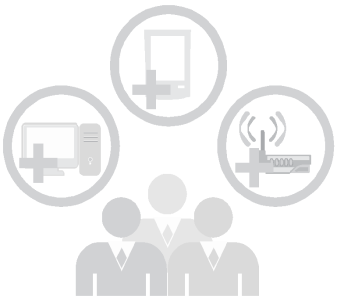
6 Critical Backup and Disaster Recovery Questions

that every owner and manager should know the answer to for their business



"There are often big differences between what business owners and managers 'think' they have regarding backup and recovery compared to what they actually have."

Nearly every small and mid-sized business (SMB) has critical data, information, and systems that it couldn't do without. From email servers, to customer databases, to critical data files — losing any of them for very long would be disastrous for the bottom line… and possibly even put them out of business.

Sooner or later — by mischief, misfortune or mistake — it is statistically likely that most businesses will face the loss of precious data or extended downtime. Despite these realities, we frequently come across business owners and managers who haven't given enough thought to backup and disaster recovery. Or, if they have given the issue some attention, we find that they haven't been thorough enough to really protect the future of their companies.

If this is a topic you haven't devoted much thought to in the past, then now is the perfect time to get started. The front page of any daily newspaper can remind you that disasters like fires, floods and storms can strike when we least expect them. Add to those the more common risks of theft, vandalism, a burst water pipe, hardware failure, or user error (which is by far the most common cause of a problem), and you can see why it's likely that you'll need a good backup and recovery plan sooner or later.

There are often BIG differences between what business owners and managers "think" they have regarding backup and recovery compared to what they actually have. Because backup and disaster recovery is definitely an issue you want to pay attention to before you need it, here are six critical questions that every owner and manager should know the answer to for their business.

1. How complete is your backup and disaster recovery system?

Many SMBs underestimate the amount of data and hardware they would need to get back up-and-running following a disaster. For example, it is not unusual to come across a business where the backup system is only backing up selected data files and folders on selected servers. Their thinking may be that "we have the most important data files, so we are in good shape. We can always just rebuild the other stuff because we have the CDs." Or they feel confident in their backups because they receive a daily email message telling them that the "job" was successful, but they are unaware that "job" only includes SOME of their files, not ALL of their files.

Wolf Consulting, Inc. is Pittsburgh's trusted leader in small and mid-size business computing. With over 24 years in the industry, our proactive approach, state-of-the-art management tools, experience, certifications and flat-rate services are just a few of the many reasons why our clients experience dramatically better results. Let our team of experts show you how to better your business and achieve greater success with professional IT service and support from Wolf Consulting, Inc.

"...It's far more common than you might think for us to perform a network assessment for an SMB and come across a well-designed backup process, only to find that it isn't working properly — or even running at all — and the business owners and managers had no idea."

The reality is that a complete backup, which allows for a complete recovery, includes operating system files and software application files. It also includes all of those lesser used data files, and it should include every server — not just some servers. Make sure that your backups aren't just covering some of your files from some of your servers. They should cover every file (operating system files, software application files, and all data files) on every server.

2. How often are your backups running?

Any backup is better than none at all. But if your company relies on access to up-to-the-minute data, and your backups only run once per week, then your business is at risk. For some businesses, even daily backups are not sufficient any more. Imagine… it is 3 p.m. and a user accidentally deletes or overwrites an important file they have been working on most of the day. Is restoring a backup from 11 p.m. last night good enough for them? If there is an unexpected problem with the server at 4 p.m., are you okay with restoring your database from last night's backup and losing all of the transactions that happened today?

Newer backup technologies allow for backup snapshots to be quickly taken multiple times throughout the day. This provides multiple "restore points" from throughout the day. So, for example, you can recover from a problem that occurs at 2:45 p.m. using a backup snapshot that was taken at 2:00 p.m.

In computer geek world, this is often referred to as a Recovery Point Objective or "RPO". It's a reference to the point in time in which you need to be able to restore from. You can have automatic backups running every 30 minutes, once a day, once a week, or even just once a month. But you should ensure that they occur frequently enough to be able to protect the information you need most.

3. How sure are you that your backups are running correctly?

It's far more common than you might think for us to perform a network assessment for an SMB and come across a well-designed backup process, only to find that it isn't working properly — or even running at all — and the business owner or manager has no idea. Often this is a result of low disk space, bad backup tapes or disks, backup software problems, incorrect configurations, user error, or just a simple lack of attention.

No matter what the reason, a backup process is only effective if it is actually working properly, so make sure you're getting regular verifications when it finishes — successfully or not.

The person or firm responsible for managing your backups should also monitor for the absence of a backup success or failure events. If the backup software stops working for whatever reason, and they are only being notified when a backup job completes with a failed status — they may never know if the backup software completely stops working.

4. Are you storing your backup data offsite?

If your backup data is stored somewhere in your office, then you could be asking for trouble. What if theft, fire or natural disaster destroys your equipment or facilities? If your backup data is lost as well, then it will be virtually impossible to get your business up and running – to say nothing of maintaining profitability – in the future.

We have a colleague who runs an I.T. consulting firm in Joplin, Missouri. A tornado ravaged their town on May 22, 2011. They had multiple SMB clients who had their backup tapes or removable disks stored onsite in a safe or offsite at someone's home. Several of them could never find those backup tapes or disks. The tornado scattered debris as far as the eye could see. Finding their tapes or disks was literally like trying to find a needle in a haystack.

Automated offsite replication of backup data across the Internet to a secure data center can be a big help. It eliminates the need to manually rotate between different physical tapes or disks, and it gets the data offsite to a different geographic location, on a daily basis. All of this happens while you are sleeping, so that by the time you arrive at the office in the morning, a copy of the backup data is already offsite — and somewhere far away.

No matter how you do your backups, it's important to have that data taken offsite on a frequent basis, and stored far away from your physical office location.

"...No matter how you do your backups, it's important to have that data taken offsite on a frequent basis, and stored far away from your physical office location."

5. How long will it take you to recover?

Having good backups in place means that you CAN recover. But many business owners and managers don't consider or truly understand how much time it will actually take to recover their system(s). This is sometimes called Recovery Time Objective or "RTO" — meaning how much time will it take to recover?

The first consideration is the computer hardware itself. Are all of your servers and critical computers covered by the vendor's hardware warranty? In far too many cases, when doing network assessments and talking with prospective clients, we come across servers with expired warranties — exposing the business to significant risk. If they have an equipment failure, they will be faced with big challenges to get it fixed, and it certainly won't be quick. For those who do have a current hardware warranty, what is the Service Level Agreement (SLA) for replacing any failed components? Most of the larger vendors (such as DELL and HP) offer same-day, 4-hour onsite service. Unfortunately, many businesses only purchased "Next Day" warranty service. Sometimes they figured they'd save a few dollars; other times the specific details were simply overlooked at the time of purchase. If you had a major hardware failure at 10 a.m., would it be okay to wait until late tomorrow afternoon for the replacement part to arrive?

Once you are in a position to actually perform the restore, how long will that process actually take? In most cases, restoring a simple data file usually only

takes a few minutes. But restoring an entire server is a different story. Depending on the volume of data to be restored, as well as the backup technology that is being used, the time for restoring an entire server can be quite a wide range — from one hour, to as long as two days. When performing assessments, we often find there is a big gap between how fast business owners and managers "think" they can recover and how much time it would actually take to recover based on their data and the technologies being used.

Many businesses no longer look at being able to recover (eventually) as being most important, but instead being able to get back up-and-running quickly. This is sometimes referred to as "Business Continuity" — or being able to continue to run the business despite an unexpected computer problem. Some newer backup technologies allow the backup system itself to actually be able to run a recent backup image as a temporary "virtual server". In the case of equipment failure of a server, this means the business could be up-and-running in less than an hour — using a recent backup (say from just 30 minutes earlier) running on the backup appliance itself. The ultimate restoration to the original or replacement server hardware can be scheduled for off-hours at some point in the future, but the business is up-and-running in the meantime.

6. Has your backup and recovery system been tested?

We periodically test backup systems for our clients. That's something you should consider, as well. You don't want to bet the future of your business on a backup and recovery system that's about to be tested for the very first time, do you? That's why it's so important to go through regular testing to ensure not only that everything is being saved, but also that your IT person or support team can restore it quickly and cleanly, and in the timeframe required.

When is the last time someone actually performed a restore from your backups? It makes sense to at least a perform a test restore of a sample set of designated files and folders on a monthly basis.

Protect your company

There aren't many SMBs that could survive the loss of critical data files or a major technology failure that lasts for an extended period of time. There are numerous unforeseen difficulties, both natural and man-made, that could bring your computer systems and communication to a halt quickly. Protect your company. Use the services of a well qualified I.T. support firm, and invest in a solid backup and disaster recovery system — one that covers everything you require, does it frequently, and can be restored in the timeframe needed. In the event that you ever need it, you'll be thankful for the advice.

To find out more about backup and disaster recovery for your business, call the experienced, certified professionals at Wolf Consulting, Inc. at 724-325-2900, or visit www.WolfConsulting.com.

Wolf Consulting, Inc.
3875 Franklintowne Court
Suite 110
Murrysville, PA 15668

724-325-2900
www.WolfConsulting.com