TECH SOURCE

December 2018

Volume 2 - Is your backup system ready for the new year?

Phone: 504-888-8324

Visit us at:
888-tech.com

What are backups?

A backup is a copy of a file that is stored in a different physical location than its source. These copies can then be used to restore files in the event of data loss, such as ransomware or hardware failure.

What files should I backup?

You should be backing up any files that you can't afford to lose. Emails, documents, pictures, videos, application installers, and online file shares are just a few of the things you should consider backing up. Check out our Backup Questionnaire to find out what files you can and should backup.

What are the types of backups?

There are two major types of backups: file backups and computer backups. **File backups** contain folders, files, or data. **Computer backups** contain *everything* on a computer. This includes things like applications, the operating system, and all the files.

Pros and Cons

File Backup - Pros
- Faster backup and restore time
- Requires less storage space
- Can be restored to any computer
- Less expensive
- Easier to understand

File Backup - Cons
- Can only restore files

Computer Backup - Pros
- Restores applications
- Can be used to create copies of a computer

Computer Backup - Cons
- Slower backup time (1+ hours)
- May need identical hardware to the original computer to restore properly
- Requires more storage space

Read more on Backup & Recovery, by SANS Security Awareness

What are the Best Practices for Data Backup and Recovery?

- **Backup your data regularly**. Have a backup schedule that suits your needs. Very frequent backups protect files well, but at the cost of computer and network performance. High-value files should be backed up more frequently than files of lesser importance.
- **Create at least two copies of your backups**. The more copies you have, the less likely you are to lose files.
- **Have cloud and local backups**. Having both options available allows you to take advantage of their strengths. Cloud backups are less likely to be destroyed but

are slower to recover. Likewise, local backups recover files more quickly but can be lost more easily (drive failure, destruction, etc).

- **Use reliable devices and hardware to store backups**. Some good options include a managed network drive, a managed cloud file-server, or an external USB drive. Try to avoid using USB sticks, floppy disks, and network drives which are only intermittently accessible.
- **Check to ensure your backups contain the intended files and that they are recoverable**. Regularly test your recovery process to be sure you can recover the proper files.

Best Practices in Data Backup, by DataONE

What product should I use for backup and recovery?

Do you want to manage your own backups?

Use the free Windows 7/10 Backup and Restore Guide

Do you want someone else to manage your backups?

The idea of the backup is simple, however, managing a healthy backup system for you or your company can be a difficult process. Even with an easy to use backup application such a Apple Time Machine, verifying that you are properly backing up files can be a tricky process. If managing your own backups is too much of a hassle, we are willing to do it for you. We have access to several different backup products to suit your specific needs, and can review your backups with our maintained service level.

Hot Topic of the Month - Ransomware

What is ransomware?

Ransomware is a type of malware that attempts to make you pay a ransom to access your files. This kind of malicious software can take many forms, such as locking your screen or file encryption, but the intent is always to get you to pay to resolve the issue.

How do I fight it?

Gartner recommends following these steps to prevent ransomware:

- **Assemble Crisis Team**. Ensure that your organization has a single dedicated crisis management team.
- **Perform Regular Backups**. Implement an enterprise endpoint backup product to protect user data on laptops and workstations.
- **Document Storage Locations**. Build a list of storage locations that users can connect to that are inherently vulnerable, such as file shares.
- **Evaluate the Risk**. Evaluate the potential business impact of data being encrypted due to a ransomware attack, and adjust recovery point objectives (RPOs) to more frequently back up these computer systems.
- **Create a Recovery Plan**. Align with the information security, IT disaster recovery and network teams to develop a unified incident response that focuses on resiliency, not only prevention.

In addition, we recommend the following:

1. Commercial grade virus protection, such as ESET.
2. Secure email provider like Office365, Gsuite, or Rackspace.
3. Have a computer use security policy in your employee handbook prohibiting the access of personal email at work.
4. Utilize DNS filtering solutions like the webroot DNS product included in some of our service levels.

More info on combating ransomware - Infrascale™

Register for Newsletter

Visit our website