



www.affinityitgroup.com



**WHY BUSINESS DATA
BACKUP AND RECOVERY IS
NOW A NECESSITY**

WHY BUSINESS DATA BACKUP AND RECOVERY IS NOW A NECESSITY



Every company these days must have a backup and recovery plan in place. The alternative is to risk losing the data center on which the company relies. You'll agree that there's no excuse for procrastination on this issue when you consider that 60% of companies who lose their data go [out of business](#) within a year. This startling figure rises to 93% for those companies who fail to retrieve their data after ten days.

The impact is clear.

THERE ARE FIVE CORE REASONS WHY DATA LOSS IS LIKELY TO OCCUR:

HARDWARE FAILURE

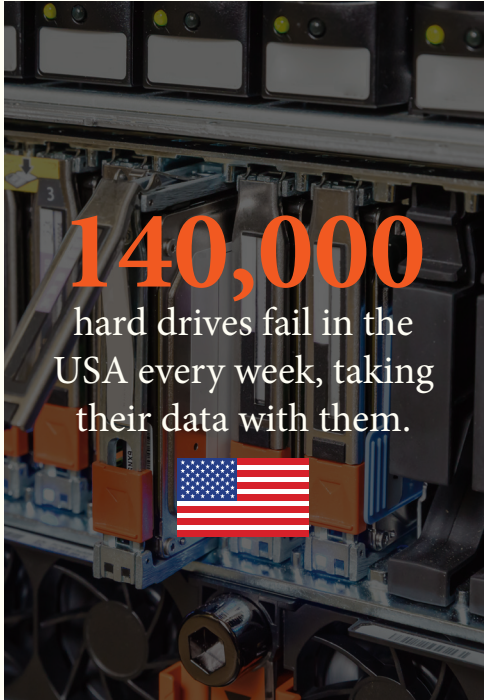
It's easy to fall into that comfortable belief that your PCs, servers, routers, and printers will live forever. Like a car, however, any hardware fails at some point.

The biggest danger can be your hard drive. As many as [140,000 hard drives](#) fail in the USA every week, taking their data with them. A Carnegie Mellon study, sponsored by Google, found typical hard drive failure rates of about [3% per year](#).

HUMAN ERROR

Whether they are malicious insiders or ignorant of their actions, humans can bring down your data center and your company with it.

Human error is cited by IT professionals as the single largest factor behind data loss. A recent study by DataBarracks found that [employee mistakes](#) were the cause of 24% of data loss incidents.



That figure could be reduced if companies adopted more stringent user policies to limit the impact of this kind of damage.

SOFTWARE CORRUPTION

Documents can be lost if the software creating them becomes corrupted. This can happen if the software is using up too much memory, or if diagnostic tools are overused.

MALWARE AND VIRUS INFECTION

Anti-malware and antivirus software should be kept updated. Once a virus breaches your network, it can spread fast. In extreme cases, the effects can be far worse than slowing PCs. Some viruses steal passwords by keylogging. Others will gobble up your data like popcorn.

NATURAL DISASTERS

Natural disasters, such as fires, floods, and earthquakes, only account for about [3% of data losses](#). What makes them so scary, however, is the speed at which they can arise and the unpredictability of their nature.

These days, it's critical to backup data to a secure offsite storage facility. This is the only way you can protect your company data against the effects of a sudden natural disaster.

With a backup and recovery plan in place, you can carry on your business operations without having to worry about the points listed above. Your plan needs to specify a guarantee that data can be recovered within 48 hours should a data loss occur.

Every day that your company is without its data risks devastating damage. Orders will go unfulfilled and your reputation could plummet. Even your most loyal customers might have no choice but to desert to your competitors.

HOW OFTEN TO BACK UP?

This depends on the size of your company, how important the data is, and how often data is updated. Backup frequencies can vary from weekly to hourly.

A high-traffic website, with a constantly updating database, will quickly render backup files obsolete. If you're receiving large numbers of orders daily, then you must backup your database daily too.

Some of the largest commercial websites backup their data on the hour every hour. Many continually write data in real-time to backup computers, a process known as replication. For companies with low-traffic websites, a weekly backup may suffice.

Either way, your company needs to have a specified interval for backing up in its backup and recovery plan. Once this plan is in place, outshine your competition by sticking to it.

FIVE BACKUP TIPS

1. Test data restores from backup regularly.
2. Encrypt all sensitive data.
3. Include an image snapshot of your data when you back up.
4. Follow the 3-2-1 rule: keep three data backup copies, store one off-site in a secure location, store the other two on different media – one of which, ideally, will be a private Cloud.
5. Copy your critical software applications, together with patches, and virtualize them in the Cloud. In the event of a data breach, your staff can continue working. This reduces costly downtime and keeps staff morale high.



BACKUP MEDIA

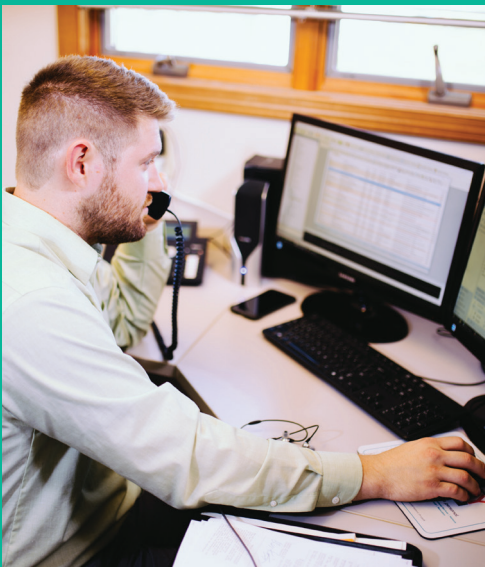
Choose your backup storage media carefully. There are several options available:

- **Tape drives** were popular in the past, but many SMEs have migrated to using low-cost disk arrays. Tape is delicate and susceptible to heat and humidity. This translates to a higher risk of a failure rate when recovering data.
- **Disk drives** are more readily available, offer low-cost encryption, and backup data much faster than tape drives. They are also more robust than magnetic tape, allowing more rewriting.

Whichever backup storage media you choose, remember that they're only effective if you use them.

Back up regularly, without fail. Your company cannot afford the inevitable pain of not doing so. Having a solid backup and recovery plan in place could save you thousands of dollars, your reputation, and even your business.

Affinity IT Group can help you secure your data backup, along with securing the rest of your technology needs.



www.affinityitgroup.com

Phone

+800.627.2214

Email

Info@AffinityITGroup.com

Address

6920 Spring Valley Dr
Suite 106
Holland, Ohio, 43528