VISUAL NEWSLETTER – NOVEMBER 2017

The Crash Plan Conundrum

For a number of years now I have recommended a backup product called Crash Plan that offered a somewhat unique set of features. Unfortunately, the Home / Small Business version of that product will be discontinued in October 2018. Some of the features that Crash Plan uniquely provided included:

1) A free version that enabled you to backup your files to your own hard drive and storage devices.

2) An encrypted backup format that made it resistant to the variety of Ransom Viruses going around.

3) An optional paid backup contract that allowed you to backup an unlimited amount of data remotely to the Crash Plan Central secure data storage site.

4) The ability to remotely backup to other computers within your company, family or group of friends.

5) Extensive versioning of complex files, that are changed periodically, allowing you to restore a file as of a specific date if a file was corrupted.

If you visit some of the discussion sites regarding this problem you will find that there is no one product that offers anything close to this full set of features. Hopefully one of the competitors will step up to fill this gap between now and next October. In the meantime Crash Plan is offering a discount on their high end Business product but this costs $120 U.S. per year per computer and does not provide computer to computer backup capabilities or any free versions for home use.

There are some free backup options like Google Drive and One Drive that offer offsite backups but they provide very limited storage, typically 5gb, in their free mode. They also usually only provide a single copy of any file so if a file is corrupted and you don't notice it for a few days then all that is available is a copy of the corrupted file should you choose to try and restore it.

Microsoft Office 365 monthly plans, starting at $10 per month provide you with Microsoft Office and extended storage capacity and once configured will provide reasonable protection from Fire, Theft and Hardware Failure for your valuable files. Businesses can also place files in Sharepoint and that does provide a degree of versioning allowing you to restore a previous version of a file, but this is still somewhat limited.

Protecting Data From Viruses

In addition to protecting our data files from Fire, Theft, Accidental or Intentional Deletion and Hardware Failure, we must now also consider Encryption Viruses as a very real threat to our personal and business files.

This is where our backup strategies must include storage media and formats that the viruses cannot find or easily attack. Generally any backup that you can browse to with File Explorer can be seen by an Encryption Virus that infects your computer and it can damage that file. In this case the original file and the backup file can both be damaged leaving you with no good copies of your valuable personal data files.

Fortunately these viruses typically only go after certain file types like Word, Excel, PDF, JPEG and MP3 files, for example, as they don't want to cripple your computer. This enables you to pay the ransom to hopefully get your files back again. If your backups are in hidden locations or in a safe encrypted format they are generally safe from these viruses and once the virus has been removed the files can be restored.

When a couple of our Libra clients were infected only their Word. Excel & PDF files were affected and their Libra files were left alone as the virus did not recognize the file formats. After we removed the virus we were able to restore the infected files from the previous day's backup with losses limited to files that were changed shortly before the virus hit the computer.

When I configure backup solutions on company file servers I like to use two backup technologies in case one of them fails. I often implement a timed schedule where I utilize Microsoft's Robocopy to mirror backup data to folders labelled Monday thru Thursday, First Friday thru 4th Friday and End of January thru End of December to provide extra flexibility in terms of our capability to restore files from different time periods. Depending of the size of your files this can require substantial amounts of storage capacity but luckily extensive storage is not overly expensive these days.

When this executes on the file server these backup folders are invisible to the users of the shared files and thus they are safe from viruses that typically infect the computers of one of the employees. A backup product , like Crash Plan, that backs up to a separate storage device or offsite location and requires software to restore files provides similar protection from viruses.