US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Data Backup Options

Paul Ruggiero and Matthew A. Heckathorn

All computer users, from home users to professional information security officers, should back up the critical data they have on their desktops, laptops, servers, and even mobile devices to protect it from loss or corruption. Saving just one backup file may not be enough to safeguard your information. To increase your chances of recovering lost or corrupted data, follow the 3-2-1 rule:[1]

3 – Keep **3** copies of any important file: 1 primary and 2 backups.

2 – Keep the files on **2** different media types to protect against different types of hazards.

1 – Store **1** copy offsite (e.g., outside your home or business facility).

This paper summarizes the pros, cons, and security considerations of backup options for critical personal and business data.

Remote Backup – Cloud Storage

Recent expansions of broadband internet service have made cloud storage available to a wide range of computer users. Cloud service customers use the internet to access a shared pool of computing resources (e.g., networks, servers, storage, applications, and services) owned by a cloud service provider.[2]

Pros[3]

Remote backup services can help protect your data against some of the worst-case scenarios, such as natural disasters or critical failures of local devices due to malware. Additionally, cloud services give you anytime access to data and applications anywhere you have an internet connection, with no need for you to invest in networks, servers, and other hardware. You can purchase more or less cloud service as needed, and the service provider transparently manages

---

1 Krogh, Peter. *The DAM Book: Digital Asset Management for Photographers, 2nd Edition*, p. 207. O'Reilly Media, 2009.

2 Mell, Peter, and Grance, Timothy. *The NIST Definition of Cloud Computing* (NIST SP 800-145). National Institute of Standards and Technology (NIST), 2011. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

3 Lewis, Grace. *Basics About Cloud Computing.* Software Engineering Institute, Carnegie Mellon University, 2010. http://www.sei.cmu.edu/library/abstracts/whitepapers/cloudcomputingbasics.cfm

your resource usage as it grows or shrinks. Some providers can also ensure regulatory compliance in the handling of sensitive data, which may benefit small businesses.

Cons[4]

The cloud's dependence on the internet can delay communications between you and the cloud. In addition, there are no universal standards, platforms, or languages for cloud computing, so you may become locked into one provider. The physical distribution of cloud data over many geographically dispersed servers may cause some organizations, especially ones handling sensitive data, problems with jurisdiction and fair information practices. Cloud customers have little or no knowledge of their service provider's cloud infrastructure or its reliability, and users surrender most of their control over their own data.

Security

Cloud service providers can often encrypt user data, making it harder for attackers to access critical information. However, cloud users have little or no direct control over their data or knowledge of their cloud service provider's security practices. Shared clouds store your data along with many other users' data in the same cloud infrastructure, posing a security risk.

Before you entrust your critical data to a cloud service provider, carefully check the service agreement for security practices. To increase the security of your data in the cloud, look for a cloud service provider that will encrypt your data with established encryption algorithms, such as Advanced Encryption Standard (AES) or Blowfish; transfer your data via a secure socket layer (SSL) connection; follow established network security recommended practices, such as the use of firewalls; physically protect the hardware that stores, processes, and transmits your data; and prevent your data from leaking to other customers on its cloud.

Internal Hard Disk Drives

Hard disk drives store data on a spinning magnetic platter read by a moving read/write head. Nearly all desktop and laptop computers use their internal hard drive to store most of the information they need in order to run, as well as the user's working, primary files. Secondary systems and backup servers also store data on internal hard drives.

You can buy hard drives in a wide range of storage capacities, from a few dozen gigabytes of data to several terabytes. The price per gigabyte of storage on hard drives continues to be lower than that of some solid-state storage media. Because hard drives are rewritable, you can use them to perform rolling backups, a method that automatically and periodically updates the backup files with the most recent versions of the primary files.

---

[4] Lewis, Grace. *Basics About Cloud Computing.* Software Engineering Institute, Carnegie Mellon University, 2010. http://www.sei.cmu.edu/library/abstracts/whitepapers/cloudcomputingbasics.cfm

Pros

Keeping primary file copies and backup copies on the same internal hard drive allows you to quickly update backup files and maintain a simple file structure, all without purchasing any other storage device.

Cons

Rolling backups can silently propagate any corruption or malware in the primary files to the backup files. Worse, if your internal hard drive is damaged, stolen, or corrupted, you could lose both your primary and backup files. In addition, your computer constantly uses the internal hard drive, so the more backup files you store there, the less space your computer has to operate. Lastly, the working lifespan of hard drives varies, and installing new internal hard drives requires some technical expertise.

Security

Backup files stored on the internal hard drive are just as vulnerable to damage and corruption as the primary files. Additionally, internal hard drives are only as physically secure as the computers that house them. You can encrypt hard drives to prevent unauthorized access to stored data, but data can be erased—and the hard drive rendered unusable—via magnetic degaussing without accessing the drive electronically. To increase the security of your internal hard drive, encrypt the drive's contents, physically secure your computer, and follow network security recommended practices, such as the use of firewalls and antivirus.

Removable Storage Media

Storage media that you can connect to and disconnect from your computer are a more versatile backup option than your computer's internal hard drive. Physically separating your backups from your computer helps keep your data safe, both from online attackers and power surges.

Pros

Removable media are a flexible data storage alternative because most are portable and work on most computers. They are also available in a wide variety of storage capacities and prices, so you can find the device that fits your needs and budget. Most removable media are also reusable.

Cons

Portability makes removable storage devices convenient but also makes them prone to loss or theft. Rolling backups may spread corruption and malware from the primary files to the backups.

Security

Unlike remote storage, removable storage media give you direct control over your data. However, that means you are responsible for protecting that data, especially when traveling with it. To increase the security of your removable media devices, password-protect them; encrypt their data when possible; connect them only to systems that follow network security recommended practices, such as the use of firewalls and antivirus; remove them from the computer when you complete your backup; and secure them physically.

Types of Removable Storage Media

External Hard Disk Drives

External hard drives are the same as internal hard drives, but they are portable and easy to install. They are still prone to physical damage and degaussing, and they are bulkier than solid-state storage of similar capacity.

Solid-State Storage

Solid-state storage, also known as flash drives, USB flash drives, thumb drives, SD and micro-SD cards, memory sticks, and solid state drives (SSD), is at the heart of many portable storage media, including most digital music players and smart phones. Unlike hard drives, solid state devices contain no moving parts, which allows them to be small, resist shock, and access data quickly. Use plug-and-play USB drives and cards primarily for data storage; use more complex SSDs, which can be internal or external, for data storage and processing.

USB drives are small enough to slip into a pocket and are plug-and-play compatible with most computers. Solid state media are rewritable, though they do not store data magnetically and so are not in danger of degaussing. Though some USB drives can store hundreds of gigabytes of data, and SSDs even more, solid state media still do not offer as much storage capacity as hard disk drives or digital tapes. Additionally, solid state media are more expensive per gigabyte than hard drives, though the price gap has been steadily narrowing. Writing data to a solid state device will eventually wear it out, though modern device controllers extend media lifespan. Many SSDs and even USB drives now come with built-in password protection and data encryption.

Optical Storage

Optical storage media, such as CDs, DVDs, and Blu-ray discs, store data on reflective discs read by a moving laser head that can also write data onto rewritable discs. Storage capacity varies greatly among the available optical media, from 682 megabytes on CDs, to as much as 9.4 gigabytes on DVDs, to up to 50 gigabytes on Blu-ray discs—none of which can rival the storage capacity of hard disks, solid state media, or digital tapes.

Most computers come with some kind of internal optical disc drive, and you can buy external drives as well. Though the kinds of discs may change, newer optical disc drives usually read older discs, making optical storage a forward-compatible backup option good for disaster recovery. Non-rewritable discs do not allow for rolling backups, so they might not contain the most recent version of primary files. However, data on non-rewritable discs cannot be accidentally erased or inherit corruptions or malware from later versions of primary files. Optical discs are also relatively inexpensive, though they do not come with built-in data encryption, so a third-party solution would be required.

Optical discs, especially CDs and rewritable discs, do not last forever. Handling can shorten their lifespan and, short of multi-disc hardware, optical discs must be individually handled.

Magnetic Tape

A digital tape system comprises a tape deck, individual tapes, and, optionally, a tape auto-loader. Individual digital tapes can provide capacities of more than a terabyte, or roughly a thousand

gigabytes, and are fairly cheap. Once installed, digital tape systems require little user interaction and access data very quickly. The reusable tapes enable rolling backups but are less vulnerable to viruses than hard disks, if older versions of files are adequately archived.

Though digital tapes are one of the least expensive storage media per gigabyte, digital tape systems are expensive and may require additional costs to install. The many different brands of digital tape systems are not all compatible, making it harder for you—or, on the plus side, thieves—to use your tapes in different systems.

Floppy or ZIP Disks

Floppy disks and ZIP disks store data on spinning magnetic platters, much like hard drives. However, their storage capacity is extremely low compared to other storage media, and the drives that read them are no longer being produced, making floppy disks and ZIP disks obsolete.

Choosing the Best Backup Option

Before you choose a data backup option, assess the advantages and risks of each media, your financial resources, and your needs, such as the amount of data to be backed up, protection for sensitive data (customer data, personally identifiable information, or personal health information), and accessibility of data (permanent archiving, temporary backups, and rolling backups).

Home users storing a relatively small amount of personal data should consider keeping primary files on the hard drive of their computer, with at least two backup copies on solid-state storage, optical storage (stored in jewel cases), or remote storage.

Individuals or small businesses who want to store large amounts of non-sensitive data should consider keeping working files on their hard drives or servers, with at least two backup copies on separate servers, high-capacity optical media, high-capacity solid-state storage, digital tape systems, or cloud storage. If the stored data is sensitive, be sure to carefully consider the risks of cloud storage, encrypt your data, and keep any storage media physically secure.

Large businesses or organizations should consider keeping one backup copy onsite and another offsite either through a separate data service (such as a cloud service provider or remote server backup) or on the organization's own offsite servers or digital tape system.

Whatever backup options you choose, remember to follow the 3-2-1 rule of backups:

3 – Keep **3** copies of any important file: 1 primary and 2 backups.

2 – Keep the files on **2** different media types to protect against different types of hazards.

1 – Store **1** copy offsite (e.g., outside your home or business facility).

Further Reading

American Society of Media Photographers. *Backup Overview*. Accessed August 8, 2012: http://www.dpbestflow.org/backup/backup-overview#321

Huth, Alexa, and Cebula, James. *The Basics of Cloud Computing.* US-CERT, 2012. http://www.us-cert.gov/reading_room/USCERT-CloudComputingHuthCebula.pdf

Krogh, Peter. *The DAM Book: Digital Asset Management for Photographers, 2nd edition*. O'Reilly Media, 2009.

Lewis, Grace. *Basics About Cloud Computing.* Software Engineering Institute, Carnegie Mellon University, 2010. http://www.sei.cmu.edu/library/abstracts/whitepapers/cloudcomputingbasics.cfm

McDowell, Mindi. *Protecting Portable Devices: Physical Security* (US-CERT Security Tip ST04-017). US-CERT, 2011. http://www.us-cert.gov/cas/tips/ST04-017.html

McDowell, Mindi, and Householder, Allen. *Understanding Anti-Virus Software* (US-CERT Security Tip ST04-005). US-CERT, 2009. http://www.us-cert.gov/cas/tips/ST04-005.html

McDowell, Mindi, and Householder, Allen. *Understanding Firewalls* (US-CERT Security Tip ST04-004). US-CERT, 2009. http://www.us-cert.gov/cas/tips/ST04-004.html

Mell, Peter, and Grance, Timothy. *The NIST Definition of Cloud Computing* (NIST SP 800-145). National Institute of Standards and Technology (NIST), 2011. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

US-CERT. *Home Network Security*. US-CERT, 2001. http://www.us-cert.gov/reading_room/home-network-security/

Walters, Pennie. *The Risks of Using Portable Devices*. US-CERT, 2012. http://www.us-cert.gov/reading_room/RisksOfPortableDevices.pdf