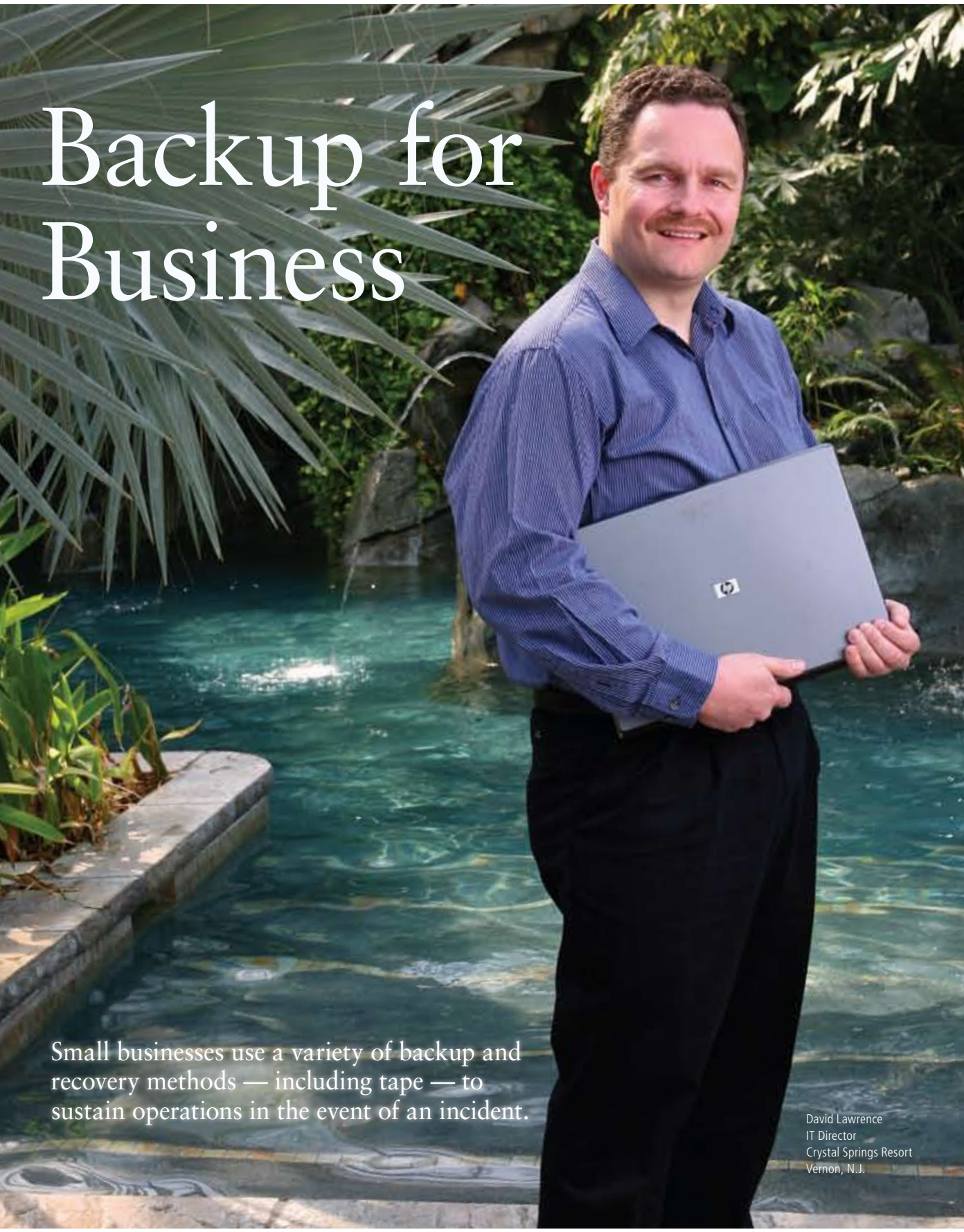
Backup for Business



Small businesses use a variety of backup and recovery methods — including tape — to sustain operations in the event of an incident.

David Lawrence
IT Director
Crystal Springs Resort
Vernon, N.J.

Today's businesses generate more data than ever before. The computerization of everything from e-mail to BlackBerry communication to million-dollar transactions has resulted in an ever-increasing mountain of digital bits needed to keep a business running.

While the importance of data is seldom debated, many businesses have not sufficiently prepared for data loss with effective backup and recovery planning. In fact, recent studies show that automated backup and recovery is one to the areas where small business is falling short.

"Small businesses face a number of persistent challenges, such as little-to-no IT support, not enough time to perform consistent backups and the pressure to have zero application downtime," says Siobhan Lyons, corporate communications specialist at Seagate Technologies.

Today, smaller companies are looking for cost-effective and appropriately sized backup and recovery platforms. Fortunately, there are next-generation technologies, along with proven processes that have been around for years, available to deliver effective backup and recovery.

Crystal Springs Resort

Striking just before a distant third data center came online, a significant data recovery failure stung the sprawling Crystal Springs Resort complex in Vernon, N.J.

"The recovery challenge demonstrated our data protection strategy was antiquated and lacked capacity," recalls David Lawrence, IT director for the four-season mountainside getaway. "We were only backing up our most critical data and user files regularly."

Complicating matters for the two-person IT team was its reliance on nontechnical personnel to initiate nightly backups. "If something didn't work according to the written procedure, then the backup just wouldn't occur," Lawrence says.

Crystal Springs needed to improve its backup reliability and consistency without adding overhead. The answer: automating backup-tape handling with an autoloader.

Automating tape backups makes sense. Performing unattended backups using an autoloader means less human intervention, which reduces the likelihood of a failure. And, it provides more capacity, which means more terabytes for less money.

Familiar Ground

For Crystal Springs, the impending completion of its new data center added urgency to the late-2008 security refresh. The resort was fast-tracking its data protection project, so it was important to stay on familiar ground with respect to backup software, Lawrence adds. As a Symantec Backup Exec user, the firm wanted a compatible tape automation device from an industry-leading manufacturer.

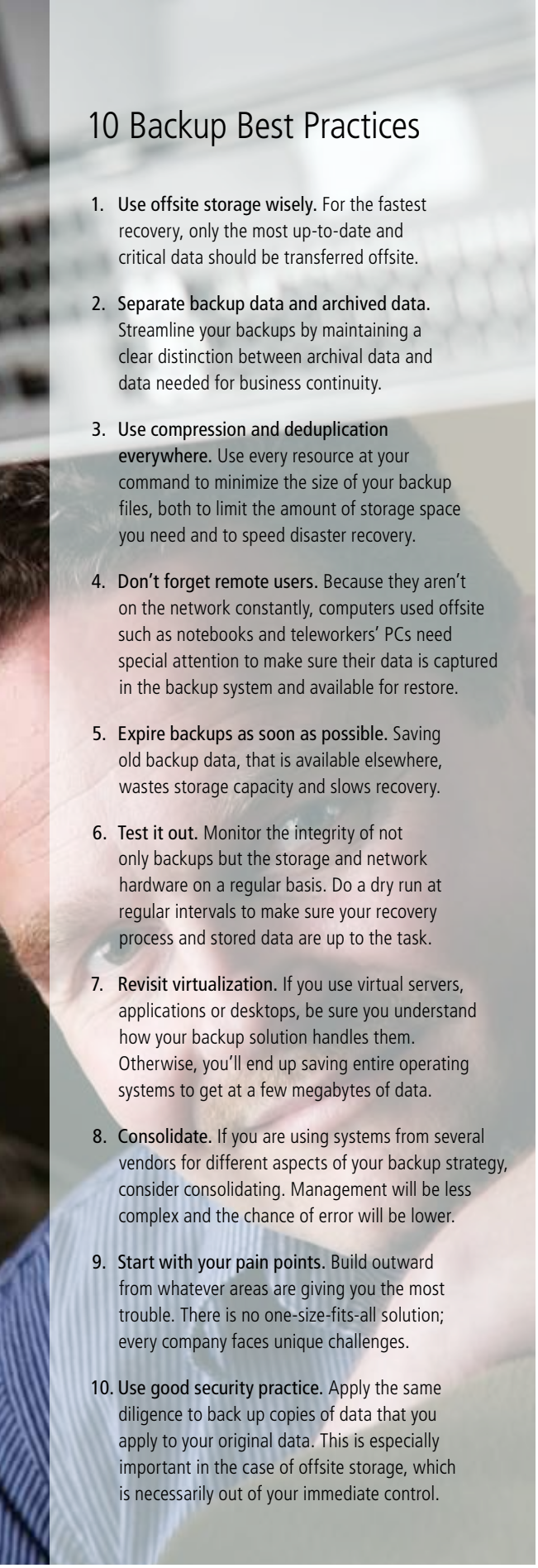
Another consideration was tape technology. Lawrence says the company looked at LTO (Linear Tape-Open)-4 for its speed, but settled on LTO-3 because it couldn't justify the added cost.

With software and tape specs set, hardware evaluation followed. Crystal Springs chose the Quantum SuperLoader 3 because an eight-tape magazine holds up to 6.4TB of compressed backups. Plus, the solution permits adding a second 6.4TB magazine in the future.

During the backup-technology planning and selection process, file server insufficiencies also surfaced. Ultimately, the company purchased three new 2TB file servers, one for each data center, and then developed a strategy for replicating the data using Microsoft's Distributed File System.

A Quantum SuperLoader was placed behind each of the three file servers to manage backups. Although the autoloader installation went smoothly, complications with other system components stretched the overall deployment into mid-January 2009.

Once completed, data security enhancements proved phenomenal. "Since we've removed the manual tape changes, backups don't fail," says Lawrence. "And, with the Quantum devices automatically performing a six-day tape rotation, we're fully backing up each server, daily." >>>>



10 Backup Best Practices

1. **Use offsite storage wisely.** For the fastest recovery, only the most up-to-date and critical data should be transferred offsite.
2. **Separate backup data and archived data.** Streamline your backups by maintaining a clear distinction between archival data and data needed for business continuity.
3. **Use compression and deduplication everywhere.** Use every resource at your command to minimize the size of your backup files, both to limit the amount of storage space you need and to speed disaster recovery.
4. **Don't forget remote users.** Because they aren't on the network constantly, computers used offsite such as notebooks and teleworkers' PCs need special attention to make sure their data is captured in the backup system and available for restore.
5. **Expire backups as soon as possible.** Saving old backup data, that is available elsewhere, wastes storage capacity and slows recovery.
6. **Test it out.** Monitor the integrity of not only backups but the storage and network hardware on a regular basis. Do a dry run at regular intervals to make sure your recovery process and stored data are up to the task.
7. **Revisit virtualization.** If you use virtual servers, applications or desktops, be sure you understand how your backup solution handles them. Otherwise, you'll end up saving entire operating systems to get at a few megabytes of data.
8. **Consolidate.** If you are using systems from several vendors for different aspects of your backup strategy, consider consolidating. Management will be less complex and the chance of error will be lower.
9. **Start with your pain points.** Build outward from whatever areas are giving you the most trouble. There is no one-size-fits-all solution; every company faces unique challenges.
10. **Use good security practice.** Apply the same diligence to back up copies of data that you apply to your original data. This is especially important in the case of offsite storage, which is necessarily out of your immediate control.

Backup Technology

There are vast arrays of data backup solutions available. The question is how do IT captains choose the right infrastructure to move their company forward and address its biggest pain points?

According to Lauren Whitehouse, a senior analyst at Enterprise Strategy Group of Milford, Mass., the speed and reliability of a backup system factors into two measurements needed when planning a business backup and recovery strategy: recovery time objective (RTO) and recovery point objective (RPO).

RTO is a measure of how long a company can afford to function without access to a particular application or data set. For example, a busy medical office might be able to manage without its accounting data for a day or two. However, it may grind to a halt without immediate access to patients' medical records.

RPO indicates a business's tolerance for data loss and again may vary depending on the type of data and the amount lost. Losing an archive of marketing materials might be painful but not crippling. However, going even an hour without having access to customer orders might be impossible to recover from.

Answering these types of questions with a company's business model in mind will lead to some data backup techniques over others. Some techniques will meet some criteria better than others, and some will be more expensive than others.

Cost and Speed

Disk-based storage is growing, especially for higher-value data that must be retrieved quickly. That's in large part because of the combination of lower cost and more advanced technology, says Pete Steege, senior product marketing manager for Seagate.

That speed is important for two reasons. First, it is almost impossible for most businesses to function without access to their data and applications. So the longer it takes to restore from a backup, the longer the business's livelihood is on hold.

Second, the ability to back up data quickly means that applications that generate a steady stream of vital information, such as files on an e-commerce server, can be backed up as fast as they are producing data — even in real time if necessary.

For especially time-sensitive applications, such as a web-based application that serves hundreds or thousands of customers at any given time, even a few minutes of data loss can be disastrous. It can bring irreversible damage both to the bottom line and a business's reputation.

Continuous data protection (CDP) systems can mirror high-traffic, high-demand applications and their data in real time. The technology is designed to keep an up-to-the-second copy of everything and restoring in a flash if something goes wrong.

"For your highest-priority applications where you can't afford to lose data, continuous data protection is the only technology that will solve that problem," says Mathew Lodge, senior director of Symantec's information management group. "Every time a change is written to disk, you replicate that change to another site."

70%

of small businesses that experience a major data loss will be out of business within a year, yet only one in four small businesses regularly back up their files.

SOURCE: HP and SCORE

Deduplication Strategy

Backup and recovery speed are also increased by the use of deduplication. This technology can significantly reduce the amount of data written and read from a backup drive.

Deduplication works by comparing data at the bit level, examining each block within a file to see if it contains strings of bits that have already been saved elsewhere. If so, it replaces the redundant data with a placeholder pointing to the original data.

For example, every time you send an e-mail you create a copy of your signature block. In a traditional backup scenario, that data is saved again and again, once for every message sent out. With dedupe, a backup saves the block once and will only save it again if you change the original.

Although deduplication reduces the size of individual backups, it also reduces redundancy between subsequent backups. "When it comes time to backup," explains Shane Jackson, director of product and channel marketing for EMC Data Domain, "I only need to push the changed data.

"If nothing's changed, the deduplication system effectively says, 'I've done a full backup, and you already have all the data,'" he adds. This speeds each backup because there's less data to write to disk and also makes recovery quicker, especially from offsite locations because there is less data that must move over the Internet.

Take It Offsite

Offsite storage is an important part of any business's backup strategy. "If there's a fire, if there's a theft, if they have an employee that was disgruntled or they had a flood, there's no onsite protection in those cases," says Jay Remley, vice president of product management and business development at Seagate.

WAN optimization, high-bandwidth connections and fast backup software (usually with built-in dedupe) make it possible to move gigabits or even terabits of data to remote data centers and recover from a disaster. And it can be done almost as quickly as if local hard drives are in use.

For businesses with multiple locations in several states, data replication — from one location to another — offers the benefits of offsite backup. It's also an effective way to leverage a company's existing storage capacity.

Businesses with only one location, or several locations close together, can still benefit from replication. The firm might want to consider storage at third-party data centers in other geographic areas to gain protection from a large-scale disaster.

Putting It Together

Often, a small business has a small IT staff — sometimes even a single IT employee. Therefore, it pays to invest in backup systems that offer a high degree of automation and easy manageability.

Some businesses will have relatively simple backup needs. For this, Seagate's BlackArmor line of network storage servers, such as the NAS 440, offers automated backups of computers and servers on the network at regular intervals and can restore whole systems or individual files as needed.

For more complex business situations where a mix of long-term storage, low-priority data and immediate real-time protection are necessary, software-based products such as Symantec Backup Exec and CommVault Simpana offer flexibility and centralized control.

With CDP functions for applications such as Exchange servers and SQL Server databases and auto-archiving to tape drives, these products allow businesses to create a set of policies that can be applied automatically across various applications and data sources that make up a typical business environment.

For most small businesses, the easiest, most flexible and most affordable storage option is a network-attached storage device such as the Iomega StorCenter ix4-200d or Buffalo TeraStation series. A NAS is a plug-and-play server holding two, four or more hard drives accessible across the network.

Both the Iomega and Buffalo NAS systems can be configured in a fault-tolerant redundant array of independent disk (RAID) configuration. That way failed drives can be replaced without data loss — perfect for backup.

Building a Backup Strategy

Putting together the right combination of tools to meet the backup and recovery needs of a small business is not difficult. However, it requires a holistic view of the organization and the different kinds of data generated.

RTO and RPO are valuable metrics for establishing the priorities of the various applications in the business. Technology resources can be balanced and apportioned in an efficient manner and seen not on their own, but relative to overall business objectives.

Consider backup and recovery another facet of a business's uniqueness. And don't be afraid to revisit the issue as the business grows. "Backup strategies are determined based on the needs of the organization as a whole," says Enterprise Strategy Group's Whitehouse. "Organizations — and requirements — evolve. So should data protection." ◊

Discover how data backup solutions from CDW can help you retrieve lost data and keep operations running seamlessly.