



The Real Cost of Do-It-Yourself Backups and Why Online Backup is Better

This white paper discloses the real costs to a small business for performing proper data backups in-house using portable hard drives, then compares this with the costs and benefits of using an Online Backup Service instead.

Every business owner knows the importance of running proper data backups. Until recently the only inexpensive way to do backups in-house was with tapes or CDs. This was a time-consuming process usually relegated to an employee who was poorly trained for the task, hated doing it, and didn't do it correctly or regularly. This is especially true in small companies with no IT staff.

As a result, most small businesses do not do proper backups. Many companies have failed because of the loss of their data from a fire or flood, a hardware failure, a virus, or just a simple mistake like erasing the wrong folder.

If you have a proper, up to date backup of your critical data, it may be only a matter of hours (or even minutes) before your business can be back up and operational after a data loss. If you don't have a backup, or your backup is too old, statistics show that your business might never recover.

This article discusses the real costs of running backups, and how you can save hundreds of dollars per month while improving your backup procedure to the level of much larger companies with large IT staffs. You can make sure your vital business data survives even the worst catastrophe.

In these tough times, it's natural to try to conserve money by reducing expenses. Companies often consider bringing outsourced work back into the enterprise to reduce costs.

This article will explain in detail why it is more expensive and less desirable to perform your own backups than it is to outsource them to an Online Backup Service.

First, a few definitions:

Recovery Time Objective (RTO) is the maximum acceptable amount of time between your request to recover a file, and its recovery. For example, if you can wait at most, two hours for a file to be recovered, your RTO is two hours. The lower the RTO, the more your backups will cost.

Recovery Point Objective (RPO) is the maximum amount of data that you are willing to lose, in time. For example, if you are willing to manually re-enter at most, one day's work without a substantial loss to your business, your RPO is 24 hours. The RPO determines how often you need to make backups. The lower the RPO, the more your backups will cost.

**390 Main Street
Worcester, MA, 01608**

**P: 866.304.4300
F: 866.304.4300**

www.tritoncomputercorp.com

The File Retention Policy (FRP) specifies how long you will retain backup copies of your files, and under which conditions they will be rotated (deleted and replaced with newer copies). The longer you keep files, the more your backups will cost.

Downtime Objective is the maximum acceptable amount of time that your business, or part of it, can cease operations without substantial loss. The lower your downtime objective, the more your backups will cost.

In the real world, RTO, RPO, and FRP will be different for different types of data. Some data is far more important than the rest. For example, you might not be able to afford an interruption of more than 15 minutes in your Online Store, but you can wait until tomorrow to recover a sales presentation.

For this example we'll set a Recovery Time Objective of two hours (you want your data back no more than two hours after you ask for it), and a Recovery Point Objective of 24 hours (you want the most recent version of a backed-up file to be no older than 24 hours). So, we need to back up your files once a day.

Our File Retention Policy is 90 days simple FIFO, saving every version of a file, retaining the most recent version forever. This FRP will back up every version of a file that changes once a day, for a maximum of 90 backup copies. As each file version reaches 90 days old, it is erased. After 90 days, a single archival copy will be retained, which will be maintained as the latest version.

We will be backing up a small server running MS Windows 2003 Server. We will back up QuickBooks files, MS Word files, Exchange, and MS Office files, totaling 20 gigabytes. Of the 20 gigabytes, only about 350 megabytes changes daily.

Do-It-Yourself Backups Using Hard Drives

Before doing backups you will need to design a backup methodology taking into account your RTO, RPO, and FRP for different file sets. Select the software and hardware you need to support your backups. Design a protocol for verifying and testing backups. Design and document procedures for backup and restore operations. Designate an employee to do the backups, and a backup to that employee, and train them both.

All companies are different, and all companies have different file sets. There is no software or user's manual that can help you design a proper backup strategy for your specific company. You will need to hire a consultant to help with this.

Proper on-site backups must be done manually. This usually means that they are done during business hours, when the network is in use and files are in unstable conditions. Some files will not be backed up because they are in use and locked.

Some applications rely on many files being backed up simultaneously to retain their relational state. While these applications are in use, their file sets are in constant change, therefore unstable and difficult to back up.

With some backup software it is necessary to stop applications so their file sets will be stable for backup. If done during business hours, this results in expensive downtime. You will need to know which applications should be stopped for backup, and set up a method to make sure nobody on the network is using them during backup time.

To do onsite backups, you'll need some hardware. There are two options: Tape drives and portable USB hard drives. (We need to back up 20GB, so CDs and DVDs are too small.)

Tape Drives: Tape drives are on their way out of fashion. They are costly, slow, expensive to maintain, unreliable, insecure, and unsupported by many backup software utilities. Here's a breakdown of the cost to set up a tape backup system for your server (This assumes you already have a SCSI controller card):

HP StorageWorks DAT 72 SCSI Internal Tape Drive - \$550

DAT72 tapes (21) - \$214

Installation and Setup - \$200

Software - \$199

Total Cost to install a tape backup system: \$1,163

USB Hard Drives: USB hard drives are getting smaller, cheaper, and more reliable. Since we only have 20GB to back up, you could also use 32GB USB Flash Drives, which cost about the same.

The only way to get the same quality of file retention using USB drives as you can get with Online Backup is to buy 91 hard drives for \$5460. But, let's assume that your FRP and Downtime Objective can be flexible enough to cut that cost to just 11 drives for \$660, and \$199 for software, for a total of \$859 to get started doing your own backups.

These drives are going to last about two years, hopefully. So we need to amortize their cost over 24 months at about \$28 / month.

Proper backups require that you remove the backup from the premises so that if a disaster happens to the main location (like a fire or flood), the backup is safe. You can then restore to a new computer at another location. So, you will be transporting USB drives to and from your office every day.

Label the drives as follows: Day 1, Day 2, Day 3, Day 4, Week 1, Week 2, Week 3, Month 1, Month 2, Month 3, Permanent. We assumed your business runs 5 days a week.

On the first Monday, do a backup to the drive labeled Day 1. Then on the second day, use the drive labeled Drive 2, and so on until Thursday. On Friday, do a backup to the drive labeled Week 1.

On the second Monday, start over again with the drive labeled Day 1, and go until Thursday with Day 4. On Friday, use the drive labeled Week 2.

On the last Friday of the fourth week, use the drive labeled Month 1. You should now have used a drive for each week in the previous month, and each day in the previous week, and one drive for the month.

Use this same procedure for the next two months to use up the rest of your drives, and on the 90th day, do a backup to the Permanent drive. This should give you a few versions (but not all of them) of most of your files, for the past 90 days.

Every time you want to do a backup, you will use this procedure:

Plug the drive into the Servers USB port, and into a power outlet.

Verify that the Server has properly recognized the USB device and has assigned it the proper drive letter. The assigned drive letter must be the same for every backup.

Start the backup software. Hopefully you will be able to find software that will back up ALL of your data, verify it, and make sure it gets on the USB drive properly, and that it will do all of this in time for you to get to your kids soccer practice.

However, most backup software won't properly handle Exchange or QuickBooks. So, in addition to running the general purpose backup software, you will also have to do the following:

Run the Exchange backup using NTBackup, which comes with Windows. Don't forget to cycle the logs. This will take about 24 minutes.

Call Accounting and ask everyone to get out of QuickBooks. It has to be run in single-user mode to do a backup. Run QuickBooks (you'll need an additional license to run it on the Server) and do a backup. Call Accounting and tell them they can have QuickBooks back.

Your backup is now completed. Let's assume the person who does your backups is properly trained, does the backups every day without fail, and spends 45 minutes to do a backup. Let's assume that person makes \$15 an hour in salary. At that rate, it costs \$11.25 per day to do backups - \$225 per month.

You also have some lost productivity to take into account because Accounting, Sales, and Shipping all lost the use of their software for about 20 minutes a day.

Now that your backup is finished, you should take it out of the building and store it securely somewhere else. What's the use of a backup if it is left in the same building as the original data? If the building burns, all your backups will go up in flames, too.

So, the next step is to remove the USB drive from the building. Should the person who does the backups take the drives home and store them there? That's the easiest thing to do, but certainly the least secure.

Further, if your business is required to comply with data protection and privacy regulations like HIPAA, SOX, or GLB, it might be just plain illegal to remove this USB drive from the building, since the data on it are not encrypted.

Now you have a little hard drive that fits in the palm of your hand, containing the very heart of your company. Right here, in a handy little easy-to-read, easy-to-lose, easy-to-steal package is everything your company runs on accounting, customer lists, vendor lists, and quotes. Anyone can easily plug it into any computer and gain access to all that information.

The best way to store drives is in a secure facility like a bank safety deposit box. So, someone should take this drive to the safety deposit box and pick up the next drive that will be used for tomorrow's backup.

Both drives will be transported in an employee's automobile, which may make several stops along the way, and might become the target of a theft.

If you are paying your employee for drive time and mileage, you can conservatively add another \$7 / day to your cost of doing backups. That's \$140 per month.

Let's add the cost of the safety deposit box. That's about \$400/year for one big enough for these drives, so add another \$34 per month to your cost of doing backups.

Lets total all this up. Drives: \$24; Employee time (in office) \$225; Employee travel time \$140; Safety deposit box \$34. Were now up to \$423 / month for doing your own backups using USB drives, not accounting for loss of productivity in other departments for 20 minutes or so every day.

So far, so good? Not by a long shot. While we have managed to get data backed up and taken off site, we have not yet verified, tested, or restored the backups.

Let's not kid ourselves. Your \$15/hour employee has not been trained to verify, test, or restore backups, has he? So, if you are going to follow proper backup procedure, you'll have to hire a consultant to come in and do it. This will cost about \$300, and needs to be done every three months, bringing your monthly cost up to \$523 /month.

RESTORING FROM DISK DRIVES

390 Main Street
Worcester, MA, 01608

P: 866.304.4300
F: 866.304.4300

www.tritoncomputercorp.com

We're assuming that your backups have been done properly, so when we need to restore data, it is there on the backup disks. However, the difficulty of maintaining the daily regimen, the lack of oversight, and the reliance on manual processes makes this a dubious assumption in most cases.

Lets not further kid ourselves. You will not be able to restore data from your hard drives without outside assistance. There is no automatic restore utility. There's no software that's going to ask you simple questions, then tell you which drive to mount, and easily go find exactly the data you want, and rebuild it for you.

You're going to have to call in a consultant who understands your process, and who can manually find and restore your data. Typically this means restoring from several drives in the proper sequence, building a stable restore set, then testing it, and doing this over and over until it is correct.

This kind of restore process can take hours and even days, and can cost hundreds or thousands of dollars, and can result in downtime far beyond your original downtime objective.

You can cut the amount of time that the restore process takes by having backups done by a professional instead of by your \$15/hour employee. However, doing so will increase your costs dramatically.

If you need just a single file restored, for example, a copy of last month's budget, you may not be able to get it quickly or cheaply.

Problems with Do-It-Yourself Backups

Do-it-yourself backups are far more expensive than it seems they are as much as \$523/month for a 90 day backup plan.

Data on the backup drives are not encrypted, and can be easily read by anyone who steals the drive. The drives are small and easy to steal. Regulatory compliance issues may not allow unencrypted data to be taken off premises.

Verification and testing of backups is next to impossible.

Proper backups must be done at least once a day. The difficulty of the process, and the trouble it causes for the enterprise, makes it easy to skip a day or two.

The person responsible for backups is often a low-level employee with little or no experience in Information Technology. He can easily fail to recognize a problem with the backups, assuming they are being done properly when in fact, they are failing.

The employee responsible for backups often has no backup. So, if he is on vacation or out sick, backups may not be done.

Restoring data is cumbersome and not intuitive. Most companies hire an outside consultant when data needs to be restored. Restoring a single file, or a small group of files, is an expensive and time-consuming process.

The procedure described here of running backups using USB hard drives works well on only one computer. It will not back up your laptops, and is very difficult to scale up to multiple servers and workstations.

Advantages of Online Backups

Online Backups are usually much less expensive than do-it-yourself backups as much as 75% cheaper.

There's no hardware to buy.

Online Backups do not require an expert employee to monitor them or run them. They are run by a very smart computer program that does all the work, even when nobody is there.

Online Backups are done automatically by software. Nobody needs to remember to do them.

Online Backups are done regularly, on schedule. If, for some reason, the schedule is missed, you will get an email.

Online Backups are usually scheduled to run at night when offices are closed, and file systems are stable. This makes sure that all files are backed up.

Because Online Backups happen at night, there's no downtime to worry about.

Online Backup software backs up ALL the proper files. There's no need to run several types of backup software to back up different types of files.

Online Backups are sent offsite. There's no need to carry or store portable hard drives.

Online Backups are encrypted before transmission, and are stored in encrypted form on the backup servers. So, they are compliant with privacy and data security regulations.

Because data are encrypted with a password known only to you, nobody except you not even the Backup Service Provider has access to your information. Nobody can steal your data.

Your data files are stored in professional, high-tech data centers with all the proper security, like cameras, alarm systems, armed guards, biometric entry systems, and high-tech fire suppression. Far better than a safety deposit box.

Online Backups are properly versioned for point-in-time restores. Multiple copies are kept.

Online Backups are automatically verified.

Online Backups are quick and easy to test.

Restores can be done in minutes by the end user by simply picking files from a list, or running a Wizard. Restores can often be done from anywhere on the Internet using just a web browser.

Online Backups operate 24/7/365 without the need for consultants or end user intervention. Restores can be done any time weekends, holidays, and nights.

There's no need to worry about running out of drive space, or replacing old drives. The Backup Service Provider handles all that.

Online Backups run on ALL computers in your company not just the file servers. Even laptops that are not connected to the office network full-time can be backed up.

You receive emailed reports after every backup. You can use these reports to help audit your business practices and to keep track of your backups. If your backups encounter any kind of problems, you will get an email describing the problem.

If you want further information for remote backup for your company, go to <http://www.tritoncomputercorp.com>