CPA
Practice Advisor

operating in the cloud, from an office, or from your home you need to be thoughtful about your data. In my professional life, strategies for keeping data safe have been mandatory for over 40 years.

Randy Johnston • Jan. 12, 2014

Data is king. Keeping it stored safely and securely is critical. Whether you are operating in the cloud, from an office, or from your home you need to be thoughtful about your data. In my professional life, strategies for keeping data safe have been

mandatory for over 40 years. A consistent rule: to be able to recover, we have to have

risky. Cloud vendors used for backup may also keep backup copies beyond your retention policy, including copies after you leave their service. For example, Microsoft deletes your files within 30 days of leaving their Office 365 service, but other vendors keep your data permanently.

What Options are Available?

Recommendations for good backup vary based on your size, recovery time objective (RTO or amount of time to recover), recovery point objective (RPO-how much data you are willing to lose), and your fault tolerance level. The quicker you want to recover and the less data you are willing to lose, the more expensive the approach will be. However, relatively short RTO and RPO is possible by using backup appliances. Backup appliances combine software and hardware into a product that operates with relatively little intervention to back up your data frequently and securely.

Costs vary widely by the solution. Clearly for homes and small firms, USB drives and Network Attached Storage (NAS) units are the low cost alternative, where a few terabytes of storage cost a few hundred dollars per month. Software frequently comes with a NAS for backup purposes. However a copy of your data needs to be in some off-site location, whether that is in the cloud or another home or office. Additionally USB and NAS alternatives typically don't backup open files, SQL databases or email files correctly. When off-site cloud storage is used, expect costs in the fifty cent to one dollar (per gigabyte per month) range, although non-professional home grade storage is typically less expensive. You should not use home grade storage for professional purposes because the data does not have adequate protection. We expect providers to offer in excess of one terabyte of storage at no charge this year. Backup Appliances vary in price between $3,000 and $11,000. Two backup appliances can be used to backup from a primary location to a secondary location, eliminating the cloud storage costs, and potentially speeding the recovery process. If you contact me

Approach	**Benefits**	**Potential Shortfalls**
Run in the cloud with all Software as a Service applications or at a cloud hosting service	Agreements provide for backup so you can “not worry about it” OR you can do a reverse backup from the cloud and have copies of the data in the cloud and in your office	Data will not be available during outages, service provider may have catastrophic loss and not have an appropriate backup site or failover plan (not particularly likely)
Tape drive	Long archival life	Long backup times possible, tapes prone to failure, manual rotation of backup media required, backup software has to be configured and updated, destruction of tapes needed for compliance with document retention policies, long restore times
USB drive	Inexpensive	May not be secure, needs encryption, has to be carried off-site for

		additional safety,

Storage (NAS) drive	provision for sharing in and out of the office	of another family member OR a NAS in your office and home and a web based backup
Web based backup	Simple, off-site, easy to restore single files, may be near continuous	Large scale restores time consuming, pricing likely to increase when more data stored
Appliance based backup	Frequent copies of data made (typically every 15 minutes), rapid single file restore, multiple versions of data stored, can run as substitute virtual servers, can back up to the web or another backup appliance in a different location	Need to purchase sufficient size drives and processors, possible to outgrow, have to be replaced every five years, off-site storage to the web fees increase with more storage, need to be tested on a regular basis (weekly, minimum monthly)
Storage Area Network (SAN) replication	Can allow continuous operation even in the event of a catastrophic failure. High probability of losing little or no data. Replication of virtual machines	Virus infection or deleted files are immediately replicated to the alternate site…an archival backup is still needed. Communication speed and systems cost

	possible with a product	can be high. Consider

Pitfalls and Cautions

Things can go wrong with your data and corrupt either production files or backups. Cloud hosting and SaaS applications minimize the amount of responsibility you have for protecting the data. However, some vendors “lock the data up” and prevent you from getting your data back easily.

If you keep your data locally in your firm or home, user error, mechanical failure, intentional internal or external maliciousness, or other intrusions like viruses can destroy all of your data. Data may be mechanically safer in the cloud, but the regulatory risks increase. For example, the Patriot Act Section 215 provides for access to data stored in any data center without subpoena or notification in the U.S. According to our research over 25,000 such requests have already been made with less than 20 of the requests denied. If you store client confidential data in the cloud, this data may be provided to governmental agencies without your knowledge. According to Time Magazine, November 11, 2013, page 31, there is approximately 19 terabytes of information stored on the public web. There are another 7500 terabytes of information stored on the hidden or secret web that is used by government agencies and criminals alike.

Although not comprehensive, the following illustrates some of the issues for you to consider:

Situation	Possible Cause	Resolution or Options
Primary production file corrupted	Power inconsistent, software error, mechanical failure	Restore from backup after issue is corrected
Bad file written over the	User error made in	Attempt to restore a

top of a good file	application, then saved,	version from document
unreadable	Physical damage	restore from backup
Synchronized cloud storage missing files (SkyDrive, Dropbox)	User intentionally or accidentally deleted files	Check for hidden prior versions or restore from backup
New backup provider chosen	Better alternative found	Ensure that all files are deleted from old provider. Check on retention period to confirm files will be removed to minimize eDiscovery risk
Production or backup files stolen or compromised and were not encrypted	Error was made in setup by IT-all drives should be encrypted.	Execute security breach reporting plan. Requirements vary by state.
Catastrophic loss of office or home from fire, flood or other cause	Bad luck or not proactively repairing faulty equipment.	Find new location if necessary, purchase appropriate equipment, restore from backup
Volume of data is so large, restoring the backup will take too much time	Internet too slow, or inappropriate product was initially chosen	Ask vendor to ship an encrypted drive with your information for restore purposes
Want to leave a cloud	Vendor is not	Review the contractual

vendor and you need	responding or taking a	obligation (which
	mechanical failure	your clients, and wait. Have manual procedures ready to execute
Backup won't restore	Backup probably wasn't tested on a regular basis	Try earlier versions of backups. Implement regular restore testing procedure (weekly/ monthly). May be contracted to a managed service provider.

Key concerns with any backup data is the ability to restore, the protection of the data, the application of records retention policies, and the amount of time required to either backup or restore. With the 2013 disclosure of decryption technology held by governments around the world, my comfort level has dropped with cloud hosting, SaaS applications, and cloud-based backup. However, my caution primarily lies around risk mitigation and unexpected exposure of client confidential data. Make sure you have read the license agreement of any cloud storage provider before you use the service. Test your backups for reliability on a regular basis. And make sure you have ALL of your data backed up no matter what!

Firm Management • Security • Technology

CPA Practice Advisor is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE

Sponsors.