EXECUTIVE SUMMARY

BACKUP AND ARCHIVING: A PERSPECTIVE ON THE FUTURE

Why many CIOs are treating backup and archiving strategies separately—and saving bundles of money

Research conducted by

CXO MEDIA

CIO
Custom Solutions Group

Sponsored by

DIGITAL™ IRON MOUNTAIN

Executive Summary

With all eyes on the future, smart CIOs are taking a long, hard look at their backup and archiving strategies—and asking a lot of tough questions.

What data needs to be recovered? How quickly must that recovery occur? What data must be accessible in the event of litigation? How granular must access be? What's to be gained from indexing?

But the all-important question is this: Should backup and archiving strategies differ?

Yes, according to a recent survey by IDG Research Services. More than half of the respondents recognize key distinctions between backup and archiving, and reveal very different reasons for doing each one.

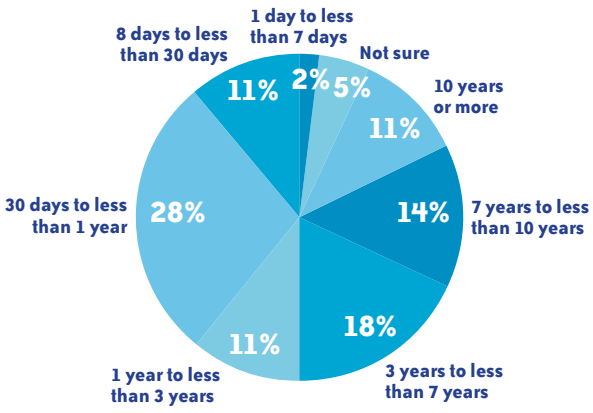
The study proves that forward-thinking enterprises have reached an evolutionary stage in their backup and archiving strategies, and are no longer thinking about them as simply "storage problems." Rather, they are evaluating all their data and making strategic decisions based on specific business needs.

"These innovators are deploying backup and archiving tools, sometimes separately, sometimes together, but always informed by business value, data accessibility and protection," says Tom Mackowski, vice president of digital product management for Iron Mountain. "And they're reaping the rewards, saving money by optimizing technology to their data needs."

Still, this IDG survey uncovers interesting—and, in some cases, disconcerting—trends in backup and archiving strategies. Some of the highlights include:

- 51 percent of respondents recognize a difference between backing up and archiving data, while a full 30 percent see no discernable difference.
- 67 percent currently back up everything; 23 percent archive everything.
- 42 percent of those that do archive consider their backup to be their archive.

LENGTH OF TIME BACKUP DATA IS RETAINED



Q: How long does your company typically keep backup data?

Base: *107 qualified respondents*

This report explores these telling statistics, with expert commentary regarding current and future perspectives on data storage, protection and retrieval.

A REALITY CHECK

Whether for a developer of aerosol technology for portable inhalers like Chrysalis Technologies or an educational institution comprised of 90,000 students like Portland Community College, ever-increasing pressure regarding competition, compliance and continuity mandate the utmost in data accessibility.

There is no question behind the value of data backup and archiving. CIOs need to make sure data is available to whomever needs it, whenever they need it, and however they need it, even when something goes wrong or when the data in question is several years old.

This certainly comes to bear in a recent survey by IDG Research Services for which senior IT executives report that the driving forces behind both backup and archiving initiatives are securi-

ty/access to data and the ability to recover a file or system to a specific point in time. Rightly so, respondents reveal very different motivations behind the two strategies.

30 percent of respondents see no discernable difference between backup and archiving.

"B" IS FOR BACKUP

Backups are for recovering data. Indeed, the top reasons cited for backing up data are disaster recovery (92 percent) and business continuity (85 percent), while issues like compliance and litigation risk mitigation are considered less important. Whether recovering from a simple system outage, an inadvertent user error or some form of catastrophic natural disaster the likes of Hurricane Katrina, business must go on. That's why 67 percent of respondents currently back up everything. In so doing, CIOs zero in on two key metrics: how fast they can recover data, meaning their recovery time objective or RTO; and at what point in time they can recover it (one week, one day, one hour, etc.), meaning their recovery point objective or RPO. In some cases, continuous backup may be warranted to address aggressive RTO and RPO requirements.

When it comes to backups, the value lies in "staying in business," says Leslie Riester, associate vice president of technology solution services at Oregon's Portland Community College. The college's backup strategy was designed to keep it from losing more than 24 hours of updated data, 12 hours on a critical day, for instance, when financial aid data is due. "Being unable to restore our primary databases would be catastrophic," Riester explains. "We are lucky that none of our systems are crucial to health and safety [like a hospital], but our students' lives can be adversely affected by losing their records." In a worst-case scenario, Portland Community College must be able to restore "old" data, so timely backups are critical.

Similarly, at Chrysalis, there is substantial value associated with maintaining "a fluid and flexible record backup process" for disaster recovery purposes. "A disaster does not have to equate to your facility being destroyed," says Andy Villers, solutions delivery architect for Chrysalis, a division of Philip Morris USA. "It could be something as simple as accidentally deleting records or a SCSI drive array failing." The point is that Chrysalis must be able to recover data to an acceptable level, within an acceptable time frame.

"A" IS FOR ARCHIVING

In contrast, archiving pertains to access to data in a searchable or retrievable format over long periods of time. The top reasons cited for archiving data are, not surprisingly, compliance (77 percent) and litigation risk mitigation (66 percent). Other issues, such as disaster recovery and business continuity, rate lower. Of those respondents that perform archives, 77 percent keep only their critical data—that which is more likely to require access in the long term. With archiving, CIOs are most concerned with the speed and granularity of data access. These metrics directly reflect the stringent expectations associated with today's regulatory climate and eDiscovery mandates, making data access at the item level an absolute necessity.

INDEXING, THE LITTLE-KNOWN SECRET TO SAVING MONEY

Only 38 percent of the IDG survey respondents indicate that their company's archived data is indexed. This seemingly benign factoid indicates significant risk, especially when it comes to eDiscovery for compliance and litigation requirements.

With regulations like Rule 26, the demands around data access and response time have increased dramatically, and CIOs need to address those demands. "Your legal team reasonably can't work with thousands and thousands of unclassified documents," says Tom Mackowski. "On the other hand, properly classified data can turn a lawyer's nightmare into a courtroom opportunity."

Then there's the potential impact on the bottom line. In addition to the time and resources expended in an inefficient eDiscovery process, enterprises can face significant fines for being unable to adequately respond to compliance and litigation requests. Mackowski says that some enterprises are "spending in the neighborhood of 2 to 5 percent of gross revenue in eDiscovery."

"When it comes to archiving, CIOs need to get serious about classifying their data and records," says Mackowski. "Indexing is absolutely critical to the speed and accuracy of access, and is proving to be the little-known secret to saving money."

For example, Portland Community College only archives data needed for institutional research or legal requirements, meaning federal and state records retention laws. Given this driver, it is important for the institution to be able to retrieve specific documents or records with accuracy. "Archives are in a 'frozen state,' and need to be locked to ensure they don't change," says Riester.

Villers of Chrysalis concurs: "In archiving, it's important to be able to trace the lineage of records." There are instances, he explains, when certain records must be provided to interested parties while "demonstrating the integrity and authenticity" of those records—even if they are decades old. Businesses need to set the value of archiving by providing an appropriate retention schedule and clear expectations of long-term archival. Villers differentiates archiving from backups based on retention times. "Backups are transient and temporary while record archival would potentially require much longer-term, possibly permanent retention," he explains.

THE DISCONCERTING TRUTHS

Despite these acknowledged differences, backup and archiving tactics are often used interchangeably, and sometimes without clear understanding of the business needs. In fact, although a strong 51 percent of the respondents recognize the distinction between the disciplines, there is still an alarming 30 percent who don't yet acknowledge the difference.

For example, some 42 percent of respondents claim that their backup is their archive. However, of the 58 percent that do archive separately, the strategy for a full 23 percent is to simply archive everything, not just critical data with potential legal or compliance implications. This reveals two disturbing trends in that many companies are still treating all data the same and that many are keeping unnecessary data for too long. It appears that a good number of respondents recognize the need for archiving, but are unfortunately missing some of the benefits and cost savings that come with a more disciplined approach to data management.

"Some enterprises cling to the idea of convergence of backup and archiving strategies because both challenges are seen only as 'storage' requirements that can be solved by relying solely on storage solutions," says Mackowski.

Oftentimes, this is just a natural by-product of politics, meaning divisions within an enterprise may solve the data storage, protection and retrieval issue in different ways. For example, an IT decision maker responsible for disaster recovery or server backup might solve archiving-related problems with backup solutions, while an email database administrator might be more likely to resolve a business continuity need with an archiving solution.

"Clearly, CIOs need to be able to distinguish between what needs to be backed up and what needs to be archived for a more direct approach to treating data differently," explains Sasha Willoughby, senior manager, product management for Iron Mountain. That's definitely where the future of data storage, protection and retrieval is headed, as indicated by a majority of the respondents.

HOW MUCH DATA IS TOO MUCH?

Survey respondents indicate that they're storing a lot—perhaps too much—data:

- ✓ 67% backup everything.
- ✓ 23% archive everything.
- ✓ 42% don't archive separately from backup.
- ✓ Backup data is kept for an average of 3.6 years, while archived data is kept for 6.1 years.
- ✓ 31% have no method in place for the regular destruction of backup or archived data.
- ✓ 62% say they're storing more data than necessary.

A good rule of thumb, says Iron Mountain's Tom Mackowski: "Keeping any data you don't need is keeping too much." CIOs need to optimize their storage policies to their business needs, he says. If not, they're missing out on substantial cost savings—and no one can afford to do that.

MAKING GOOD BUSINESS SENSE

"In the end," says Riester of Portland Community College, "data backup and archiving will always be about good business practice."

But what constitutes good business?

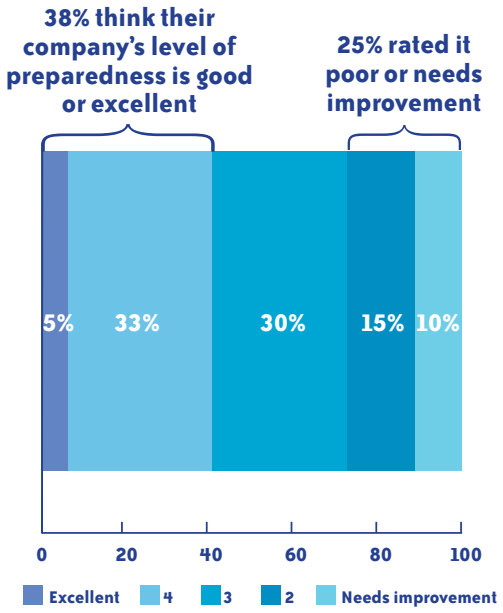
Mackowski says that can be easy to come by, and offers some practical advice for developing winning backup and archiving strategies going forward:

- ✓ Look at all data and make informed decisions based on business value, data accessibility and protection requirements.
- ✓ Consider the information life cycle, the importance and purpose of the information throughout its life cycle, the likelihood of future retrieval requirements and its role in regulatory mandates.
- ✓ Evaluate backup and archiving as discrete but complementary needs to optimize storage.
- ✓ Continually reevaluate backup and archiving policies, including the definition of "critical data."
- ✓ Consider automated online options for continuous protection of critical servers (for example, remote offices).
- ✓ Use indexing to classify data so that business-critical information can be segmented appropriately for backup or archiving.

All of this requires a methodical evaluation of business needs and thoughtful selection of solutions based on those needs. "You mustn't fall back on backup strategies as the answer to every storage challenge," warns Mackowski. "Nor should you rely on archiving as a catchall to any potential future need for data access."

42 percent of respondents say their backup is their archive.

LEVEL OF PREPAREDNESS TO RESPOND TO LITIGATION REQUESTS



Q: Please rate your company's preparedness in terms of its ability to respond to a litigation request today on a scale of 1 to 5, with 1 being "needs improvement" and 5 being "excellent."

Base: *107 qualified respondents*

The key lies in optimizing storage to unique business needs in order to minimize storage requirements and maximize effectiveness—a CIO's dream. Without optimization, enterprises may be spending too much money backing up too much data for too much time. "When you look at backup and archiving as discrete but complementary needs, you can shorten the storage window and lower the overall cost of data management," says Mackowski. "That's a win-win all the way around."

CALL TO ACTION:

If you would like to learn more about Backup and Archiving, please visit **www.ironmountain.com/digital**