

 SearchDataBackup.com E-Guide

Get More Out of Your Data Protection Plan

Every storage pro is looking to do more with less, especially in today's economy. This eGuide offers the practical advice storage pros need in order to get more out of their data protection plan, an increase overall IT efficiency.

Sponsored By:





Get More Out of Your Data Protection Plan

Table of Contents:

[Data Protection Trends for 2009](#)

[Free and easy ways to speed up your backups](#)

[Backup 101: Seven tips for better SMB backups](#)

[Resources from HP](#)



Data Protection Trends for 2009

Lauren Whitehouse

Looking back on 2008, data protection/data backup saw several noteworthy trends. The factors that elevated some technologies over others were driven by a tenuous business climate and initiatives that focused on efficiency, cost savings and environmental sustainability. Some of the issues IT organizations faced, not surprisingly, included:

- Data growth. Enterprise Strategy Group (ESG) estimates annual data growth at 50% to 60% per year for many organizations. Collaboration, the use of messaging systems and copies made for data protection all contributed to organizations' capacity glut. The inability to keep pace with data growth added pressure on already-strained backup windows and/or recovery objectives.
- Volatility in global capital markets. ESG surveyed North American medium-sized businesses regarding the factors perceived as having the greatest influence on spending over the next 24 months and "internal pressure to reduce overall costs of doing business" ranked second in factors impacting IT infrastructure decisions. IT organizations, accordingly, were faced with reprioritizing and postponing projects, reducing capital and operational budgets, and oftentimes working with less staff to get it all done.
- Green data storage initiatives. Social responsibility has been less of a driver than the power, cooling and space efficiency challenges forcing "green" initiatives in companies of all sizes. These initiatives aim to reduce costs, improve the environment and create new business opportunities by eliminating waste, conserving energy, reducing carbon footprints, and taking new approaches to the development and marketing of products and services -- often relying heavily on IT to help meet goals.
- Compliance and litigation support. Compliance has become a business imperative for most organizations because failure to meet regulatory or governance requirements can lead to severe penalties, legal sanctions or damage to a company's reputation. Organizations have been challenged to develop standard operating procedures that include comprehensive electronic records management programs and information privacy practices, in addition to preparing for audits to prove compliance.
- Risk mitigation. ESG research found that IT spending will be closely aligned with initiatives that support or protect the business. In addition to improving backup and recovery, survey respondents indicated that their top three IT spending priorities will focus on improving business processes, decreasing costs and bolstering security controls in an effort to reduce risk.
- Dynamic and complex IT environments. Organizations have been undergoing dramatic changes and nowhere is that more evident than in IT. In an effort to expand globally, maintain competitiveness and increase revenues, organizations have adopted new technologies to improve IT infrastructure. Therefore, IT is challenged to not only maintain the status quo, but to continually refresh and improve technology infrastructure investments.

ALTERNATIVE THINKING ABOUT DATA PROTECTION:

Get a world of data protection from a single backup system.

The HP StorageWorks 2502i Backup System gives you more than just disk-based backup with rapid restores. You get a complete data protection storage solution. At 2 TB and 50 MB/s, you can significantly reduce your backup window. HP Dynamic deduplication lets you retain up to 50x more data for instant access. Integrate the system into your existing tape environment and get the best of both disk and tape technologies. With HP, protect your data and it will protect you.

Technology for better business outcomes

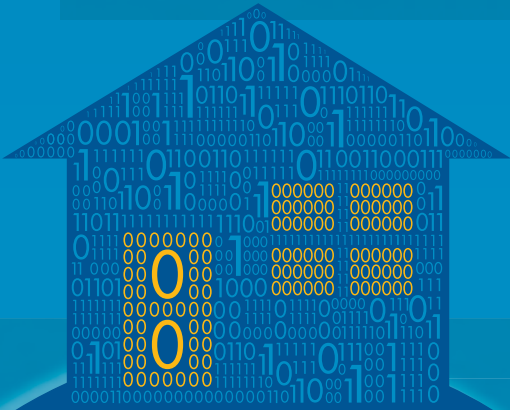
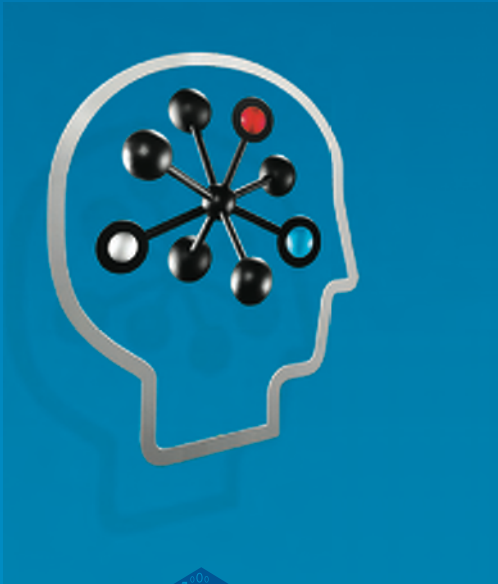
2502i Backup System

Designed for small or mid-sized data centers and distributed environments

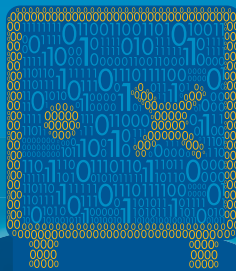
2 TB disk storage in a 1U rack-mount form factor

2 iSCSI interfaces

50 MB/sec performance with deduplication and low bandwidth replication



BACKUP AND RESTORE



ARCHIVING



DATA DEDUPLICATION



ENCRYPTION

How can HP help you provide complete data protection?

Get the white paper at hp.com/go/datadedupe



Free and easy ways to speed up your backups

Rich Cook

The first step and the most time-consuming part of inexpensive data pruning is setting the criteria for what you want to prune and what you want to do with it.

The first step and the most time-consuming part of inexpensive data pruning is setting the criteria for what you want to prune and what you want to do with it.

The next step is to decide what you want to do with different types of files and then set criteria such as length of retention for the different categories. It may turn out that all those JPEGs cluttering up everyone's disks aren't just collections of naughty pictures, for instance, and simply banning JPEGs from backups will create more problems than it solves. It might be better to use a single-instance storage scheme for all those charts saved in JPEG format rather than trying to eliminate JPEGs altogether.

Also, as is usually the case with anything directly affecting your end users, there's a certain amount of social engineering involved in making changes and seeking input is an important way to build consensus.

Once you've quantified the kinds of data you're dealing with and their uses, you can start cutting the size of your backups. Here are several free and easy things you can do right now to reduce your backup windows.

Eliminate the obvious

A good deal of what is saved to disk doesn't need to be backed up at all. Things like temp files and internet caches seldom need to be backed up. This may amount to less than a gigabyte per user, but the size adds up and it's easy to automatically eliminate file types from your backup.

Get rid of non-business files

Video files need to be watched very closely. If there's no business reason for having avi files or YouTube videos, then don't back them up.

Use single-instance storage

Many modern backup programs allow you to store multiple instances of a document just once. This is especially useful for attachments, which tend to be large and have multiple copies within the organization. Most of the major backup vendors have products that support data deduplication.

Establish reasonable retention policies

Don't keep stuff you don't need. While some data must be retained for compliance regulations or company policy, most data has a definite lifespan. Once a file ages beyond usefulness it should be eliminated from storage, or at the very least not backed up any more.

Emails are a particular problem because most users turn their mailboxes into filing cabinets, saving messages for a year or more. It is safer and more efficient to require that email be moved to another directory after, say, 90 days. Why is this safer? Because email applications are archiving and they were never intended to be. They're not designed or structured for long-term retention and it can be hard to recover a specific message from an email "archive" in the event of a crash.

Archive your data

According to a ClearPath Solutions Group study approximately one-third of the data being stored by a typical company hasn't been accessed in 180 days or more. That data may need to be retained (or maybe not, see previous point), but it probably shouldn't have to be backed up regularly. By transferring the data to an archive, it can be saved once and eliminated from the regular backups.

Setting policies: Cutting your coat to fit your cloth

In setting backup policies it's important to match your goals to your resources. That is, if you are seriously constrained on your backups, you need more rigid policies on retention, time periods and such. When setting policies be sure to allow for expected growth in backup size, even with the new policies in place, and adjust your quotas and such as needed.

Backup 101: Seven tips for better SMB backups

While the backup needs of small-mid-sized businesses (SMBs) are essentially the same as those of enterprises, there are some important differences that should be considered. Because budget and technical expertise are frequently strained in SMBs, an effective backup strategy must take those issues into consideration. The following tips can help you make successful backups.

Do it!

The most important habit of effective backup is to make effective backups. "Effective" means regular backups of all the information you need to preserve at the appropriate intervals.

This is especially critical with remote sites and corporate laptops. These systems are harder to oversee and it's easier to let backups slide. But if they contain important information, they need to be backed up.

Keep in mind that mirroring is not backup. Neither is imaging on the same system. Just because your array has two copies of your data doesn't mean it is completely protected.

Also remember to back up more than just the data. If you don't have copies of your configuration files, program patches and system state information, you are, at the very least, in for a lot of work if you need to do a full restore.

Image it

Today, there's simply no reason not to have a current image of your system instantly available. Most backup software will take images at pre-set intervals. A number of specialized programs offer more sophisticated abilities and Windows does this by default.

A system image isn't the same as a full backup, but it can handle about 90% of the things you need backups for, like restoring files or folders that were deleted by error or somehow corrupted.

Automate it

The more human involvement you have in your backups the more likely they are to fail. Although human error is usually listed as the second leading cause of backup failure after media problems, a lot of problems with media, such as improperly handling tapes, are actually caused by human error as well.

At the very least you should automatically back up your system on a regular schedule. Most backup software will let you schedule backups and you should replace the products that don't with ones that do.

Prune it

At the same time, you don't need to back up everything on your system. Most of what's there, such as .tmp files and browser caches, doesn't need to be saved at all.

Pruning your data reduces backup times and saves media cost, but it does require a little more work to decide which files and folders you need.

Duplicate it

One copy is better than no copies, but it still isn't really secure. The depressing fact is that a lot of backups can't be restored when needed. By having more than one copy of your data in backup, you increase your chances of being able to get all, or most, of your data back.

You need at least two copies, although they don't necessarily have to both be current. One common scheme is to keep the last two full backups as well as the partial backups.

Store it — safely

At least one full copy of your data should be stored securely away from your system. That way you can be sure of having your data even in the event of a disaster.

That means at least one copy of your last full backup is stored offsite in a place where it is available 24-7 (a safety deposit box at your local bank doesn't qualify). For a lot of SMBs, this means the offsite backup goes home with someone. This isn't as good as using a secure, always-available repository, but it's better than nothing. If you use this strategy, be sure the backup is encrypted before it leaves your premises.

If you have systems in two or more locations, another strategy is to send the backup copy over a WAN or the internet to another system.

Test it

In backups, ignorance is not bliss; it's an invitation to disaster. Just because your backup software says it has successfully created a backup, doesn't mean you're going to be able to get that data back when you need it.

To make sure, you need to test your system by restoring all or part of the image from the backups at regular intervals. One good way to do this is to create a separate partition on your system and restore to it for testing. Another way is to restore it to another machine.

This is an important test because if something happens to your computer, you'll have to restore to another system to make sure you can do it without any setbacks. Again, your backup software should provide facilities for this.

Resources from HP



[HP Dynamic Deduplication - achieving a 50:1 ratio](#)

[Integrating HP Data Protector Software with HP Data Deduplication Solutions](#)

[HP Simply Business Protection: Reliable Data Protection for Business Continuity](#)

About HP

HP is a technology company with 321,000 employees operating in more than 170 countries. HP is the second-largest technology services company in the world.

For 69 years, HP has helped people, businesses, and communities around the world simplify technology experiences. HP's three business groups drive industry leadership in core technology areas: The Personal Systems Group (business and consumer PCs and devices); The Imaging and Printing Group (printing, digital photography and entertainment); The Technology Solutions Group (business products). HP is a global leader in blade servers and distributed system management software.

HP is among the world's largest IT companies; with revenue totaling \$118.4 billion for the four fiscal quarters ended October 31, 2008. In 2008, HP was number 14 on the Fortune 500 list. The company's corporate headquarters are located in Palo Alto, California.

