DATA BACKUP
AND RECOVERY

DATA ARCHIVING:

10 COMMON MISTAKES (AND HOW TO AVOID THEM)

Are your supposed **archiving best practices** actually costing your company time and money? Read on to discover the 10 worst things to do (or not do) with your enterprise data backups – and **how to mend your errors.** ▶

IRON MOUNTAIN®

THE DON'TS ARE ALWAYS MORE FUN

It's a quirk of human nature: The mistakes of others – whether they're fashion flaws, home improvement mishaps or social faux pas – amuse us, and make for great TV and magazine fodder. But that amusement may turn to shock when you recognize your own mistakes in those shows and articles.

Luckily, no one's going to be doing a TV show anytime soon about data archiving blunders. But if they did, would your company be in the spotlight? Ask yourself these questions as you think about the answer:

- **"Should we adopt a DIY backup strategy?"** Even if your company currently lacks the resources to support an offsite data vault, sending the IT director home with a backup tape each night isn't a great Plan B.
- **"Is it time to upgrade?"** Saying "we've always done it that way" is no excuse. If your company's data backup technology hasn't been updated in a while, it may be time to upgrade.
- **"Who created our retention policy anyway?"** Just because the company lawyer or your law firm crafted your policy, don't assume that it's rock solid. Unless your counsel really knows your business, immerse yourself in compliance issues, or consider tapping the expertise of a trusted archiving partner to guide you.

Mistakes, you've seen a few. But then again, not too few to mention. Having an archiving plan should be simple, but data backups can go wrong in so many ways. Here are the 10 most common mistakes and what you can do to avoid or remedy each.

1. FAILING TO TEST BACKUPS

Perhaps you've heard a horror story like this: A company dutifully makes daily tape backups. Then, after experiencing a loss, it tries to recover its data, only to find blank and/or corrupted tapes. Yes, drives can fail. And if yours isn't recording properly, you'll need to know about it sooner rather than later. Test recorded tapes regularly to eliminate unwelcome surprises.

2. HAVING ONLY ONE BACKUP

If a server fails, you don't want to rely on a single tape or set of tapes. Create a system that automatically creates a backup of your backup. Why? Because the more redundancy in your backup and recovery plan, the greater your peace of mind.

3. FAILING TO CHECK TAPE LOGS

If there's a problem with backup, such as a group of files not being recorded, employees who aren't well-versed in the system might not spot the error. That's why it's critical to study the log files for each recording; they'll be your first line of defense when a problem occurs.

4. KEEPING TOO FEW BACKUPS

Sure, space is at a premium, and you may not want to store your backups indefinitely. But it probably isn't good enough to keep only a few weeks' worth or to warehouse the bare minimum. Why? First, a discovery or audit request can send you way back in time to grab information. Second, your backups may become corrupted, so the more backups you store, the greater your chance of recovery. The best defense is to create both long-term and short-term backup policies.

5. KEEPING TOO MANY BACKUPS (A.K.A. FAILING TO IMPLEMENT A RETENTION POLICY)

Some companies save everything, but that's usually a waste of space. You'll know what to save if you develop a retention policy – a formal plan to preserve information. Consider that different types of data may call for different policies.

6. NOT RETAINING OLD EQUIPMENT

When you're upgrading equipment, you may find that a new system doesn't support your old backup materials anymore. In that case, you'll need to hold onto the previous generation of hardware, at least temporarily, in case you ever need to read those older files. Even better, plan to re-record archived information every 10 to 15 years to guard against tape degradation and data corruption, and to keep up with newer technology. Be sure that everyone in your organization knows why your company is storing those older drives, so they aren't accidentally discarded.

7. TAKING A CASUAL APPROACH TO SECURITY MEASURES

Make sure your security measures protect your data, but don't lock out your team from access. For instance, if you were to ever leave the company suddenly, does anyone else on your IT team know the passwords needed to access your backup media? Or at the other extreme, have you created generic authorizations for data access? It's best to be as specific and discretionary as possible about who gets access to what (and under what conditions).

8. LEAVING DEPARTMENTS OTHER THAN IT OUT IN THE COLD

Running backups might be your IT department's responsibility, but that doesn't mean you can (or should) leave other departments out of the archiving process. Be sure to solicit input from R&D, marketing or any other relevant group for your archiving plans. You'll learn how they create data, what information they need access to and what special legal concerns they have regarding data retention.

9. MISSING OPEN FILES

When your colleagues leave their computers on night after night, they're quite possibly leaving files open, too. And most data backup systems don't address active files. To guard against this potential backup gap, create a policy that requires employees to close all files each night – even if they insist on keeping their computers running.

10. DISCOUNTING AN OFFSITE TAPE VAULTING STORAGE OPTION

If you're storing your backups locally – even in a fireproof safe – you're not getting total security. A safe can't protect your data against all perils. Even if your information does survive a natural disaster, for example, what if you can't get to the office to retrieve it? To protect your business, choose an offsite storage partner to whom you'll send your tapes regularly.

IRON MOUNTAIN SUGGESTS

Keep on Top of Archiving

Create internal systems to ensure that your company's backing up the right data at the right times. Here's how:

- **Know what data to protect.** Gather information from all departments. Make sure all managers are heard. Learn what data should be stored and for how long.
- **Develop multiple redundancies.** Make more than one copy of everything. And be sure that material is stored on your premises for quick access, as well as offsite for longer-term needs.
- **Assign tasks to designated leaders.** Ensure that everyone concerned with data storage knows and understands his or her responsibilities.
- **Team with a trusted partner.** Solicit the help of an offsite data backup and recovery specialist to support all of your requirements. An experienced partner can make regular pickups, provide convenient access and store your tapes in climate-controlled vaults. Working with an expert partner means you'll spend less time defending your data backup and recovery procedures to internal or external auditors.

HOW TO LEARN MORE

Do you have questions about data backup and recovery? **Read additional Knowledge Center stories** on this subject, or contact Iron Mountain's Data Backup and Recovery team at 800-899-IRON (4766). You'll be connected with a knowledgeable product and services specialist who can address your specific challenges.

RELATED ARTICLES

- **A Best Practices Checklist for Backup Tapes**
- **Far from Home: Keeping Data Safe, No Matter Where It Travels**
- **The (Business) Day After: Making a Double Rebound from Disaster**

ABOUT IRON MOUNTAIN. Iron Mountain Incorporated (NYSE: IRM) provides information management services that help organizations lower the costs, risks and inefficiencies of managing their physical and digital data. Founded in 1951, Iron Mountain manages billions of information assets, including backup and archival data, electronic records, document imaging, business records, secure shredding, and more, for organizations around the world. Visit the company Web site at www.ironmountain.com for more information.