

A One-Page Expert Guide from Ramon Ray

Editor & Technology Evangelist, Smallbiztechnology.com

10 Tips to Achieve Backup and Recovery Success

Security and backup go hand in hand. Having secure network and computers is great, but it is only half of a comprehensive security solution. Having a secure network (and secure computers) means that your network is “hardened” against attacks from hackers, viruses, unauthorized users, or other threats. However, if your data is lost, all the security in the world cannot bring back lost customer records or employee files. A rock-solid backup strategy is great, but it is not a complete solution. If all your data is backed up but your network is shut down and your website hijacked on a daily basis, you simply cannot conduct business.

Not properly backing up your data can result in data loss that can mean:

- a) damage to your brand,
- b) loss of customer trust,
- c) civil and/or criminal penalties,
- d) shareholder lawsuits, and more.

If you are like most business owners, you know that you have to back up your local computer systems and file servers. However, it is also of utmost importance to keep the servers for your email, database, video, telephone systems, and other data properly backed up as well. These specialized systems often require specific backup solutions that are compatible with their particular data structures. Make sure you work with a local security consultant to properly back these systems up. You must have a properly implemented security and backup solution. The following 10 tips will give you practical guidelines for better backup protection.

1. Map where your business's data resides

It is impossible to properly back up your data if you do not know what you have. Work with your local computer consultant or an IT professional to learn what information you have and where it is kept. For example, is your data residing on a server in your corporate offices? Is critical data stored on a remote server in a satellite office? Is data stored on your senior staff's notebooks? Inventory what type of data you have. You may, for example, have a large assortment of client testimonial video files, and just 100 of them could take up gigabytes of storage space. You may have profiles on 700 of your clients, yet only need a few megabytes of storage space to house them. Lastly, you may have personnel files for your employees, including video files that take up a lot of space and may grow fast, client profiles that take up little space and may be easy to recover, and personnel files containing private and confidential data whose security and storage may be regulated. The type of data you have—and its content—will be a factor in how the data is backed up.

2. Keep your data and applications backed up

Often, businesses do not consider backing up their applications when they devise their backup solution. They back up the data files they create, but they often do not think to back up the installed software and operating system files. It is important to create an image of your servers and computers to make sure that the data, applications, and operating system can be completely and seamlessly recovered to their “pre-disaster” status. To properly, completely recover from disaster, you need your applications, your system files (operating system), and the data files you have created to run your business. Recovering just your data files, but not the applications to run your computers or operating system(s) to run your servers, is not complete recovery.

3. Point of recovery time

Backup systems are quite flexible regarding how much historical data they can recover. Do you always need to recover the last six months of data? Is having the most recent week's worth of data all you really need? Are you in a regulated industry where a backup solution must handle a full seven years of data? The point of recovery date and time are an important consideration.

4. Remote workers

Don't forget the data of your employees on the road. Maybe your sales manager travels around the country with her notebook computer or netbook. Do you have a strategy in place to back up the data residing on her USB key, hard disk, or external drive?

5. Online or on site

Traditional backup solutions include backing up to a local hard disk, external drive, tape, or other removable media such as DVD or CD. Over the past few years the use of online backup services has blossomed. You will need to consider which solution is best for you. Online solutions are great for remote workers and for backing up smaller amounts of data. However, they limit your backup (and recovery) speeds to the amount of bandwidth you have. Larger amounts of data will take a long time to download, and you should not only back up the data locally, but also keep a copy in off-site storage to ensure faster data disaster recovery times.

6. Test. Test. Test.

The only thing worse than not backing up your data is not properly backing up your data. Imagine that a disaster strikes your neighborhood and all your business data is completely destroyed. If you go to recover your data and find out your backups are corrupted, the wrong files are backed up, or some other terrible scenario has occurred, what will you do? Test your backups to make sure that your data is properly backed up.

7. Don't forget your servers

Your business data is not just what's in the "My Documents" folder of your area on the company's shared file server. The data in your email server, application server, and any other servers you use (including your website and hosted data) must be backed up as well.

8. Backup documentation

Make sure that more than one person (trusted) knows your backup and recovery procedures. In the event of a disaster, other members of your "business continuity team" should have the proper authorizations (if needed), overall information, and technical competence (or a local technology consultant to work with) to recover your business data.

9. Backup policies and procedures

Backing up your data is not a one-time event; it is a critical part of conducting business life, welcoming a new employee, or buying new real estate. Have procedures in place so that, as your business grows, the data it generates is safely backed up and ready to be recovered.

10. Engage trusted advisors

With limited time, budget, and employees, you should look to a solution provider to help create plans, implement automated protection solutions, and monitor for trends and threats. Your trusted advisor can also educate your employees on retrieving information from backups, when needed, and suggest off-site storage facilities for protecting your critical data.

So why is backup so important? The question is not IF you will lose your data, but WHEN. Whether it is due to accidental deletion by an absent-minded employee, intentional vandalism by a rogue vendor with access to your network, or a massive attack of thousands of infected computers, losing your data is a business reality. The question is, can you get your data back—and how fast?

Ramon Ray is a Technology Evangelist with Smallbiztechnology.com and author of *Technology Solutions for Growing Businesses*.

Ramon is not "just" a technology writer, but, as a former small business technology consultant, he has years of hands-on experience in building networks, installing software, upgrading computers, and supporting the technology that small businesses use on a daily basis. He has written thousands of technology articles and news items for Smallbiztechnology.com and other media, including *Inc. Magazine*, *New York Enterprise Report*, *Black Enterprise Magazine*, *CNet*, *VAR Business*, *TechTarget*, *Entrepreneur.com*, *Small Business Resources*, and others.