Choosing a Cloud Service Provider for Storage and Backup

More and more individuals are using the cloud for storing and backing up their personal files, and you might be thinking about doing that too. The cloud is affordable, hands-off, and convenient. You don't have to worry about taking up memory space on your devices; keeping track of physical documents; or purchasing, installing, and maintaining additional hardware. But before choosing a cloud provider, you'll want to keep a few important considerations in mind.

Security controls
Security should be your top concern, especially if you're backing up files that contain personal information and sensitive data, such as your tax and financial documents and your medical records. Without adequate controls in place, cloud computing could expose stored information to a range of threats, including theft and unauthorized access.

Data encryption
You'll want to ask how your potential cloud service provider handles encryption, specifically:

- **Will you or the provider locally encrypt the data?** Without question, you will want your data to be locally encrypted, which means that it will be encrypted *before* it is uploaded to the cloud. You can do this yourself with software like TrueCrypt of BoxCryptor, though many providers will encrypt your data locally for you. If the provider does the encrypting, you should be able to create and manage your encryption key so that the provider has no idea what you're storing and couldn't see the files if he or she tried.
- **What about server-side encryption?** This is an additional layer of security that many cloud providers offer, meaning that your data is encrypted while at rest (i.e., while it is stored but not being accessed).
- **Will your data be encrypted while in transit**, including when the provider uploads it to the cloud? This should be done via an encrypted SSL (secure socket layer) tunnel and with at least 256-bit encryption. Fortunately, this is commonplace for most cloud service providers!

Data access
You'll want to be absolutely clear regarding who has access to your data and why.

- The cloud service provider's employees will have access to its data centers and servers. Be sure that *only authorized employees* are granted access and that authorization is based on a business need.
- Be sure that the servers are owned, operated, and maintained by the cloud service provider itself and not by a third party. Some providers use servers that are owned and maintained by third parties. This means that you would have less control over data access and security.
- You'll want to consider whether any of your family members will have cloud access. That would be entirely up to you.

Extra precautions
Once you've decided on a cloud service provider, follow these steps for added security:

1. **Enable multifactor authentication** on your cloud account.
2. **Audit your files frequently.** If you no longer need to retain a backup of the data, take it off the cloud. Be sure to back your files up *often*—daily if possible.

Questions? If you have any questions about the information shared here, please feel free to call me at 610-280-9330.

110 John Robert Thomas Drive ● Exton, PA 19341 ● 610.280.9330 ● www.seidefinancial.com