

By Erik Eckel

Takeaway

Automated backup programs greatly simplify administrative tasks. However, it's possible to become overconfident in an automated backup. IT Consultant Erik Eckel reviews 10 things about automated backup programs that could save yourself and your organization from a recovery nightmare.

Automated backup

Automated backup programs, whether used to create local backups or copy data offsite via high-speed Internet connections, greatly simplify administrative tasks. Properly configured, automated backups -- including [Remote Data Backups](#), [Spare Backup](#), [Dr. Backup](#), [Yosemite Backup](#), Windows NT Backup and [Symantec/Veritas Backup Exec](#) -- ease not only an administrator's workload but peace of mind.

Eliminating the daily pressure of having to manually back up an organization's critical data opens valuable time that can be dedicated to other responsibilities. However, it's possible to become overconfident in an automated backup.

Alaska officials, for example, recently [revealed](#) a computer technician accidentally deleted data on a hard drive. Seemingly no trouble, the case took a bad turn when, attempting to recover the data from a backup tape, the state found the media unreadable. Recovery costs are estimated to exceed \$200,000.

Review the following [ten things](#) to know about [automated backup programs](#). They could save yourself and your organization from a similar nightmare.

1

Tapes aren't trustworthy

It's a sad truth. Many expensive tape backup systems fail when needed most. What's worse, many tape failures are never caught. Whether it's a case of a tape drive requiring cleaning or media failing over time, often tape errors aren't caught until too late. Just ask Alaska's Department of Revenue, whose \$38-million oil account (including 800,000 electronic images) had to be painstakingly rebuilt by more than 75 employees because backup tapes proved unreadable.

2

Tape maintenance is dicey

In addition to tape drives and tapes themselves proving questionable, even proper-operating media are only as good as the operator. Unless administrators and others charged with rotating the actual tapes complete the task on time using the correct media, tape backups can prove worthless. Even veteran IT professionals occasionally insert the wrong day's tape or confuse recovery sets. For this reason it's important that schedules and media are carefully monitored and tracked.

3

Data locations change

Data locations move and change over time. For example, an organization's public relations files might originally be installed within a server data folder labeled PR. Following an acquisition, a new storage strategy might be implemented in which those same PR documents become part of a Marketing folder. The same thing happens with databases, e-mail accounts, user directories, departmental archives and other data. Unless backup operations are updated every time data storage locations change, backups run the risk of missing critical data.

4

Backup operations occasionally fail

Just because a backup operation is scheduled does not mean that backup procedure will complete. Electrical outages occur. Thunderstorms intervene. Backup media fills. Backup drives get dirty. Systems freeze. The list of elements that could derail a backup is unending. Thus, you should never consider backups covered just because they've been scheduled. Instead, make reviewing backup logs a daily routine. Better yet, make restoring backups to test their efficacy a regular event.

5

Backups back up bad data, too

When backup operations complete properly, they tend to complete exactly as programmed. Backups don't care if whole directories or partitions have been deleted since the last time they ran; backups usually back up what they're told to back up. For this reason, administrators should not depend upon a single backup set. Users occasionally mistakenly delete whole folders and directories, but sometimes require several days to realize the error. If your organization is working with only a single backup set updated daily, the likelihood of recovering the erroneously deleted data decreases every day. Maintaining multiple backup sets (or performing differential backups throughout the week) provides organizations with additional options for recovering data.

6

Databases, exchange require TLC

Many applications -- including those that depend on Microsoft SQL Server and the Microsoft SQL Server Desktop Engine (MSDE) to power their data -- store their most critical information within multiple database files. Unless the complex instructions that link the information between those databases in meaningful ways is also backed up, just having those database files saved to a backup drive won't enable successful restoration. Be sure to follow the manufacturer's backup guidelines when working with such third-party software.

Exchange servers require special treatment, too. E-mail servers require applications that can perform online backups, as it's impractical to assume an organization could down e-mail servers during specific windows daily just to complete backup operations. Instead, organizations must ensure their backup applications support online or active operations. In the case of Microsoft's popular e-mail server, such programs are described as being Exchange-aware.

7

Some apps work better than others

Many vendor promises amount to sweet nothings; not all products work as promised. Some applications fail to back up all the files, folders and drives you specify. Others perform a differential backup even though you called for an incremental. Still others fail to properly write data to specific media or don't complete within reasonable time frames.

Worse, competition within the online backup space results in many providers going out of business. Often firms go under with little notice and take your data with them. So, shop carefully when considering software manufacturers and online providers. Reputation and reliability typically outweigh cost savings when selecting a backup partner. Whenever possible, don't forget it's a best practice to first test an application before deploying within a production environment, too. Doing so helps reveal anomalies and incompatibilities before damage can be done.

8

Documentation is critical

The best defense against data loss, and a crucial component of any disaster recovery plan, is documentation. Only by documenting which systems are backing up what data and when (and where that data is stored) can an organization have confidence its critical data is properly protected. In addition to tracking this information, documentation should provide instructions for testing backups to ensure the backup sets enable proper recovery.

9

Proper backup strategies require regular reviews

Data locations change. Often, documentation doesn't keep pace. As a result, it's easy for an organization's backups to begin tracking the wrong data. IT departments can help prevent disaster by scheduling regular reviews of its backup strategy. Scheduling quarterly meetings to review backup strategies can help ensure backup operations keep pace with organizational changes.

10

Security is easily overlooked

Once data is committed to a backup that does not mean the data's safe, there is security to consider. Headlines are rife with stories of sensitive data slipping the hands of couriers or being misplaced or even stolen. Since backups often contain confidential and protected information, companies must take pains to protect not only the principal data but the backups, too.

In fact, depending upon the industry within which the organization operates, legislation may require special steps be taken to protect backups from public release. Be sure, when extending backup and restoration privileges and handling backup media that appropriate steps are taken to guard against unauthorized access. For online backups, this means ensuring the provider supports 128-bit encrypted data streams (and a separate encryption key for recovery).

Additional resources

- [Subscribe to TechRepublic's Downloads RSS Feed](#) [XML](#)
- Sign up for TechRepublic's [Downloads Weekly Update newsletter](#)
- Sign up for TechRepublic's [Storage NetNote](#) newsletter
- Check out all of TechRepublic's [free newsletters](#)

Version history

Version: 1.0

Published: April 11, 2007

Tell us what you think

TechRepublic downloads are designed to help you get your job done as painlessly and effectively as possible. Because we're continually looking for ways to improve the usefulness of these tools, we need your feedback. Please take a minute to [drop us a line](#) and tell us how well this download worked for you and offer your suggestions for improvement.

Thanks!

—The TechRepublic Downloads Team