

4 Mistakes that Will Kill Your Data Backup Plan

...and how to avoid them

Blake King MCSE CCNA

7/28/2010

This ebook is free and you are welcome to copy it, print it out, post it and share it with friends. Please don't sell it or alter it.

The links in this PDF file work... just click on one to go to the web.

For more information about Blake or G6 Communications [click here](#)

**“By failing to prepare,
you are preparing to fail”**

Benjamin Franklin

Back, Back, Back it up

I think we can all agree that the issue of protecting company information is of high concern to business owners and managers alike. It takes a lot of time and money to create all of the information that we have in our businesses and losing it would be catastrophic.

I'm sure that we've all heard the statistical horror stories like [these](#) cautioning us to backup or fail. While most of you probably have some sort of [data backup](#) plan in place I want to highlight 4 key mistakes that will kill your data backup plan.

1. Not backing up all important company data

The biggest issue we face here is with companies that are backing up their servers but do not have any methods in place to backup their employees' workstations. Our employees generate a ton of information over time and losing the files on their workstation because the hard drive fails or they delete them could be a huge setback.

Let's face it, giving them a flash drive and sending them on their way is **not** an effective plan.

The easiest recommendation is to setup a shared drive for each employee on a server. Set the permissions so that only they have access to it.

(Do not forget this step! If they don't trust that the information they store in the directory is for their eyes only they will not use it!)

Once you have the drive setup have them map a network drive to the share. Then instruct them that they should store any important files that they have on that drive.

It is also possible to automatically store an employee's profile on your server. (i.e. Desktop, My Documents, etc.) This is much more technically advanced so I recommend that you consult with your IT guys to make this happen.

The benefit of doing this is to remove the option of storing the information on the server. Sometimes, no matter how much we encourage something, it still doesn't happen. So why leave it to chance? Make it happen automatically!

The goal here is to get all of your important information stored in a central location. This will make the data much easier to both backup and restore.

2. Not scheduling data backups frequently enough

My guess is that many of you have a nightly backup scheduled for your server(s). Now don't get me wrong, this is much better than not backing your data up at all. My question though, is it really frequent enough?

If your server fails, you stand to lose a whole day's worth of data! Think about that for a second. How much information comes into and is created in your business on a daily basis?

For instance, I know that my company generates a ton of data on a daily basis. We are logging events and systems statuses for all of our customers' equipment, our customers are submitting service

requests, our techs are entering their time and inputting data describing resolutions to those requests, sales proposals, invoices, etc. If we lost a whole day's worth of data it could literally cripple us and quite possibly put us out of business!

Now, some of you may be limited by the technology you have available i.e. tape drives. Backing your systems up to tapes generally takes a long time. Combine that with the amount of system resources being used and the inability to backup files that are in use, you're stuck backing up nightly after business hours.

The good news is there are a lot of other options out there. Just changing your backup media from tapes to external hard drives can reduce the time it takes for backups to run and not cost you a fortune.

Though it requires a larger investment, it might make sense for your business to install a separate backup server to handle the load and allow more frequent backups.

Another option available is online data backup. Most companies out there offering online data backup allow you to pay as you go based on the amount of storage you are using. This option also removes the added step of taking your backups offsite.

The point here is to analyze your business and make sure you are backing your data up frequently enough to protect yourself from a loss of business critical information.

3. Failing to store data offsite

You must protect your business from a disaster. I know, I know, I can see the eye rolls now and hear the comments “Come on, what are the chances a tornado hits tonight or my building explodes?!” My response to that is those are famous last words if I’ve ever heard them...

The fact of the matter is: **This risk is just too easy to avoid!**

A simple plan is to take the previous night’s backup tapes or hard drives home the next day. An even better option is storing them in a safety deposit box at the bank.

The problem with this plan or any plan for that matter is that it’s worthless unless it gets executed. All too often we hear businesses describe this as their offsite plan and then with a little more probing we find out that the backups are rarely ever transported offsite.

There are just too many other things going on and taking backups offsite quickly makes its way to the bottom of the list. You must make it a standard practice.

The easiest way to make offsite storage happen is to automatically store your backups in the “cloud.” What I mean is there are companies out there that sell storage online. These companies usually encrypt and securely transport your backups to redundant data centers around the country. They charge you for the amount of data that you are storing on a monthly basis.

This removes the human interface. Offsite transfers are scheduled once and then they just happen. Do a search for “cloud backup” and you will see what I mean. Also, if security is a concern, check for companies who have successfully achieved the SAS 70 Certification.

4. Failing to verify backups on a regular basis

I have saved the worst for last. This is a horrible mistake and my guess is that it's a mistake most of you are making. You can backup all of the data in your business relentlessly without fail but if you can't recover the information from those backups then they are completely worthless!

Backups should be verified on at least a quarterly basis for two reasons; to correctly verify that you are backing up all of the correct information and to ensure that you can completely recover a failed server from your backups. To verify backups a full restoration to a spare system or virtual server should be performed.

This is the only way to ensure that your data integrity is intact and that you can fully recover. This is also a good way for your IT department to practice in case of an actual disaster. When things go bad for real it will not be a good time to find out that your data is lost forever!

Do yourself a favor and review your data backup plan today!

Blake King is a Microsoft Certified Systems Engineer, Cisco Certified Network Associate and Co-founder of G6 Communications LLC. He can be reached at bking@g6com.com , by phone at 800-560-3359 ext 7 or check out his website at www.g6com.com



Want G6 to handle your backups for you? 800-560-3359

The **G6 TotalBDR™** data backup, business continuity, and disaster recovery plan combines all the features necessary to make it the most complete and reliable server data backup solution available for your business.