i365
A Seagate Company

Solution Brief

12 Best Practices for Data Backup and Recovery

1. Reliability. Up to 71% of restores from tape contain failures.

Best Practice: Use disk-to-disk technology for backups. With disk-to-disk technology, your backup data resides on disk drives, proven to be far more reliable than tapes. When your backup completes, you know the data is secure and accessible on the disk drive. With tapes you never really know if your data is usable until you try to restore it, at which point it's too late.

2. Breadth of Offering. Choice in product and service offerings meet your business' needs.

Best Practice: Don't settle for less than what you need. Vendor offerings vary widely. Some are designed primarily for consumers and others for enterprise data centers. Choose a solution that scales (see scalability below), and offers the features you need to provide the level of service you expect. De-duplication and delta-block technologies will improve performance, reduce your data footprint and save you money. Find out if their de-duplication offering is at the file level or the block level. Make sure the solution can back up servers, PCs, and laptops as well your applications.

3. Security. 60% of organizations using tapes don't encrypt their backups.

Best Practice: End-to-end encryption with no "back door." Using encryption with tape makes backups run slowly and often takes too long to fit within a backup window. As a result, most people simply turn encryption off, creating a security risk. Even with the physical safety of disk-to-disk backup, encryption is essential. Look for 256-bit AES. Find a solution that encrypts your data during transmission and storage. Make certain there isn't a "back door" that would let someone else view your data.

4. Accessibility. Companies waste thousands of hours waiting on tapes.

Best Practice: Ensure that you can get your data back with minimal delay. You should have direct access to your backups, with no time spent on physical transport (no trucks, no warehouses). Your restores should take minutes, not hours or days. Set yourself up to work with your data, not wait for it. Make sure your solution provider can meet your Return-to-Operations (RTO) and Recovery Point Objectives (RPO) which determine how quickly you can recover your data and maintain business continuity. Inquire about onsite and offsite replication that provide both improved performance and a solid disaster recovery strategy.

5. Scalability. Some backup systems can't scale readily.

Best Practice: Invest in a data protection architecture that can grow with your business. You should be able to back up your data no matter how large it grows. Starting small? Look for an option that handles your backups automatically. Then, as you grow, gives you tools to manage complex environments. Look for "changes-only" and compression technologies to speed backups and save space. And insist on bandwidth throttling to balance traffic and ensure network

availability for your other business applications. Make sure that their solution offerings rely on common technology to scale easily as your business—and data—grow.

6. Cost-effectiveness. Companies lose an average of $84,000 for every hour of lost activity.

Best Practice: Calculate the true total cost of tape-based back up. When you do the math, the dollars make sense: Go with disk-to-disk. Unlike tape, there are close to zero handling costs—no rush deliveries, loading, accessing, locating, or repeated steps. And there's one benefit you can't factor directly: Reputation. Reliability and security can make an incalculable difference with just one avoided breach or failure.

7. Compliance. Most companies have problems satisfying privacy, security, and data retention regulations.

Best Practice: Choose a data protection partner who has deep know-how about compliance, and the technology to ensure it. How do you recognize a strong compliance partner? They'll gladly show you a table of regulatory requirements, and list for you how their products, services, and technology help you satisfy them. Even better: Use a vendor who successfully completes an SAS-70 Type II audit every year which helps you comply with regulatory requirements.

8. Disaster Recovery. Most companies lack a comprehensive, tested plan for disasters.

Best Practice: Find a vendor that delivers a complete DR solution. You can't say your data protection is complete until you have a disaster recovery plan that is itself complete and tested. Your backup vendor should have both the product mix and professional services team to help you prepare for a worst-case scenario. Make sure they can help configure your backups so you rebound quickly. Best bet: A vendor who can train you to deal with disasters confidently, based on your company's actual configuration.

9. Ease-of-Use. Some companies don't —or can't—manage their backups from one place.

Best Practice: Get control and reporting you can use anywhere, with ease. Managing your backup environment should be simple, and the software you use should eliminate any guesswork that could lead to lost data. You should know at all times if your data is protected across your entire network—including remote offices—by simply looking at a dashboard. The software should be simple to configure using wizards, yet powerful enough to meet your specific needs with customizable views, job propagation, and roles-based security.

10. Operating System and Platform Support. Most backup vendors support a limited range of OS, server types, and applications.

Best Practice: Look for broad and deep technology that supports your complete environment. Your backup solution should accommodate your environment, not vice versa. Demand a single solution to protect your laptops, desktops, and servers regardless of the platform and applications they're running. Beyond the broad claims, check the fine print, and the level of protection offered for applications such as Exchange. For example, can they restore individual mail messages or contacts, and can they support Exchange running on a Microsoft Cluster?

11. Customer Support. Backup vendors' product support varies widely.

Best Practice: Find a vendor whose support is passionate, maybe even slightly obsessed. Customer support should be one of your vendor's main selling points. You shouldn't have to wonder if they'll be there to help when you need them most. Do they offer phone support or email only, are they available 24x7, and who exactly are you talking to when you call that 800 number? Find a vendor that will treat your data as if it were their own.

12. Reputation. Does your backup vendor have a quality reputation and the financial resources to stay in business for the long haul?

Best Practice: Find a vendor with strong financial backing and customer references. There are a lot of vendors that have come and gone. When you consider a service provider, look for one that has strong financial backing, a solid business plan and the ability to be in business as long as your data needs to be stored. Ask for customer references and case studies as their customers are the best validation you can get.