NFIB GUIDE TO DATA BACKUP AND STORAGE

$12.95

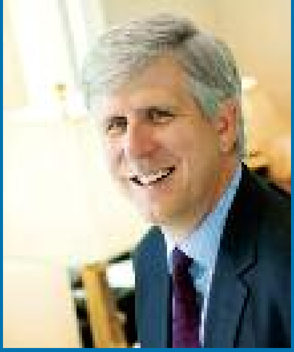
WHAT'S INSIDE

Managing Your Intellectual Property

DEVELOPED BY

DELL

NFIB
The Voice of Small Business.®



Dear NFIB Member:

As a small business owner, information and data play a significant role in your operations. Whether your business is one that inherently involves large amounts of electronic information, like accounting or law, or if you simply have to keep track of ever-changing day-to-day details like customer information and invoices, your data is growing, and growing fast.

Dealing with data growth can be stressful territory for small business owners. That's why we've compiled the *NFIB Guide to Data Backup and Storage: Managing Your Intellectual Property.* Within the pages of this guide, you'll find the answers to your most basic questions, such as why planning ahead is important to your business's health, to more complex issues, including how often and how much of your data you should be backing up, and in what manner.

Preparation is vital to overcoming the worst-case scenario (losing everything). Data loss happens more often than you might think. Recovery is possible when you have a plan in place. How quickly you're back up and running, however, depends on the option you've chosen for your backup strategy.

You work to keep your business running smoothly, but unfortunately, accidents happen. Whether it's a natural or manmade disaster, in the event of data loss, it's wise to prepare for the worst, while you hope for the best.

Helping you stay current in an evolving business environment with the *NFIB Guide to Data Backup and Storage* is just another way we're working to help you successfully grow your business.

Sincerely,

Todd A. Stottlemyer

Todd A. Stottlemyer
NFIB President and CEO

CONTENTS

ABOUT NFIB GUIDE TO DATA BACKUP AND STORAGE

Welcome to another edition of the Small Business Guides, our exclusive series of publications providing practical solutions to the challenges faced by small business owners. The *NFIB Guide to Data Backup and Storage* has been compiled to assist you in planning for and managing your business's data growth. Covering backup, file sharing, restoration strategies and more, your handbook will help you manage and maintain access to your intellectual property.

ABOUT NFIB

The National Federation of Independent Business is the leading small business association representing the consensus views of its members in Washington and all 50 state capitals. NFIB's mission is to promote and protect the right of our members to own, operate and grow their businesses. NFIB gives members access to many business products and services at discounted costs and provides timely information designed to help small businesses succeed.

ABOUT DELL

Dell was founded in 1984 by Michael Dell on a simple concept: By selling computers directly to customers, we could understand their needs and efficiently provide effective computing solutions better than our competition. This is especially true now. Dell has specially trained small business sales reps that can help you determine the best technology solution to meet your businesses needs, whether it is how to manage your point of sale data, to wireless security, to which software you need to design your next big product, to how to set up your first server network. Dell focuses on what you need so you get only what you want.

In 2003, NFIB partnered with Dell to provide computers, printers, servers, monitors and point-of-sale solutions at a discount to NFIB members—that was just the beginning. Five years later, Dell's commitment to NFIB is stronger than ever, branching out to support members in numerous ways.

Dell is excited to bring you a series of NFIB Small Business Technology Guides, focusing on up-to-date information addressing technology issues and solutions for small business. Whether you need to purchase a new computer, printer, or software, or just need some helpful technological information, look to NFIB and Dell to provide you with the perfect small business solution.

INTRODUCTION:

FAST GROWTH BRINGS ADDED CHALLENGES

Your business is growing, and so is your data. Here's why you should care. . .

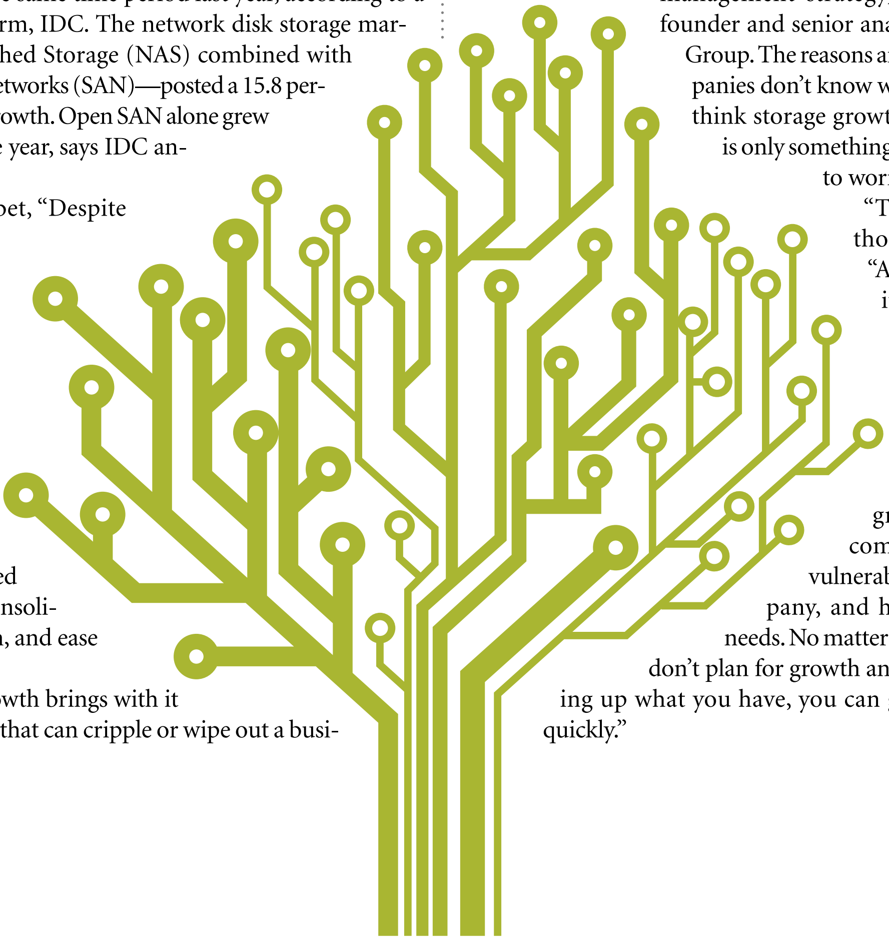
The 1984 movie Gremlins contains a key scene where the loveable little hero, Gizmo, gets into a little hot water—literally—spawning hundreds of other gremlins, all of whom aren't that nice. While you probably wouldn't compare your important data and files to an imaginary movie character, many business owners might agree that dealing with unfettered data growth can be just as scary as dealing with gremlins.

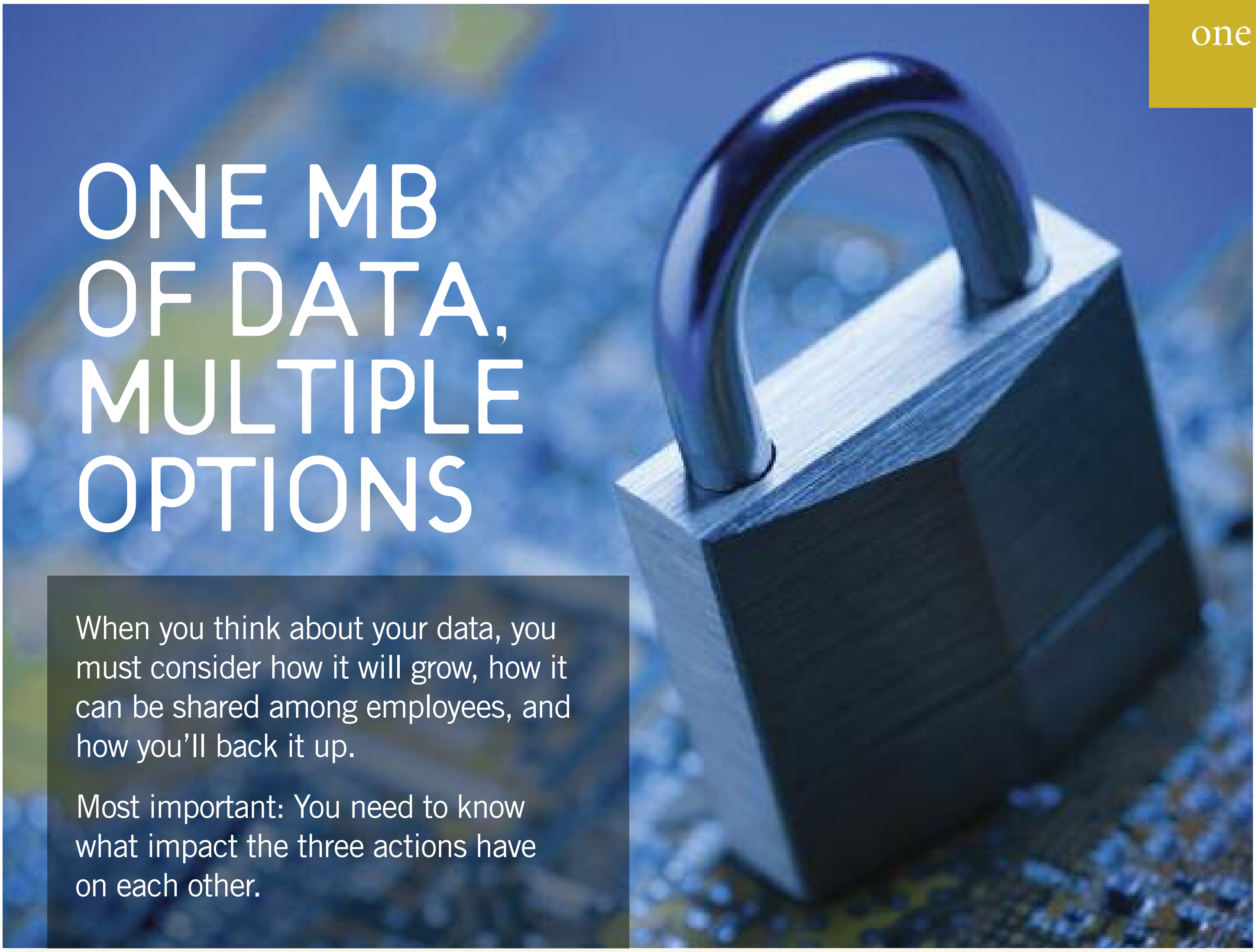
And data—as well as the need for devices and media to store it—is growing pretty quickly. In fact, worldwide external disk storage system revenue grew 9.8 percent year-over-year from the fourth quarter of 2006 to the same time period last year, according to a report by research firm, IDC. The network disk storage market—Network Attached Storage (NAS) combined with Open Storage Area Networks (SAN)—posted a 15.8 percent year-over-year growth. Open SAN alone grew 17.2 percent over the year, says IDC analyst Brad Nisbet.

According to Nisbet, "Despite the current global economic uncertainties, the disk storage systems market is benefiting from a wide variety of drivers, ranging from the simple need to store ever-increasing volumes of business data to the more sophisticated objectives around consolidation, virtualization, and ease of management."

Unfortunately, growth brings with it a series of challenges that can cripple or wipe out a business completely if the challenges aren't handled correctly. This is especially true for small businesses. The biggest problem: Most small businesses don't have a formal storage and data management strategy, says Greg Schulz, founder and senior analyst with StorageIO Group. The reasons are varied. Some companies don't know where to start. Others think storage growth and management is only something big enterprises need to worry about.

"The notion is clear, though," says Schulz. "A company—whether it has 10 or 500 employees or two or 100 computers—relies on the data contained on those servers and PCs to the same degree. In fact, a small company can be more vulnerable than a large company, and have greater storage needs. No matter what happens, if you don't plan for growth and if you're not backing up what you have, you can get into big trouble quickly."





ONE MB OF DATA, MULTIPLE OPTIONS

When you think about your data, you must consider how it will grow, how it can be shared among employees, and how you'll back it up.

Most important: You need to know what impact the three actions have on each other.

IT'S ALMOST INEXPLICABLE, BUT ACCORDING to The U.S. Commerce Department and the 2007 CSI Computer Crime and Security Survey, intellectual property theft costs U.S. businesses about $250 billion each year. Even worse, the U.S. economy loses about 750,000 jobs to intellectual property theft. And the worst part: the criminals may be the people sitting next to us in our offices. Insider attacks are the number one security threat for U.S. businesses. All businesses should have a disaster recovery plan in place. One of the basic elements of such a plan—data management, something that small businesses know they need to think about, but often don't execute as well as they should, says Arun Taneja, founder and consulting analyst with Teneja Group, a consulting and research firm.

> "The more data needs to be shared, the more data that needs to be moved, the larger the chances are of the data being lost, dropped, corrupted or destroyed in one form or the other...."

There are three key components of data management: growth, data sharing and protection. All are interconnected, and all affect an overall backup and disaster recovery plan.

You can't create a plan unless you know how fast your company and data is growing year-over-year. You need to identify this figure so you know how much backup space you'll need—whether you're outsourcing your backup, doing it in-house, or using an online service—as well as how much it will cost in the long run. You also have to figure out who needs or wants access or shared access to each individual file or application. Unless you know who will be using a file, you can't choose the right backup and sharing technology. And the final must-have fact when choosing a backup solution: how often your data is accessed, and how long you can be without it should you experience a failure and be forced to execute a restore. Each category is equally as important as the next when it comes to your data's security and safekeeping, says Taneja.

"The more data needs to be shared, the more data that needs to be moved, the larger the chances are of the data being lost, dropped, corrupted or destroyed in one form or the other," he says.

YOUR OWN CRYSTAL BALL

Why planning ahead can help you manage data growth and keep your business healthy.

YOU MAY HAVE PLENTY OF SPACE on your laptop, desktop, or file server today, but chances are that will change over the next two years. That's because the amount of data created and used on a daily basis just keeps growing. And that's just the data that's created from normal, everyday business processes. Those companies that plan on adding an on-site data replication and backup plan in the immediate future will instantly find themselves with double the data—and double the need for space, says Greg Schulz, founder and senior analyst with research firm, StorageIO Group.

"Realistically, if you want to back up all you have in-house, you will be making a copy of everything you have, which will double your storage needs," he says. "But it's not out of line to expect that your data needs will come closer to three times what you have on hand right now."

And it's not just something you can put off until you start running out of room. Full data storage devices run more slowly and can affect your productivity. Plus, you never want to be faced with the prospect of having to make changes without the benefit of research, planning, and careful execution and backup when migrating to a new server or adding additional space.

> "Pruning and archiving regularly will reduce growth. . . .But unless you're willing to make the commitment, which most people don't have the time or energy to do, you'll need to plan for doubling your storage every six months to two years."

Of course, figuring out how much storage you'll need requires you to know how much you actually have today. Thankfully, for most companies, if you know where you've come from, it shouldn't be too hard to plan for future growth. Although data growth varies wildly from one company or industry to the next, "there are some standard assumptions you can make as long as you don't fall into a high-growth category such as architecture, oil and gas, or digital image creation and storage, among other industries," says Arun Taneja, founder and consulting analyst with Taneja Group, a consulting and research firm. But what happens if you don't know exactly how much storage space you're using today? Take an inventory. For example, anything that contains customer information—databases, contact directories, invoices—should be saved for at least seven years. Likewise, if you fall into an industry that has strict regulations, such as health-related fields or financial services providers, you'll need to store anything that relates to a customer's records. This means you'll be keeping e-mails, instant messages, contracts, and documents. And then there are your own employee and business records, as well as scanned documents, Web site or marketing elements, and banking records. All of these can mean the difference between being agile and falling behind.

"You'll also want to consider your overall business growth," says Schulz. "You can definitely correlate the resources you'll need with how fast your revenues are growing."

There is one more aspect you can consider when planning for growth: how much time and effort you're willing to put into actively deleting, pruning, and archiving your data. Those business owners who can commit to doing all of the above on a regular basis may not need to allocate as much money and disk or tape space for data growth.

"Pruning and archiving regularly will reduce growth, as well as the manpower and money needed to manage an ever-expanding pool of storage," Schulz says. "But unless you're willing to make the commitment, which most people don't have the time or energy to do, you'll need to plan for doubling your storage every six months to two years."

SHARE AND SHARE ALIKE

File sharing can make your life easier. It also provides additional storage options and gives you yet another tool in your backup arsenal. Here's what you need to know to do it correctly.

YOUR OFFICE. THE AIRPORT. HOME ON A SUNDAY NIGHT. These are just three of the hundreds of places you probably work as a small business owner. Doing so has never been easier with the ever-growing list of file-sharing products and technologies that let you access your own data, as well as that of your employees.

Removable drives, built-in operating system functionality, dedicated peer-to-peer file-sharing software, and a new breed of online productivity applications makes it easy for anyone to enable and use document and data sharing. So, for example, applications and data repositories such as Amazon Simple Storage Service, Symantec's Online Storage, Google Apps, IBM's Lotus Symphony, and OpenOffice, among many others, let multiple users access and share data and files over the Web without the need for local storage, while more traditional software applications such as the Microsoft Windows or one of the many Linux operating systems lets you access your company's files from wherever you are. If you're like most small business owners, you're already doing so, says one expert. The result: better access to your files whenever and wherever you want it.

File and data sharing has become more ubiquitous than people realize. In fact, in a small business, you're likely to be sharing files and not even realize it. The key is, if you are a small business, you probably have approximately 10 workstations and one main server set up as a file server for ease of use as well as convenience. This eliminates the need for each workstation to have to do its own backup—as long as the backup is set up correctly.

> "File and data sharing has become more ubiquitous than people realize. In fact, in a small business, you're likely to be sharing files and not even realize it."

Indeed, this byproduct—the fact that your files live in more than one place as well as the fact that you can copy files to another source should you start running low on space—is a reason to look into the technology. However, it's worth noting that if you are looking for additional storage space as well as a replica of what you've got on your main servers, there are several issues that you should consider before making a service or software choice. Version control—being able to have the most up-to-date version of a file—becomes murky unless the technology you're using automatically looks for and updates files regularly. Backup is also an issue, especially if users get into the habit of saving files only to a remote server. This means that, although the remote server functions as a data repository, you still need to back it up, too, or risk losing data.

When you're using an in-house file-sharing application, you can set up the server to automatically go out and back up all the files on the clients to the server. But if you're not backing up the data that's stored remotely, you could be missing critical information. You should set up your backup application or service to periodically pull data of those repositories, too.

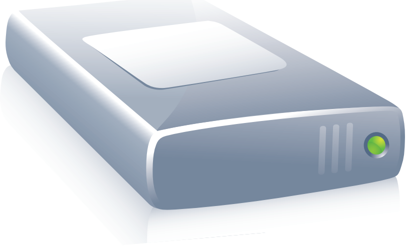
Transfer of data is also a concern, especially for sensitive files or customer information. If you're sending and downloading data over a public Internet connection, there's always the possibility that someone can intercept those files and use them for their own personal gain. A good fix: Make sure everything important that's sent or received remotely is also encrypted. Of course, no matter what file-sharing options you allow or use, there are other security aspects surrounding file sharing that most companies either overlook or forget about, including ownership and control. Both will be a big issue if your solution includes an online file-sharing site. Any data on that site doesn't live exclusively on your premises, and is no longer in your control. Best case, if the service goes down, so does your data. Worst case: From a control standpoint, it's very difficult—if not impossible—to set limits on who can view, alter or download your data if it doesn't live on an internal drive.

"Putting something on an online site makes it much less secure," says Greg Schulz, founder and senior analyst with storage research firm StorageIO Group. But this may be a moot point since even files that are copy-protected on your own site may be ripe for the picking, he says.

People can always do Control/Print Screen (which takes a copy of their screen) and then send it to a USB drive or smart phone. "Your best defense, maybe your only defense, is keeping key documents to yourself."

four

JUST THE (STORAGE) BASICS



Don't know how to get started with a backup and restore plan? You're not alone. Two experts weigh in on the very questions you're probably asking yourself.

IF YOUR DATA IS UNAVAILABLE, it costs you money—a lot of money, says Arun Taneja, founder and consulting analyst at research firm Taneja Group. "In terms of large businesses, the average cost per hour is in the $100,000 vicinity, but the range really goes from $50,000 an hour to several million dollars per hour," he says. "For smaller businesses, the range is between $25,000 to $30,000 per hour."

Clearly, having a data protection, backup and recovery plan in place is crucial whether you're a one-person show or a mid-size business with 300 employees. The good news is you don't need to spend a lot of money or time putting that plan into action, say experts.

Here are some of the most common questions about data protection and the answers to help you get started.

Q: HOW OFTEN SHOULD I BE BACKING UP MY DATA?

A: IT REALLY DEPENDS. There are so many different variables. If the data you're protecting is mission critical—you need that data to run your business and you'll be left twiddling your thumbs without it—you'll want to be backing it up often; possibly every time the data changes. Customer data is especially vulnerable since you not only need to have it backed up, but also encrypted, so if it falls into the wrong hands it can't be used against you. And of course, regulations come into play, too. If you are required by law to keep copies of specific data, that should be your first priority when laying out a data protection plan.

Q: HOW MUCH OF MY DATA SHOULD I BE BACKING UP?

A: TAKE A LOOK at the different types of data you're creating, consuming, and counting on every day. You've got documents, e-mail data, presentations, customer databases, applications, your operating system, financials—everything needed to run a business. But remember, business continuity requires more than just basic data backup, says Henry Baltazar, storage analyst with research firm The 451 Group. "Unless you own and keep track of all your application installation disks, you'll need to have at least one instance of your operating system and applications somewhere else in case you have a true hard drive or server crash," he says. Called a bare metal backup, this type of restore takes an exact snapshot of your operating system, applications, settings, and files. Companies like Symantec, Acronis, and FarStone Technology offer software that can facilitate this type of backup. You should do this at least once, and then again before installing something new.

A better recommendation would be to do a bare metal backup before installing something like a service patch or any new application. You can put it on a USB drive or a CD so if there's a problem you can just go back to what you had prior to the installation.

Once you've got your infrastructure backbone backed up you'll want something for your files. Again, if the files are really important—your company's growth will suffer if they are lost—consider an application or service that performs incremental backups, re-saving files every time they change.

Also, don't forget data that lives on devices other than PCs or laptops. You and your employees probably have important files on BlackBerrys, PDAs, online e-mail services, e-mail service provider databases, and software-as-a-service programs. All should be backed up periodically, too.

Q: WHAT TYPE OF BACKUP TECHNOLOGY SHOULD I USE?

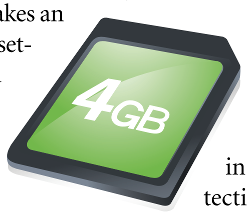
A: AGAIN, THIS GOES BACK to the importance of your data. Specifically, how quickly will you need to restore it should something happen? Online services and managed service providers do a great job in of storing data, but you may have to wait a while before achieving a full restoration. If you do it in-house, restoring from tape can be cumbersome and time-consuming. If you need data back very quickly, you probably need multiple copies on a media that can be used for fast reinstallations.

Online services are a good choice for people who have dedicated, high-speed connectivity such as a T-1 line; ISDN or cable modem service may be fine for smaller document downloads, but not fast enough for larger files.

Q: HOW DO I CHOOSE A BACKUP PROVIDER OR SOFTWARE PROGRAM?

A: THE OLD ADAGE that there is no free lunch definitely applies. Don't jump on a service or software just because it's the cheapest. Do your homework. Ask yourself, "In a disaster, what will I get back and how do I get it back? How do I get to my data? Do I need an intact PC to send it back to?"

Future growth should definitely be a consideration. Will the software and service grow with your company or will you need to start from scratch once your data reaches a certain size threshold? You may have a simple file server feeding data to 10 PCs today, but what happens when you're large enough to install a storage cluster? Or when that cluster becomes large enough to fill a room in a data center facility? Can you still get the same protection you have today?



PREPARING FOR THE WORST

Even the most careful backup plan sometimes goes awry. Here's what you can do if you lose everything.

You can back up all of your files daily or even hourly. You can keep an archive of tapes that goes back a year or more. You can even have a second server that replicates everything in near-real time. But every once in a while, something is going to happen that causes data loss. Sometimes, that something is technology-related; a server or disk dies. Other times, it's a human error or issue. Maybe your managed service provider—the company that's handling all your backups—goes out of business, or someone steals or misplaces your backup tapes. An even more common move: Someone overwrites a disk or tape, installs a program over an existing program, or deletes files accidentally. Viruses and spyware can also leave your hard drive in ruins—and inaccessible. The third option relates to the weather: Your data can be damaged or lost due to a fire or flood.

Data loss happens more than you think and it's not an easy thing to fix. Chances are, you will spend a significant amount of time and money trying to get some or all of your data back.

The good news is, it's not impossible. For example, experts were able to recover data from servers that looked like they were irreversibly damaged when Hurricane Karina hit. Even servers that were underwater for days contained information that was retrievable.

So what can you do if you've lost data? The first and easiest option is to examine your other resources for replicated data. Even if you aren't doing regular backups—and if you're not, you should be—you may be able to find what you're looking for on a laptop, BlackBerry, or old PC. Another possible location: remote or second office sites, which may use the same files you're looking for.

If that doesn't work and you're trying to retrieve a file that's been overwritten or one that's on a damaged drive, close all open software applications so you're not potentially overwriting the files yet again, and consider using a file restoration software program. There are many available options that are simple to use. These programs, including Migo Digital Rescue, Recover My Files, and Quick Recovery, look at your storage device and pull data from your file directory, even if you can't see it anymore. (Just because you delete something doesn't mean it's really gone, which is why you should always take care when disposing of old hard drives and storage products.) These products range in price from free to about $150.

And if you're still out of luck? That's when it's time to bring in an expert.

Companies like DriveSavers, Seagate Recovery Services, and DiskDoctors will take your hard drive to a clean environment, pop it open, and restore whatever they can get, which can be a fairly sizeable amount.

The downsides to this type of service, however, are price and time. It may take several days to several weeks, and you're going to pay several thousand dollars for the service. Unless it's a very important piece of data, you're probably not going to want to try and restore it this way. This is why it's far better to make sure you're doing lots of incremental backups and protecting those backups by sending them off-site whenever possible.

CONCLUSION:

WHAT'S YOUR DATA BACKUP STRATEGY?

Choosing the right option for your company is easier than you think. Here's a cheat sheet of pros and cons to help you get started.

DATA PROTECTION AND BACKUP ISN'T ROCKET SCIENCE, although it might seem like you need to be an engineer to make the right technology and media choice. Should you try and set up a backup strategy in-house? If so, do you go with a tape option or a disk-based solution? Maybe an online backup service is a better option for your company, you might think. Or maybe a managed service provider is the best choice; someone who will handle everything from figuring out when files and applications need to be backed up, as well as which technologies to use.

Whether you're looking to get started backing up your data or switch from a current solution, there's plenty to consider.

You've got to think about whether you're just looking for data backup—backing up the files you create every day—or if you're going to back up everything on your servers and PCs, including the operating system, system settings, and applications. You might want to be prepared for both a bare metal restore, where you can bring your entire machine back if your laptop or hard drive goes bad, as well as data restoration.

As for your backup media: this depends on your own technology comfort level as well as your willingness to take responsibility for your data. Tape backup is extremely cost-effective, but it's also slower than backing up to a second disk drive or array. And it's not always reliable, since people often forget to switch out tapes or the actual media fails.

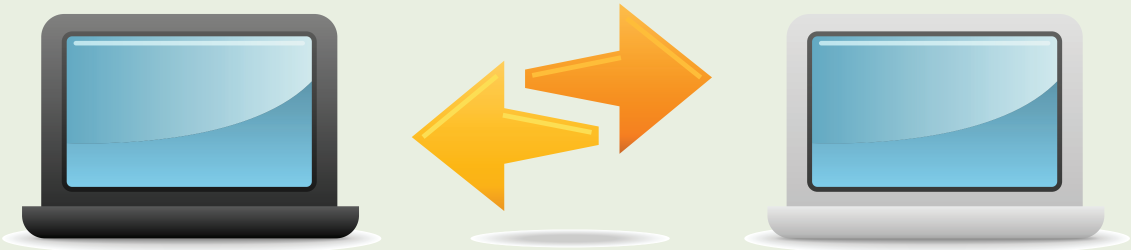
"We've found that, in many shops, up to 30 percent of all recoveries from tape fail," says Arun Taneja, founder and consulting analyst with the Taneja Group.

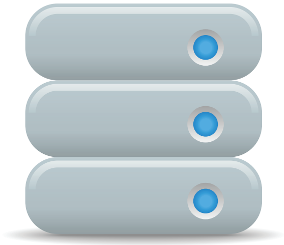
DVDs and CDs may be a good alternative, but you still run into the same problem of needing to take the media off-site for full protection.

Your best bet, agree experts, may be a mix of media. Backup to a remote storage server so you're protected if your original drive goes down, or you experience either a natural or man-made disaster. Backup infrequently used data to tape, and keep a second copy on an online service.

Once you've figured out which media type to use, figuring out how you'll get it all done is purely a matter of looking at the pros and cons of each option and deciding which is right for you. It's all a balancing act. You have to think about your threats, risks and needs.

Your task: Take a look at the security level needed, the speed of restore necessary, and how much you want to spend. Combined, you'll find the solution that's right for you.





Doing it In-House

PROS:

TOTAL CONTROL. You pick where, when, and how often you'll be backing up as well as what you're using to do so.

MOST SECURE. Your data doesn't leave your hands unless you want it to, so there's less of a threat of losing data to theft or outside system outages.

FAST RECOVERY. If your data is backed up onsite, you can theoretically restore more quickly than if you had to download it from an online service or wait for your managed service provider to come and do it for you.

CONS:

EXPENSE. Can be more expensive since you—or someone you hire—has to buy, manage, and take care of your backup option.

NETWORK PERFORMANCE MAY SUFFER. If you're backing up to an in-house server, your network may take a hit every time it's used to store incremental data changes.

POTENTIAL LOSS. Unless you follow through on your plan and execute backups, you won't be truly protected.

Online Option

PROS:

EASE OF USE. Most online services provide an application that automatically starts backups at specific times or when specific events occur, such as file changes. Some services also make manual file transfer easier by appearing as a drive in your Windows Explorer interface, so all you have to do is drag and drop your files to copy them.

PORTABILITY. Once something is copied to an online service you can get to it from anywhere you've got an Internet connection. This also makes it easier to share files between remote offices without the need for extensive networking capabilities.

CONTINUOUS DATA PROTECTION. Online services have agents that watch for changes and upload individual files or settings as they change, which means you always have the most up-to-date version of your data sitting out there waiting for you.

CONS:

CONNECTIVITY AND PRODUCTIVITY MAY SUFFER. If you're uploading to an external service, not only will your network connection lag, but your computer's performance may, too. You can avoid this problem by setting your service to update only when you're not doing resource-intensive tasks, such as transmitting large files or working with complicated applications.

EXPENSE. As with most software-as-a-service models, you pay for what you use. In the case of off-site storage, you pay by the gigobyte. The more you have to store, the more you're going to pay monthly or annually.

RESTORATION SPEED. If you do have a failure, you won't be able to get to your files without a live Internet connection. In addition, it can take days or even weeks to restore everything should you need a bare metal restore of your data.

Managed Service Providers (MSPs)

PROS:

NO THINKING INVOLVED. An MSP is going to do everything for you. You can hand off all the decisions and keep thinking about what makes you money: your business.

AUTOMATIC BACKUPS. Most MSPs buy hardware and software, install it and configure everything. They can often do manual backups remotely as well.

BEST-OF-BREED OPTIONS. MSPs, which function as resellers, often benefit from volume discounts that small businesses can't achieve on their own. The result: better pricing with the best providers out there.

CONS:

SECURITY. Unless you're dealing with a large MSP, there's always a chance your provider may go out of business or be acquired, which can result in data loss or security breeches.

RESTORATION SPEED. If you have a problem, you'll need to call your provider and get them to retrieve your data and either send or bring it to you. This may take at least a day or so, if not weeks, depending on your service level agreement.

LESS CHOICE. Since MSPs are usually resellers, they may have an agenda, pushing you to use the service they get the best margins for selling.