and begins to start Windows.

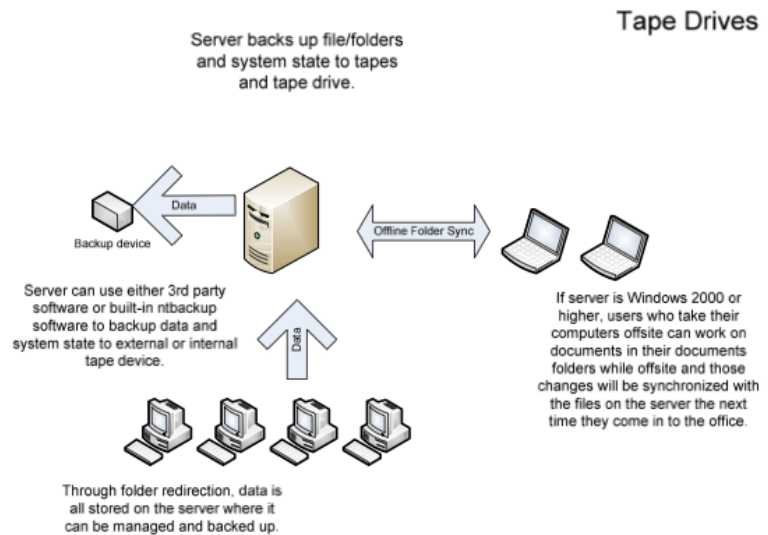
Once Windows is loaded, the user may or may not need to log in depending on the configuration of their computer. Once logged on to the computer, the user is looking at what is called the desktop. The desktop consists of open space where the user can place files, shortcuts to files/folders/network locations and programs. It also contains the task bar. On the task bar is the Start Button, quick launch toolbar and the tray icons.

	Recovery Time in hours
Traditional	170
SBS 2003	150
Imaging	90
BDR-c	0.5



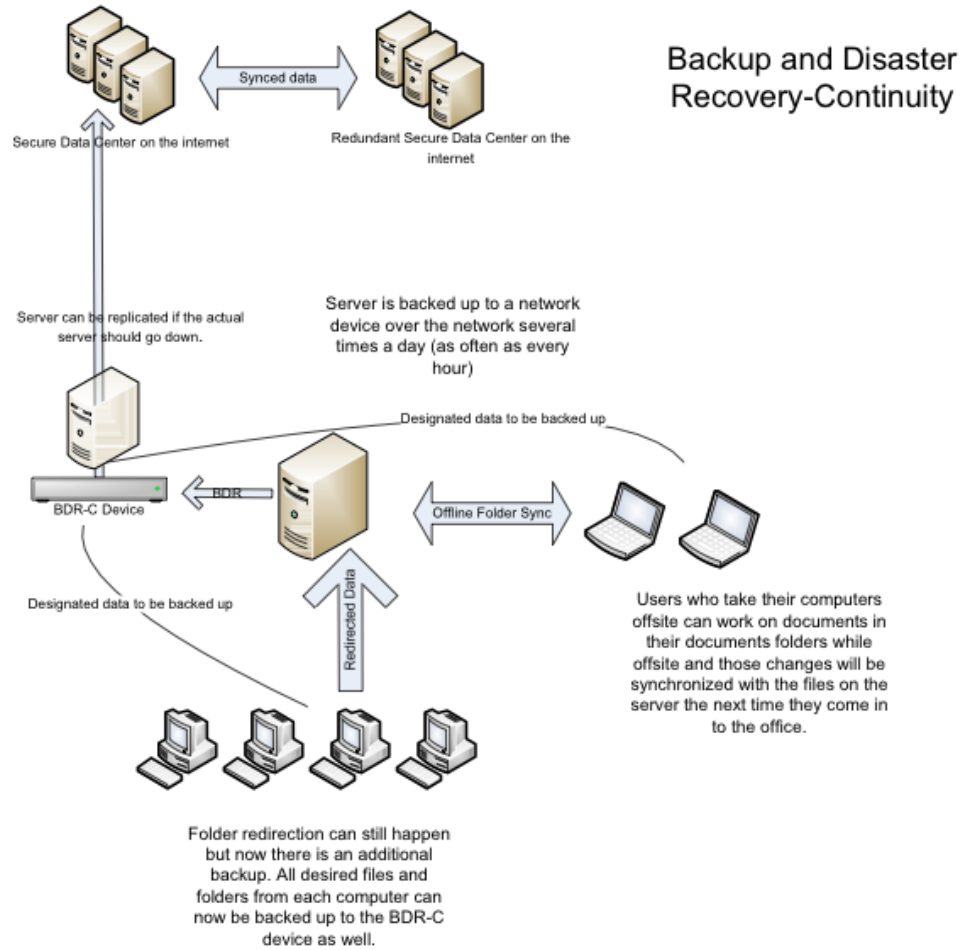
Every option except BDR-c requires server repairs or replacement to be made before network/users are back up. BDR-c can have your network/users back to work within 30 minutes. They can be productive while repairs or replacements are done.

Traditional Backups Vs. Backup and Disaster Recovery and Continuity



Pros	Cons
All data in one place for easy management if folder redirection is used.	Computers are may not be keeping a local copy of data on the local hard drive. If the server and backups fail, ALL DATA IS LOST.
Data is accessible from more than one desktop in the office.	Slow restoration of failed hard drives...usually more than a day.
	If domain needs to be rebuilt, data recovery can be impossible due to Windows security restrictions.
	No offsite solution
	Tape backup jobs fail to run successfully most of the time.
	Tapes need to be replaced regularly.
	Tapes and tape drives are very expensive
	Tapes are very limited in terms of how much data they can store.
	Offsite data storage is unreliable and usually neglected.
	Tapes are difficult to manage and archive.
Rating: 1=usless, 5=Flawless	1

Traditional Backups Vs. Backup and Disaster Recovery and Continuity



Traditional Backups Vs. Backup and Disaster Recovery and Continuity

Pros	Cons	
Doesn't matter where data is kept on the network...it can all be backed up.		
Fast restoration of any machine on the network.	In the case of total network reconstruction, recovery of everyone's documents is difficult due to Windows security structure...but not impossible.	
If server and server backups fail, documents will still exist on the user's computers and accessible as long as the domain credentials still work.	No native System State backups. There are ways to get that done though.	
Rating: 1=usless, 5=Flawless		4

Cybernut Solutions

Mailing Address

1515 North Town East Blvd
Ste 138-122
Mesquite, TX 75150

Phone: 972.216.8800

Fax: 972.767.5842

Email: stephen@cybernut.net

Web: www.cybernutsolutions.com