16 Best Practices to Protect Your Company Data

Against

Loss, Theft, Damage, and Manipulation

BackupChain®

Backup Software for Professionals

This guide was put together for you by BackupChain engineers and contains evergreen information on how to protect your files, PCs, and servers and never lose a file again.

Visit us at http://backupchain.com and download BackupChain today!

On our website you will find additional resources and a free 20-day, fully functional download of BackupChain Backup Software.

Email technical questions to: support@backupchain.com

Sales: sales@backupchain.com

Call: 1-800-906-5150

Contents

Good to Know

- ✓ Correlation is not causation. Even though your equipment has been working reliably, it doesn't mean it will keep working forever. Past performance is not necessarily an indicator of future performance.
- ✓ PCs and servers have become so complex they resemble "living organisms". Nothing really remains constant and it's difficult to test and narrow things down conclusively.
- ✓ Digital technology, especially storage components, is fragile and subject to wear and tear.
- ✓ The best defense against malicious software is isolated data backup.
- ✓ Common marketing fluff misleads business owners to think data protection can be automated to the point where you 'set it and forget it'. However, protecting your digital assets requires at least some labor, investment, oversight, and occasional testing of worse case scenarios.
- ✓ Would you outsource your checkbook? Data backups are technical, but even if you feel that's better handled by someone else, certain competences are best handled in-house, especially since data loss would be fatal or at least very costly to most businesses today. Most business owners probably prefer a lost checkbook over a total data loss.
- ✓ Just as everything in life, every strategy and technology has pros and cons. Conflicts of interest also exist nearly everywhere.
- ✓ In order to find out what kind of data backup system you need, you will first want to uncover how your company produces and handles data and what equipment you have. This guide contains various data backup strategies that may work well for your company. Feel free to contact us if you need assistance and have questions.
- ✓ This guide contains evergreen information on how to protect your business from losing its digital assets. You will find tips and tricks as well as a list of best practices that apply to all backup systems, no matter which backup system you end up using.
- ✓ We are always open to questions and suggestions! Email us at support@backupchain.com or call 1-800-906-5150 to simple and cost-effective ways to protect your business data.

How to Lose Your Digital Property / How Files Vanish

Chaos

The simplest way to lose your data is to lose *access* to your data. Once you have enough documents, if you can't find or recollect where it was stored, it's basically lost…at least for a while. See Best Practice #1 for tips to prevent this.

Corruption Due to Software Errors

Windows and other software packages are shipped with countless software bugs, usually in the tens of thousands! Most are harmless but some can cause corruption to data files. Because general purpose software has to work on millions of different devices with different configurations, it's impossible to guarantee the software will work on all devices at all times as expected. Certain issues only occur at rare combined events, such as a full system drive or a broken communications link. Sometimes combinations of programs are incompatible, such as an anti-virus software interfering with another software package, leading to files not being saved, etc.

Virus, Malware, and Ransomware

Viruses can be a big problem and often cause loss of data. Before you know it, hackers take control of your computer through Trojan horses which are injected to your system in the background while you browse the Internet. Even if you never download anything, these malicious programs find their way through the internet or other office computers to your system.

Ransomware in particular can be tricky to notice. It encrypts your files without you knowing it. Then a screen appears blackmailing you to pay money to have your own files decrypted. If you don't pay you can't access your files anymore. Unfortunately, backup files can be affected as well if the ransomware finds a way to access them. That's why it's crucial to use disconnected backup media and cloud backups.

Theft and Vandalism

Theft can occur anywhere: at home, at work, while you commute or visit a client.

Break-ins aren't the only problem. Since smartphones and laptops are taken outdoors frequently, and they are the prime subject for thieves. Small and light makes them a perfect target.

Theft is a common cause of data loss. Risk areas: airports, public places, parks, bars, even client visits. Office theft: Unfortunately, kleptomaniacs are present in all socioeconomic classes and all organizations in the world.

Disgruntled employees and hackers may gain access to your data either on your own PC and office network or online where you may be using web services, whether it's LinkedIn or other websites.

Accidental Deletions / Accidental Edits

Sometimes a document is edited by accident, a selected area was deleted unintentionally, or a file was deleted in a folder along with other unimportant files. The problem with accidental deletions is often they go unnoticed for a while until days or weeks later when we need access to the file.

Water Damage

All kinds of electronic equipment is sensitive to water. Whether it's a laptop being carried in the rain, a basement flood, sewer backup, or sprinkler malfunction; it only requires a drop of water to break a hard drive for good.

Children

Important equipment should obviously not be placed within reach of children. Not so obvious is that in a networked home and home office, files may be accessed via the WiFi network and damage can be done unintentionally without having physical access to the computer where the files are stored.

Fire

Fire can spread rapidly and is obviously catastrophic to all kinds of properly. Electronic storage devices are particularly sensitive to higher temperatures even if not exposed directly to a flame.

Accidents

Laura was in a rush the other day, grabbed her laptop case and ran downstairs to catch the bus. It seems, she forgot to zip up the laptop case and after just two steps the case opened and her laptop took its first flight lesson. There's barely a chance for a hard drive to survive this type of a mechanical shock.

If you accidently hit external drives and desktop PCs while they are running, for example with your shoe or hand, the mechanic shock can be strong enough to damage the sensitive magnetic surface of hard drives and thereby cause file corruption.

Dust

Not just disgusting and unhealthy: carpets, clothing, hair, pollen, exhausts, there are many sources of dust in households and offices and you will want to make every reasonable effort to keep your area clean. Not only because all the toxins contained in dust are bad for your health, but also because dust is generally bad for electronic devices, too.

Most computers have fans and the high-end modern PCs come with a dust filter. Most people are not aware of it but you need to clean the dust filter (if the device even has one) often to ensure the air circulation within the computer is sufficient to keep components cool. This is especially important on hot days or if you live in dry areas your computer may overheat due to lack of air circulation.

Another thing to consider is that dust accumulates inside hard drives and CPU heat sinks. You may be able to vacuum clean your PC inside but you won't be able to clean the hard disks from the inside. An IT network administrator from a major corporation told us: “the servers run for years, but when we switch them off for maintenance sometimes they don't come back on. The hard drives fail because the dust finally gets to settle.”

High and Low Humidity

Humid air, very low and very high humidity levels are bad for your computer and likely bad for your health, too.

You sure know why a cold beer bottle gets wet when you take it out of the fridge; however, many people are unaware of condensation that occurs in the winter when you move your laptop from the cold to room temperature, unpack it and switch it on right away.

If you don't wait long enough for the laptop to warm up before switching on, the temperature difference will cause condensation to occur inside the device, which in turn may lead to permanent damage and data loss if the hard drive is affected.

In areas of high humidity this is indeed a problem even in the summer. For example, when you take your camera out of your cool air conditioned hotel room to take pictures outdoors where it's hot and humid, you will notice the condensation on the lens. As with your camera, you will want to watch out when moving your laptop from cold to warm environments and vice versa.

Dry air with levels below 40% humidity is also a problem. Static discharge is likely to occur in dry conditions (summer as well as winter), and produce voltages of over 10,000 Volts. The voltage can enter the PC or laptop through the keyboard. If you are lucky the device is shielded and grounded properly but many cases were reported to us where static discharges lead to a blank screen, permanently.

Spilled Coffee

All experienced computer users have come across this one often enough. It's scientific fact: Keyboards and coffee naturally attract one another! Especially when this happens to laptops, it's likely to result in data loss, too.

Lightning, Power Surges and other Power Interruptions

What the seasoned IT administrator calls “PC Blitzkrieg” is indeed a common cause of data loss.

Every electronic device should be connected to a power surge adapter but most power surge adapters can only handle a surge of certain strength, *and* most surge adapters do not disconnected power after a surge occurs. Subsequent surges, which are also common, will expose your equipment to risk despite having a surge protector.

Ideally you should invest in a good UPS (uninterruptible power supply), also known as battery backup. However, these precautions protect you only from power voltage fluctuations and interruptions (which can be also very damaging, especially the unnoticeable split-second power interruptions). Short interruptions are damaging because coils produce high induction voltages when receiving a sharp pulse.

Your computer will most likely be connected to a wired network as well, such as Ethernet. These devices may not be shielded against power surges and the surge may reach your PC through that wiring. Wireless LAN is not affected because there is no wired connection.

The safest thing to do is to simply unplug all cords from your computer after work and during a lighting storm to avoid damage.

Wear & Tear and Mechanical Failures

Give your PC a break!

Wear and tear includes, for example, electronic and mechanic disk failure, bad disk sectors, worn out RAM and flash memory cells.

Things don't last forever—just as with your car, the longer your gadgets are powered on, the shorter their expected lifespan will be. This is especially true for hard drives and motherboards. It's not uncommon for hard drives to die silently or with a “funny” knocking noise. CPU fans can suddenly stop, resulting in an overheated system. Newer SSD hard drives and flash drives have a limited lifetime and storage cells wear out over time.

Temperature

Temperature that deviates from regular room temperature increases the risk of data loss.

Also, don't keep your computer in the sun light and keep it away from windows. Ensure there is enough air circulation but do not expose PCs to direct A/C air streams.

Computer needs fresh air as well as circulation; hence, do not operate computers in closed areas, such as furniture enclosures.

Hard drives and CPUs are amongst the strongest heat generators inside your PC or laptop and need constant cooling. Cooling requires large volumes of colder air to be effective. When you start hearing the ventilation fans get louder you may need to check fan dust filters or dust accumulation inside the device and perhaps place the PC elsewhere.

Mechanical Shock

The mechanical shock and following vibrations on an office desk can become strong enough to cause a head collision inside your hard disk drive. Hard drives contain tiny heads responsible for reading and writing information. These heads are rotating just fractions of a millimeter over the magnetic cylinders disks. Vertical movement beyond what a hard drive can compensate for will result in instant death for your hard drive.

Mechanical shock may occur if you drop an item on your desk while the laptop is on. Modern hard drives park their heads when turned off; therefore, the risk is much smaller if the device is powered off. A good reason *not* to buy external hard drives in vertical configuration is that they can easily tip over while turned on.

Magnetic Fields, Bit Rot, and Cosmic Radiation

You wouldn’t want your kids playing with magnets near your computer, TV, or monitor. It can magnetize your screen and, even worse, destroy your hard drives. After all, hard drives are magnetic storage; hence, another stronger magnetic field in the vicinity and….your files are history! Magnetic fields are also generated by older tube-based TV sets and electric motors, such as the one in your vacuum cleaner and other motorized gadgets and toys.

Cosmic radiation is a major cause of bit rot. The rays from the universe can damage the extremely densely built memory chips in a way that can’t be easily detected. Bit rot can show as so-called ‘flipped bits’ where a 1 turns into a 0, for example, or a character inside a Word document ends up elsewhere in the text, which is very difficult to notice.

RAM addressing defects are extremely difficult to pinpoint because most error correction standards focus on single bit errors. If your PC’s or server’s RAM is damaged and has an addressing defect, every time a file is copied, accessed, or saved, it will become corrupt. Characters inside letters can flip or become misplaced. A = B may turn into A – B, or you see random letters in whitespace that look like an accidental typo. You may want to check your computer’s RAM and hard drive perhaps twice a year to prevent this rare but serious source of data loss.

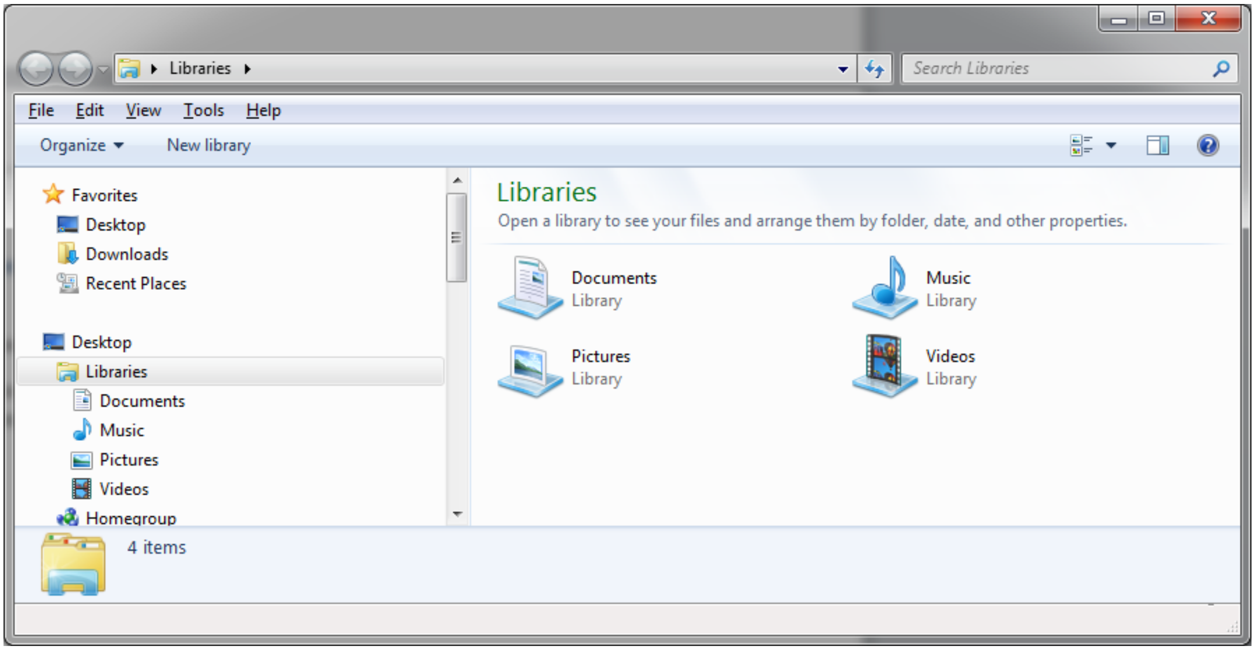
Bit rot may occur also on newer flash-type drives where cells wear out over time. While these types of hard drives have built-in mechanisms to cope with worn out cells, corruption is still a possibility.

Best Practice #1: Keeping Files in Order

Knowing where your critical documents are at all times requires some discipline and is absolutely crucial. Without having a clean hierarchical or other structure that your team is familiar with, you might soon forget that a certain document ever existed!

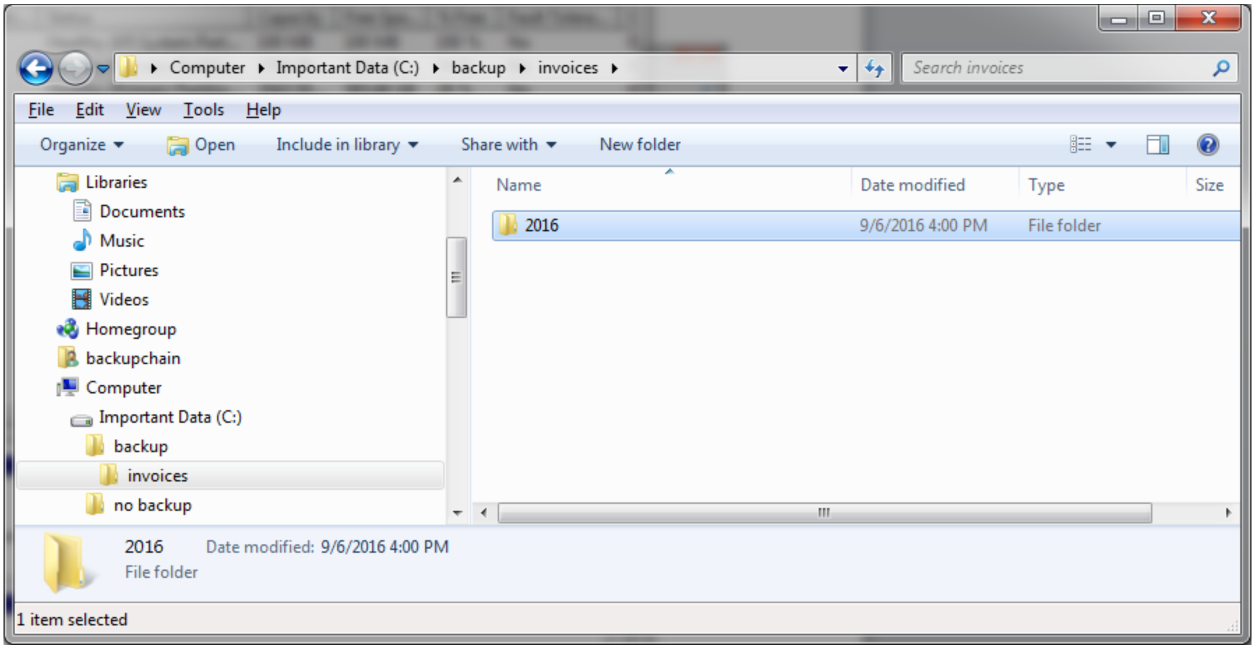
Unfortunately Microsoft has confused people with each version of Windows and pushed people into a counter-intuitive way of handling their data.

On Windows 7 when you open the Windows Explorer you see “documents”, “music”, and so on. These are virtual folders, separate for each computer user. Barely anyone knows the true location of these folders on disk:



This a major issue when you back up or recover files. Instead of using the "documents", use a dedicated folder, or even better, a dedicated folder on a dedicated data disk.

In the screen below we have an example. The drive C: is the data drive with two folders: "backup" and "no backup". As the name of these folders implies, only one will be protected by backup software. Whatever we place in the other we don't want backed up, i.e., losing those files would not matter:



Also note the hierarchy. Try using a hierarchy that is meaningful to your team. Hierarchies speed up retrieval and that helps when backing up and recovering files as well because you know exactly what needs to be copied in an emergency.

How to Find out How Much Backup Space You Need

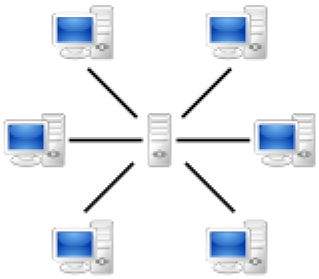
Having all your important files in one single folder (or very few) makes it also easy to tell how much overall data you have. Simply right click on the folder ->Properties and let Windows count the number of files and total byte volume. If you do this every week or month you can quickly get a reasonable estimate of how quickly data grows over time.

Knowing how much data you have and how quickly it grows and by what amount is extremely important before purchasing hardware for your backup system, so you don’t buy too little or too much.

As a rule of thumb, buy ***at least 4x*** the size of your original data. For example, if your files total about 500 GB you need to buy at least a 2 TB disk as a bare minimum. Ideal would be 4 TB or more. To give you an idea, today (2016) you can buy an 8 TB hard disk for about $200 and 10 TB drives are also available.

In addition, if you have a lot of data, you will need to estimate how fast it can be backed up without slowing down computers and affecting your network and daily work activities.

Best Practice #2: A Centralized File Server



As soon as you have more than one computer you run into 'logistics' issues. You could create network shares on each PC and access each other's files; however, as you add PCs and people accessing the same files, things can get complicated, especially when you want to ensure all data is properly backed up.

A centralized file server doesn't have to cost a lot. It could be just a simple PC for a small workgroup to which everyone has access. Larger teams might want to opt for a Windows Server, ECC RAM (reduces RAM error probability), and RAID (files are copied instantaneously to several hard drives within the same server).

You could also use a NAS device instead (Network Attached Storage) but, assuming you use Windows in your office, we do not recommend that unless the device uses a Windows operating system. The reason is simply that most NAS manufacturers save money by not using Windows and when you copy files from a Windows PC to a non-Windows device, there is a potential for several issues, mainly limitations of file name length, file name characteristics, and file size limitations. In addition, many NAS devices cannot copy file access permissions as-is. A Windows NAS, sometimes called Windows Storage Server, however, is a compatible choice as it uses NTFS internally, just as all modern Windows PCs. Common NAS brands include Drobo, QNAP, Netgear, and Synology; some of which may offer a Windows operating system as an option.

A Linux-based NAS device offers some of its own advantages and may work for your company; however, it's best to be aware of the pros and cons and risks involved in all available technologies before making a purchase.

At the very small scale a PC with one or two external drives will also work well.

Advantages of a Centralized File Server

- ✓ Simpler backup and recovery
- ✓ Simpler and more convenient file access from anywhere in the company
- ✓ It may be easier to find information when it's centralized
- ✓ Client computers, such as laptops, may be stolen or at higher risks for virus attacks
- ✓ Can be physically secured in a locked area
- ✓ Larger centralized storage may be cheaper

Disadvantages

- ✓ Single point of failure
  - If your file server is damaged or power is out where the server is located, no one can work
  - If the file server is attacked by ransomware, all data becomes inaccessible
  - If hackers get access to the file server, they have access to all the data in your company
  -
- ✓ May require management of file / folder permissions
  - You may want to allow only some users access to certain folders
- ✓ Requires more expensive hardware (server and network) in order to serve a larger number of users

Best Practice #3: Determining How Much Data You Have and How Often to Back Up

How much and how often to back up is a matter of weighing risks, costs, and labor involved. As you would expect, every strategy has its own pros and cons.

Assume you have all your important data in your C: drive in a folder called C:\Important and Windows reports 500 GB data in it.

With 500 GB data you can expect the following:

- ✓ You should have at least 2 TB backup space (4x original size)
- ✓ A full backup to a USB 2 drive or to a network server will take about
  500 * 1024 / 40 / 60 / 60 = 3.5 hours
  That's 1024 MB in one GB. 40 MB per second is the typical hard drive speed over USB2. There are 60 seconds in a minute and 60 minutes in an hour, leading us to 3.5 hours for a full backup.
- ✓ Backing up to a USB3 drive, an internal hard drive, or over a 1Gbps fast Ethernet network may be twice as fast.
- ✓ Cloud backup speeds depend very much on the available internet upload bandwidth. To estimate your internet provider's upload speed, use www.speedtest.net
  For example if speedtest.net reports you have 10 Mbps upload, you can expect about 1/9th of that in MB/sec => 1.1 MB/sec (megabyte per second). Using the above formula:
  500 * 1024 / 1.1 / 60 / 60 = 129 hours => 5.3 full days
  Hence, if you could switch to a 50 Mbps upload plan with your internet provider, the same upload would only take 1 day.

As you can see from the above examples, scheduling backups depends greatly on:

- ✓ Overall data volume, in our example 500 GB
- ✓ Internet speeds or hard drive speeds
- ✓ Available time. Can backups run only at night or also while you work during the day?
- ✓ Full versus incremental backups. Is a full backup always necessary?

Full vs. Incremental (Changes Only) Backup

When you are dealing with a file server that only holds documents, the following rules of thumb can be applied:

- ✓ File servers hold mainly constant information: documents rarely change
- ✓ The majority of files on a file server are old
- ✓ File servers grow usually by a very small percentage per month, such as 5%
- ✓ It makes sense to use incremental backups

The incremental backup strategy uses one full backup at the beginning. After the first full backup, only new and updated files are processed.

If you have a large customer or parts database (Microsoft Access, SQL Server) or virtual machines on your PC or server, you may want to consider that:

- ✓ Repeated backups will take a long time and use a lot of backup space because databases and virtual servers are very large

- ✓ Classic incremental backup schemes are not useful as every backup will require another full copy to be made

- ✓ Incremental deduplication (see later chapters) may be used to scan and find changes within databases from backup cycle to backup cycle. Deduplication can reduce backup space usage by up to 95%.

How often to back up

Backing up as often as possible may appear to be a simple and desirable strategy; however, you may want to consider:

- ✓ Backups cause system stress

- ✓ Consider the wear and tear on both source and target hard disks

- ✓ Backups may slow down servers and network traffic. Alternatively you could slow down backups but that would make the process take more time to finish.

- ✓ Some types of backups (mainly backups of databases and virtual machines using deduplication) are more efficient when done less often, as they require a file content scan.

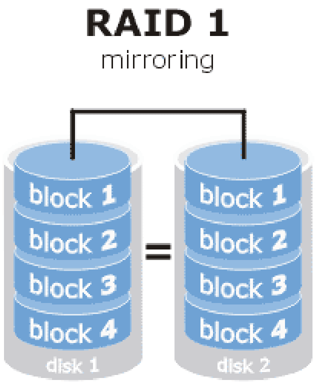
- ✓ Backing up on a short continuous schedule (say 30 minutes) is feasible on file servers, where most files won't change from cycle to cycle. In certain products like BackupChain, skipping files that are already backed up is quite fast.

- ✓ If backups are rather large and use a lot of server time and network traffic, you may want to run backups at night. In that case, backups should finish within about 12 hours or less. The actual time needed depends on total byte volume, and link and hard drive speeds, as mentioned in the above section.

- ✓ Backing up often may, under certain circumstances, may be wasteful in terms of backup space.

Best Practice #4: RAID

A RAID (redundant array of independent disks) is basically a method used in more expensive PCs, servers, and some laptops. Mirroring RAID (disk 1 is copied automatically to disk 2) is probably the most essential from a data loss prevention perspective; however, for servers there are more advanced ways to configure storage.



Some laptops and most higher-end desktop PCs can be set up to use RAID-1, called data mirroring, where files written to one drive are automatically also written to the second drive.

RAID can be somewhat complex to set up; however, once set up, it performs in the background without further intervention.

The main disadvantages of RAID are higher complexity and costs. In addition, recovery in case of a hard drive failure can be much more complicated. RAID software sometimes fails to detect imminent drive failure until it's too late.

Also note, having a RAID does not mean you have a backup. It just covers a single drive failure, not the other dozens of common risks of data loss!

Best Practice #5: External Hard Drive Backup and Rotation

External hard drives are a very convenient and cost-effective backup medium. Today an 8 TB external hard drive costs about $200, which is just 2.5 cents per GB. External hard drives connected at USB 3 ports perform almost as fast as internal hard drives, with sustained transfers of over 100 MB/sec.

In many companies external hard drives have replaced tape drives as they are cheaper, faster, and also offer very fast random access. Tape, on the other hand, has its own advantages; however, the higher cost and complexity makes tape more appropriate for enterprise users.

Using disconnected backup media in rotation

The best protection again ransomware (malicious software that encrypts all your files and then blackmails you) and various other risks, such as power surges, vandalism, theft, fire, and natural disasters is to have one or more external drives disconnected at a safe location.

For example you could back up to two external drives in rotation and take one home every day. Tools like BackupChain do not require any configuration to set this up. Simply plug in a new hard drive and change its drive letter to be the same as the other disk.

Other IT administrators use five disks, one for each workday. It's recommended to not keep these disks connected to the computer so that they are shielded from various risks, such as malicious software and viruses. Taking one drive home at a time or storing most of them offsite is a low-cost, yet elegant way to protect your business data from most risks.

When you have all your data on one single device, whether a laptop or an external drive, and take it outside of your office, keep in mind that now you are exposed to a new risk: theft.

To prevent theft, it's recommended to have all data leaving the office encrypted, which is the next best practice in our list.

Best Practice #6: Encryption and Compression

When there is a possibility that data on a device can be stolen (physically as well as digitally in the case of cloud backups) it's very important to encrypt the data on the device.

For external hard drive backups this basically means backups should use encryption. The industry standard for data encryption today is AES256. This method is being used in most modern backup systems.

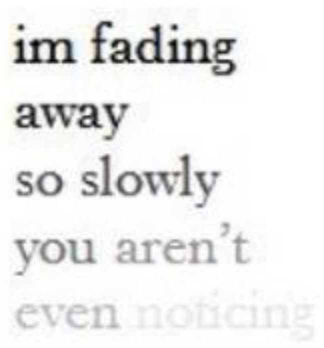
BackupChain and other systems also compress data first before encrypting it. This is another best practice because by compressing the data first, repetitive patterns in the data are removed before encryption takes place. This makes it much more difficult for attackers to find out your encryption password.

Cloud backups, which send files over the internet to a backup server, should use encryption before the file is sent and the files should remain encrypted on the remote backup server. You would want to make sure that your provider has no access to the data. But also keep in mind that if you forget your encryption password the backup files can no longer be restored without it.

Don’t travel with all your data if it’s confidential

If you handle confidential information and need to place it on a portable device, consider using BitLocker (whole drive encryption) or an encrypted ZIP archive to hold just the files you actually need.

Best Practice #7: Bit Rot Protection



im fading
away
so slowly
you aren’t
even noticing

Computers and their components have a limited lifespan as they are exposed to wear and tear, deterioration, and environment, such as cosmic radiation. Bit rot occurs when bits in memory or storage cells switch randomly from 0 to 1 or bit may become stuck on one value. Sometimes bytes are written to the wrong address when the indexing component is damaged.

Bit rot can take place for quite some time without being noticed. Some technologies exist to prevent data loss and corruption but these technologies are either expensive or address only some bit rot effects and not others. Hence, the ideology “if it ain’t broke, don’t fix it” is not recommended when your goal is protecting your data against loss and corruption caused by bit rot.

Bit rot can affect computer RAM memory as well as hard drives and other components. Some components, usually hard drives, use a so-called checksum to verify consistency when bits flip unexpectedly. This process covers mostly only single bit errors. Desktop RAM chips have no protection against bit rot. You could open a Word file, add a word and save it and thereby damage it irrevocably if the damage occurs to the file header. By opening the file and loading it into faulty memory, it can become corrupt and unreadable next time you try to open it. Another symptom of bit rot is characters that appear like typos or in previously blank areas of a Word document or spreadsheet. Thus, bit rot is extremely difficult to spot. By the time you notice it and conclude that something is wrong, lots of files will be affected.

Recommended Practice

Detect RAM Memory Bit Rot

Run a RAM memory scan and a hard drive sector scan when you buy a new computer and twice a year. Because these tests take a long time, it’s best to run these over the weekend.

To run a memory scan, open the start menu and type mdsched.exe. A new screen will appear where you can either reboot now or later. When the computer reboots it will start a scanning process.

Alternative RAM test tools require a bootable CD or USB stick and include: MemTest86+, DocMemory, and GoldMemory

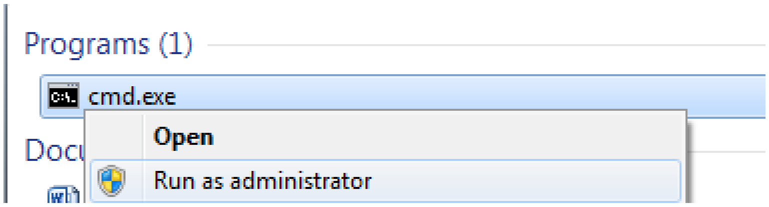
Detect Hard Drive Bit Rot

Because storage tends to fade it makes sense to check *as well as refresh* the data on hard drives. Use the Command Prompt as administrator and run:

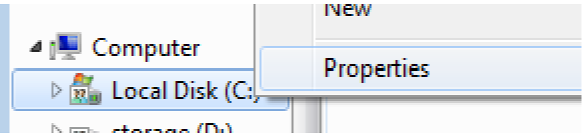
Chkdsk C: /b

Where C: is the drive you want to scan for bad sectors.

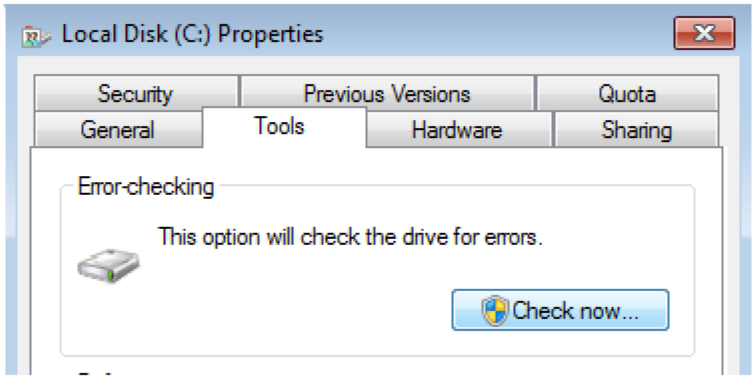
To access the command prompt, press the Start key, type cmd and when you get this screen below, right click and ‘run as administrator’. Then use the chkdsk command above.



Another way to do it: open Windows Explorer and right-click on the drive, click properties:

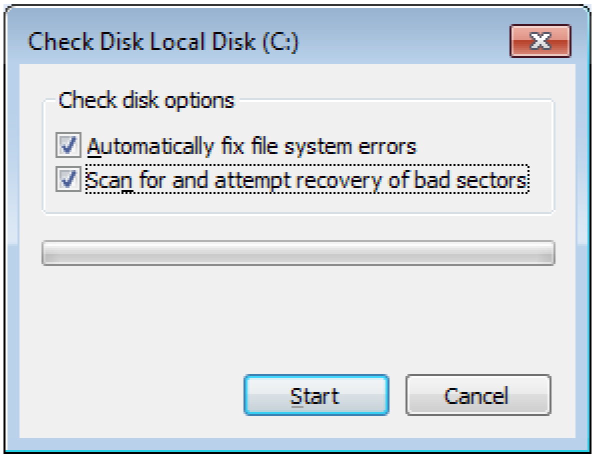


Then switch to Tools and click Error Checking, check now:



This option will check the drive for errors.

Then check the box “scan for and attempt recovery of bad sectors”



Check Disk Local Disk (C:)

Check disk options

☑ Automatically fix file system errors

☑ Scan for and attempt recovery of bad sectors

The chkdsk command in the command prompt window does the same thing.

Best Practice #8: Setting up a Backup Server or PC

If you work alone, a backup PC is simply a second laptop with your data on it.

If you already have a centralized file server, the backup server would basically be a second server.

Your backup software can be scheduled to copy the data from server A to B every night or perhaps every couple of hours. If the main server goes down, all your files can be accessed on your backup server and everyone can continue working until the main server or PC is fixed.

BackupChain can do this so-called ‘replication’ for all sorts of data beyond file servers, such as databases and virtual machines, see http://backupchain.com/kb/exact-file-copy-utility-and-backup-software-for-windows/

A unique twist to this method in BackupChain is that you can hold on to deleted files for a certain period of time (which you specify) and also you can keep a file history for each file. So basically your backup server doesn’t just have the latest version of all files, it could also store previous versions of documents and files that were deleted on the main server, for a period of time, say 30 days or a year.

We call this feature “file versioning”, where the backup software creates and manages a history of file changes. Delayed deletion is when the backup software holds on to a file in the backup server for a certain amount of time when the original has been deleted. The details are discussed in the next section.

Best Practice #9: Keeping Track of File Changes

Sometimes you work on a document for a long time. When you work on a very important document on all day for weeks, you obviously don't want to lose it or part of it but you also don't want distractions. *Ideally you will want to track every single step in certain intervals.*

File versioning is a process where the backup tool backs up the file while you work on it and creates a new version in the backup folder automatically. If it's something really important but rather small compared to your hard drive size you may want to keep all of its backups forever. If you accidently delete a section inside the document you could simply rollback and open a previous version, then copy out the parts you need back into the current document. Accidental edits and accidental deletions are very common. A simple versioning mechanism offers solid protection against these common mishaps.

Another scenario to illustrate the usefulness of this strategy: a ransomware virus infected the CEOs laptop with all data on it. The ransomware goes ahead and encrypts everything on the laptop, even the recycle bin contents. Then it blackmails the user and demands payment. The IT admin had set up all devices to be replicated to a central server and BackupChain kept track of all file versions automatically. The infected files appeared as new files and the originals remained untouched in the backup storage. A simple restore operation was enough to restore everything as it was before the attack. This worked well because the virus had no access to the backup store. If the virus also infects the backup store you could be left with nothing, unless you have a detached external drive backup or a cloud backup to restore from.

Best Practice #10: Replacing Hard Disks Before They Fail

Based on our experience it makes sense oppose the popular philosophy "if it ain't broke, don't fix it" when it comes to hard drives. You will definitely want to scan hard drives when you first receive them and twice a year after that (see above section). In addition, we recommend retiring PC and server hard disks **after two years**.

By replacing disks before they fail you can avoid the potentially chaotic situation of having to restore disks when there is so much else to do in the day. The replaced disks may be used as backup disks in a backup server, so nothing is wasted. In addition, the new disks can be of greater capacity and usually also offer better speed performance so you can stretch the life expectancy of your server or PC by a few years.

An often overlooked indicator of imminent hard drive failure, overlooked even by some seasoned IT administrators, is the Disk warning in the Event Viewer in Windows. This misnomer leads people to believe all is well when many disk warnings are really an indicator that the hard drive is about to fail completely. Other indicators include: system freezing up for about a minute when files are opened or saved, failure to boot Windows within reasonable time, blue screen errors, and clicking or other noises coming from the hard drive.

Best Practice #11: Many Copies, Multiple Media

A variation of the 'backup drive rotation' strategy is to have multiple independent copies of your data. You could set up a copy task to copy from the main server to a backup server. In addition, designated external hard drives would hold monthly backups for a year. Another set of drives perhaps weekly and daily for up to four weeks.

To make all of this efficient, tools like BackupChain use compression combined with versioning. Since only new and changed files are backed up and added to storage, space consumption depends on how much data is added each day. By compressing daily changes, you can fit roughly twice as much on a backup drive when data is compressed. However, when data is copied you have the advantage that it is immediately accessible. Compressed data needs to be restored first, which requires an additional step.

When you are dealing with large database systems and virtual machines, those type of files are gigantic and require and deduplication to reduce backup space usage. Deduplication brings down the daily load to just 5% (95% reduction); however, as with compression, the data isn't immediately accessible.

Hence, to balance the best of both strategies you would want, if you can afford it, separate sets of backups. One set is replicated, copied as-is, for immediate use in case of an emergency but requires much more storage space. Then, on a separate set of disks, you could use compression and deduplication to keep files for a much longer time; i.e., the file history would be much longer and hence you can go back in time say for 90 days rather than just 30.

On a typical file server documents and most other files do not change much over time. For that reason it's recommended to use a separate set of disks just for monthly backups and quarterly backups. These types of backups have the advantage that they are full, independent snapshots of a given point in time and are thus good for longer term archiving.

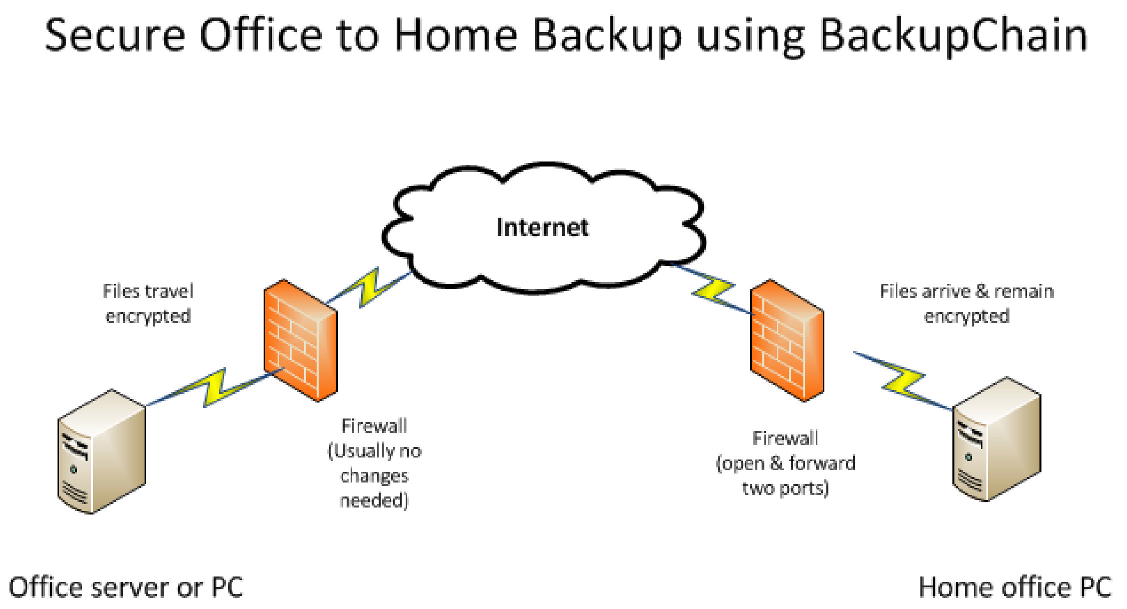
You will find that most recoveries are 'spot recoveries' where you need just a small number of files from within the last few days. This 'short-term memory' type of backup is best set up as a separate task using a dedicated target disk or server.

In summary:

- ✓ Use external hard drives locally for hourly or nightly local backups for immediate access with short history
- ✓ Use a replicate task to copy all main server data to a backup server for immediate access

- Use external hard disks connected to main server to create backups with a longer history
- Use NAS devices or other storage on the network for medium-term archiving with compression
- Use drive rotation to protect against ransomware, power surges, vandalism, and other risks
- Disconnect and place external drives in a safe, ideally in a different location. This method is the lowest cost yet effective protection against all likely local risks: fire, flood, theft, etc.
- Use cloud backup for automated offsite backup
- Use separate backup tasks on separate schedules to create independent medium and long-term archives

Best Practice #12: Back up Office Data to Home Office and Vice Versa


Secure Office to Home Backup using BackupChain

Internet
Files travel encrypted
Files arrive & remain encrypted
Firewall (Usually no changes needed)
Firewall (open & forward two ports)
Office server or PC
Home office PC

If you live in an area where high-speed internet is available to both your office and home, you can set up your DIY "cloud backup" by having the office server (could be your main central server) send its files to your house. The process can be bidirectional as well and cover multiple offices and secure office-to-office backups.

With tools like BackupChain and DriveMaker you can access your home computer's disk as a mounted drive and open files directly from your office. By using encryption, your office files will be encrypted before going over the wire and remain encrypted on your home server.

The setup with BackupChain requires just two ports to be opened on your home internet router so that the office server can reach the home PC. Additional security can be achieved by configuring the firewall to accept connections only from your office and from nowhere else, in addition to user authentication via password and encrypting files with a second password and AES256.

How fast does the internet need to be?

First you need to find out the total data volume on your office server (see best practice #1). Then use the website www.speedtest.net to obtain upload and download speeds at home and at the office.

The main link is from the office (upload) to your house (download). Use the smaller of the two numbers, usually quoted as Mbps.

Using our example from previous sections, if speedtest.net reports you have 15 MB download and 10 Mbps upload, we use 10Mbps. Hence, you can expect about 1/9th of that to be the actual throughput, which is in MB/sec => 1.1 MB/sec (megabyte per second).

If your data is 500 GB total, using this formula to determine overall upload time:

500 * 1024 / 1.1 / 60 / 60 = 129 hours => 5.3 full days

Note that there are two effects you need to consider. First, the first backup is a full compressed backup. With compression set to 'very high' the 500 GB would usually come down to about half or even less, say 250 GB. This would bring the upload down to 2.5 days. Then after that, only new files are being uploaded. The actual daily backup after the first one is incremental and likely to take only an hour or two, making this setup feasible.

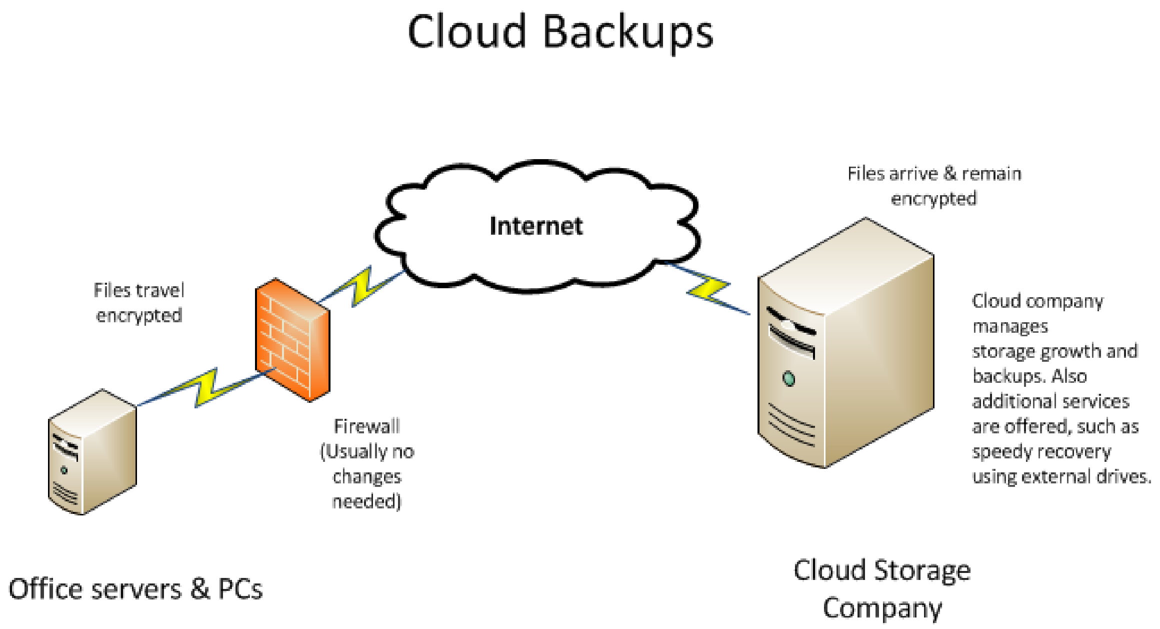
Whether it is doable to back up to your home office depends on the available bandwidth (10 Mbps in our example) and the total byte volume, we used 500 GB. If your link is considerably slower and/or your data volume is much higher your backup process will take much longer. The two options left then would be to either buy a faster internet plan from your ISP or to use cloud backup from a provider, such as BackupChain.

Your Internet Is Too Slow?

If your internet connections are too slow simply use an external hard drive backup. Take one drive to the office and leave the others at home. While this isn't automated if you have a lot of data it's much more efficient and economical than using the internet. As with cloud backups, discussed next, you would want to definitely encrypt the contents of those drives when you take them outside of the office.

Best Practice #13: Cloud Backups and Offsite Backups

While backing up to a home office is a lower cost solution, it also requires that you keep equipment running and available at all times at home. In addition, fast internet has to be available at your home as well as office.


Cloud Backups
Internet
Files arrive & remain encrypted
Files travel encrypted
Cloud company manages storage growth and backups. Also additional services are offered, such as speedy recovery using external drives.
Firewall (Usually no changes needed)
Office servers & PCs
Cloud Storage Company

If you don't want to bother using your home equipment or in areas where your home doesn't have a fast enough internet but as long as the office has fast upload bandwidth available you could use a cloud backup plan from a third party. BackupChain offers such plans as an option to the software.

The advantage of cloud backup is that the cloud backup company takes care of the storage side and the only limiting factor is the upload internet speed at your office. Storage can be bought as needed and many services, including BackupChain, offer seeding and restore services based on external hard drives, for quick recoveries.

Cloud backups are only meant to be your 'third choice' / last resort and are not meant to be used as the only type of backup you have. Because cloud backups use the internet, backups are rather slow compared to local and local network backups. In addition, in-house storage in the form of external drives involves much lower costs. Offsite backups, as discussed earlier, in the form of physically transporting external drives from office to office may be a better option in areas where no high-speed internet is available; however, this process requires labor and disks may be lost or damaged on the way.

Unfortunately, when disaster strikes, sometimes the only backup left is the cloud backup because it is stored far away at another location. Typical examples: tornadoes, fire, theft, vandalism, virus attacks that spread from the internet through to the office network and infect all PCs and backup servers, etc. Cloud backup gives you the advantage that it is automated, geographically separated and isolated, and at the same time it's very unlikely to be damaged by something happening at the office.

Best Practice #14: Disk Images and File Backups Used Wisely

Disk images are basically clones of the contents of a hard drive at the bits and bytes level. File backups are copies taken on a file by file basis. The two methods have their own pros and cons, discussed below.

Disk images can be used when hard drives fail or when you buy a new, bigger hard drive for your computer. The main advantage is that Windows and all programs are moved over to the new hard drive and you don't need to reinstall everything from scratch.

However, you shouldn't use disk images as your sole backup strategy for several reasons.

1. The new hard drive is likely to be bigger than the old one. You end up with some extra space left over and will need another tool to enlarge the partition or create new ones. In Windows 7 and later you can do that via the disk management console.

2. In many cases you need a new software license on your new PC if you want to restore a backup from your crashed PC.

3. Disk images are usually stored in a proprietary format. In BackupChain, you can use open standard formats; however as of today open standard formats do not support compression and deduplication. Direct access to your files is not available, only via intermediate steps.

4. Microsoft and other software vendors lock software to the hardware of your PC. If you restore the image on the same PC you will be able to get it to work fine. However, on a new PC the hardware codes and IDs are different and you need to re-activate Windows and other software packages.

5. If you restore the image on a new PC, it's likely that you will get blue screens during boot or intermittent crashes due to driver software mismatch. It's possible that either the system won't boot, or it will be unstable. This is because the drivers don't match your new PC's hardware. In addition it's an unnecessary hassle as all new PCs and servers come with Windows already installed.

6. Image backups take a *very long* time to complete, even in incremental/differential backup mode. If you have a lot of data to back up, you're better off just backing up specific folders using file backup methods.

7. Image backup software isn't that smart yet. It's all or nothing. Either the image can be created and restored in full or you end up with nothing. For example, if your external drive ends up being too small you won't know until you have the backup run for hours and then it will stop saying 'drive is full'. It will complain about the drive being full and leave you with no backup at all. At least with a file backup, you would have most of your files in case of an emergency.

8. If there are bad sectors on disk (source or target) the backup will likely fail, leaving you potentially with nothing at all to work with. File backups, in contrast to that, are file-by-file; hence, most files are usually still accessible when there are bad sectors present on disk.

9. On a new computer it is generally recommended, if not required, to reinstall everything from the beginning. At least then you know you have a clean system running smoothly

The reasons for #8 include: a disk image copies everything over to the new drive, including fragmented files and bloated system files that are no longer efficient. Viruses and other hidden malware are also "preserved" and moved over to your new PC.

For users other than IT administrators and power users it doesn't make much sense to bother with disk images. If it's going to be a hassle to reinstall software applications you could simply preinstall them on your backup server so they are ready to go when needed. What matters most is you have your file server structure *immediately* accessible so you do not lose time or access to your documents when you need to respond to client requests quickly.

Best Practice #15: Increase Productivity by using Virtual Machines

Do you have older servers that need to be replaced? You could convert them into a "virtual server". The benefit: use just one new physical server and run dozens of older PCs and servers as so-called "virtual machines".

This technique has gained momentum in the last decade and leads to thousands of dollars in potential savings; however, not every old server can be converted into a virtual machine. If specific hardware is being controlled by the old server you have, hardware access may not work when the server is virtual. You may want to consult with the hardware manufacturer to discuss your options.

For regular PCs and servers, virtualization can be a huge money saver. Rather than buying a dozen new servers to replace the old ones, you buy a much more powerful "host" server and run the virtual machines on it. Popular platforms are Hyper-V (Windows based) and VMware (proprietary operating system).

Simple Backup & Restore - Move Servers Around Easily

Virtual servers can be moved from server to server rather easily. The same is true about backup and restore. Backing up and restoring virtual machines is usually done on the host server and all virtual servers can be backed up at the same time from one convenient location. Virtual machines can be restored and copied elsewhere as necessary without much reconfiguration.

The downside of virtual machines is that when you had several servers, it would have been extremely unlikely for all of them to have failed simultaneously; however, if you run multiple virtual servers on a single host server you basically have a single point of failure. If the host dies, all virtual servers are gone with it. The most cost-effective “fix” for this type of eventuality is to use a backup server (see Best Practice #8).

Protect Your Company from Software Corruption & Malicious Software

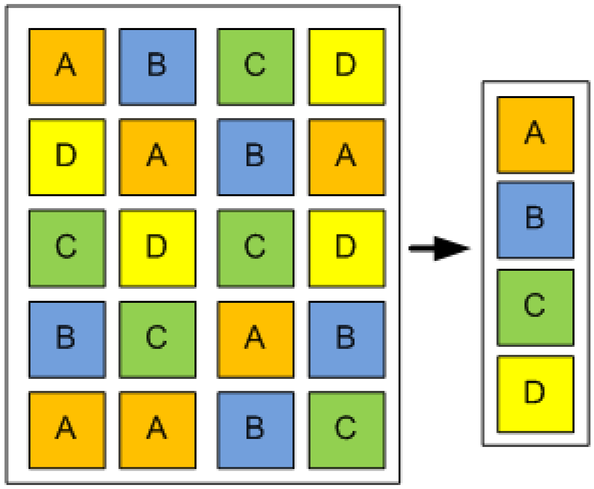
While a good portion of virtual machines are used for all sorts of testing, virtual machines offer some protection against viruses, ransomware, and software bugs.

Virtual machines can be backed up using file versioning so that you can go back in time if necessary. All common virtual platforms (Hyper-V, VMware, VirtualBox) also offer a snapshot mechanism that you can use to ‘freeze’ a certain state of the server and go back to it instantaneously if necessary. If corruption or a virus attack occurs you can immediate retrieve the prior state of the virtual machine, losing only a fraction of data.

Some security cautious IT departments utilize virtual machines for browsing the web. The virtual machine is then reset after each session to minimize the potential for virus attacks. In addition, each virtual machine can be completely isolated from the company network if you want. This makes browsing the internet much safer.

Best Practice #16: Use Deduplication for Efficient Archive Storage Usage

Deduplication is a process where repeated data (duplicates) are removed, similar to compression:



Deduplication is a major space saver when you back up virtual machines (discussed in previous section) and large databases. Instead of taking a full copy with each backup, only the differences are stored. Since only a small fraction of large database changes from backup to backup (usually from day to day), the total storage savings can easily reach 90 to 95%!

For example, a large customer database of 100 GB would fill a 1 TB drive after just 10 days when backed up nightly. However, using deduplication, the first backup would be 100 GB and each subsequent “increment” just 5 GB (on average, based on previous observations). Hence, a 1 TB disk (1000 GB) could hold now 100 GB + 180 * 5 GB => 181 days worth of backups! Naturally the 5% change per day is just a rule of thumb estimate and some days will use considerably more storage space than others. Our example here shows an 18-fold gain, which is not uncommon.

Server Administrator's Checklist: Manual PC + Server Monitoring

Below is a general checklist aimed for basic server administration and server monitoring when done by hand:

When you unpack a new computer

Hardware defects with brand-new servers and PCs are unfortunately not uncommon.

To be certain your hardware is in good condition before you put your server in production:

- Run chkdsk with /b on all drives (looks for bad sectors on disks)
- Run a long (24-48 hours) RAM test (ensures there are no RAM issues)
- Run a CPU stress test (ensures CPU and heat sink are installed properly)

Weekly

- Check Event Viewer logs (app, system, Hyper-V, security)
- Look for errors and disk/NTFS warnings which usually indicate a disk issue or upcoming disk failure
- Look for application, service, and system errors
- Check for hardware issues
- Check RAID status
- Check disk and RAM utilization
- Check disk free space is sufficient
- Check all vital applications and services are running
- Check logs of important services and applications
- Check if applications need to be updated
- Check for CPU temp alerts
- Review user accounts: delete/disable those no longer needed
- Defragment all drives (do not schedule this)
- Windows Update (do not allow to run automatically by disabling update service)
- Anti-virus update
- Check system security, also check security logs in Event Viewer

- Check for tasks with unusually high network activity, RAM or CPU utilization
- Run chkdsk without fix option

Backups

- Check backup logs in each task. confirm previous backups were running and successful
- Check backup destination disks are working and have enough free space (enough for a month or so, say 100GB minimum)

Monthly

- Test replication backups by booting replicated virtual servers without network
- Test other backups by restoring to a temp folder

Every 6 months

- Check RAM by shutting down server and boot with RAM check option. RAM should be checked for 24 hours during which server must be kept offline
- Run chkdsk with /b option for all drives to check for bad sectors (again downtime is needed for C: drive check)
- Check and wash or vacuum dust filters

Every 24 months

- Replace all server hard disks (PCs every 3 years), including backup drives if permanently connected
- Run chkdsk with /b option on all new hard drives
- Vacuum CPU heat sink, fans, and wash dust filters.

The Secret to a "Perfect" Data System

There is no secret and there are no tricks when it comes to protecting your digital business assets.

But there is indeed a secret to success: good questions leading to insight, which leads to a good decision and worry-free environment where you know all relevant risks are reasonably well covered.

Another truth is that many companies are sold equipment that is too big, too expensive, and too complex for their setting. Depending on your circumstances, however, a big and complex system may actually be a reasonable choice. We'll provide you with the questions you need to decide on your own.

Either way, every company has to have a sound strategy in place to deal with various risks. Losing data can be fatal to a business but usually this insight comes to most business owners *after* a dramatic loss.

Implementing a good strategy needs a time commitment. Above all, you need to determine how data and other documents in own business are produced and should be best protected:

- ✓ Which are the most important servers, PCs, and files?
- ✓ Is all data stored at a central location, or at least copied to one?
- ✓ How much data do we actually have? 100 GB? 10 TB?
- ✓ What would happen if we lost some of it right now?
- ✓ If lost, which data would be crucial to business and why?
- ✓ How long can your business operate without access to crucial files in case of a disaster recovery effort?
- ✓ How many days of data can you afford to lose?
- ✓ How much data is being added every day?
- ✓ How long should data be archived? Are there legal requirements?
- ✓ If you have a backup system in place, is it being tested regularly?

We'll help you narrow down these questions step-by-step and make you aware of potential traps and implicit risks with various technologies out there.

In small businesses, just as it is with marketing and your core business competence, the *strategy* to secure your critical data assets should be developed and monitored by the business owner and relevant staff who are aware of how data is being used throughout the company and the true business impact that data loss will have. Furthermore, data backup systems offer protection features at different price levels; hence, making the right choice requires knowing the technology as well as being aware which risks and costs are associated with each technology.

We at BackupChain have been developing backup software systems for over a decade. We can guide you through the process and discuss your needs—either with you or your IT service company.

Call us today at 1-800-906-5150 for a free consultation. Tell us about your company and setup. There is no obligation to purchase anything.

Contact us via email: support@backupchain.com / sales@backupchain.com

Get a free, independent opinion on your current backup system, or recommendations for a new system.

What Our Customers Say about BackupChain

"We conducted an extensive search of prospective backup software for our operations. In the end, only one product provided everything we need, including the flexibility of backing up in a format that was accessible even through our ordinary non-BackupChain software, the handling of long directory/file names, and an intuitive easy-to-use format, not to mention great costumer service. I would recommend BackupChain for any lawyer or law firm as an effective backup tool for our profession."

--Benjamin A. Kranc, Kranc Associates, Immigration Lawyers, Canada

"Just wanted to let you know that I love using BackupChain. It has saved me a couple times already."

--Dave Skoczylas, U.S. Department of Education, 100+ BackupChain Enterprise Servers in operation

"I have been using BackupChain for almost two years. My company is called Jackson, Key Practice Solutions and we have a datacenter that hosts the software for about 100 small doctors offices. We have about 25 servers, both stand-alone and in a Hyper-V virtual environment. We use BackupChain (BUC) for all of it. It is especially nice when backing up the VM's from the Hyper-V hosts. It does a good job of this, competing with products like Symantec that costs thousands. Their support has been great and for the price I've not found a better solution. In fact, I am writing this review because I really like the guys in support. They've been with me through a few tight spots and I feel I owe them."

--Albert Key, Microsoft Partner, Author of the novel and Hollywood movie: "Alabama Moon"

"I have chosen your software just because I like to have someone to talk to, it is my data and as you said a data recovery that doesn't work can be devastating. I do not want to talk with a big corporate in case of problems, where who responds is a guy that must follow thousands of customers and you are just one more annoying customer. I want to talk with someone that can listen and help if necessary.

This is your main selling point; I was surprised how good your support is"

---Tiziano Galizia, Austria

“Phenomenal support when you most need it – and we are using your product in real anger and it is simply doing what it’s meant to do. One never expects or hopes to have to restore a huge server from nothing, but today we’ve seen it all. Our many thanks to you and all the team alongside you.”

-- Nick Justice, The International Online Bridge Club Limited

BackupChain® Customers Worldwide include: ORACLE ASU ARIZONA STATE UNIVERSITY maxim integrated USDA UNIVERSITY OF CALIFORNIA JOHNS HOPKINS UNIVERSITY SANYO

Our notable customers include:

City of London (http://camden.gov.uk 60+ Enterprise Servers)
Northwest Pennsylvania Area Health Education Center
Plastic Surgeons of Northern Arizona
Holmes County Bank and Trust www.holmesbk.com
Arizona Medical Board www.azmd.gov
General Motors www.gm.com
Scobag (Swiss Bank) http://www.scobag.ch/
Grundfos, the world’s largest pump manufacturer https://us.grundfos.com/
Oracle, the world’s leading database software developer www.oracle.com
Stadtsparkasse Monchengladbach (German Bank)
Sanyo www.sanyo.com, VTech www.vtech.com
U.S. Department of Education (100+ Enterprise Servers)
Georgia Legal Services, University of Maryland, Baltimore County www.umbc.edu
Kordsa Global, Rider University
Ritchie Bros
BMW
vtech
San Francisco City Planning Department sf-planning.org
United States Bankruptcy Court, University of Missouri, Maxim Integrated
and many more, see http://backupchain.com/i/notable-clients

Please contact us to obtain additional copies of this guide.