EVault®
A Seagate Company

White Paper

Beyond Technology: Backup and Recovery Best Practices

Best-practices backup and recovery programs extend beyond the data protection technology to incorporate people and processes.

Consider This Before You Call Your Backup and Recovery Plan Complete.

Data connects you to customers, suppliers, and partners, and drives decisions at all levels of your organization. Without data, your business is dead. So you need a backup and recovery solution that protects your data and systems from all threats.

If you're like most IT experts, you'll focus first on the technology. You'll make sure you have the hardware and software to perform backups. You'll build out the required storage, making sure you have floor space and power in a data center, and so on. Next, you'll tier your systems: What data is most critical? How often does the data need to be backed up?

Beyond the backup and recovery technology, however, you'll need to consider the expertise required to create, maintain, and execute a backup and recovery plan. What team should you have in place? What type of communication and cross-functional planning do you need? What are the program deliverables, milestones, and proof points?

Backup and recovery is not a "set it and forget it" proposition. By definition, it's a living entity—an ongoing program that you regularly test and refine to match your evolving environment (infrastructure, staffing), policies (security, compliance), budget, and needs.

Read on to learn about the four best practices for achieving a successful backup and recovery program: assigned ownership, managed expectations, rigorous audit preparation, and a recovery team with a deep bench.

Best Practice #1: Assigned Ownership

If everyone owns the task then no one owns it. Designate one person in your organization: often an IT manager—to own your backup and recovery program. This person may not perform the actual operations, which are often handled by a backup or network administrator, but he or she will maintain the plan. The owner is also responsible for scheduling recovery tests and reporting on the organization's readiness to respond to various disaster scenarios.

The owner needs the backing of senior IT management, who should make the program a top priority and support it with a budget for necessary tools, testing, and travel.

Real-Life Lessons in Backup & Recovery

The Responsibility for Keeping Pace with a Rapidly Changing Environment

Let's look at what can happen without assigned program ownership.

Six months after an insurance company created a full data protection plan, it conducted an operational assessment—and learned that its well-constructed plan was useless. New servers and applications had been deployed, but hadn't been noted in the plan document. Plus, the new servers' retention policies weren't up to corporate standards, so the system was out of compliance the moment it was implemented.

This haphazard approach had put the company at risk because it lacked a comprehensive, documented plan for fast data recovery across its critical servers following a disaster. A designated owner tasked with keeping the plan current, viable, and effective would have known about the infrastructure upgrades and would have planned appropriately.

Best Practice #2: Managed Expectations

You've established your backup and recovery strategy, you've set target recovery time objectives (RTOs), and you've tested your ability to meet those targets. Now, what about service-level agreements (SLAs)? Your business partners need realistic expectations, based on the results of a thoroughly tested plan, for how quickly the organization can recover from a disaster. And you need to commit to meeting those expectations.

These SLAs and testing results should be communicated, at least quarterly, during an IT operations review meeting. This gives your stakeholders insight into recovery processes and confidence in your ability to get the business up and running after a disaster.

Real-Life Lessons in Backup & Recovery

No SLAs = Lost Credibility

What happens when you don't establish and communicate realistic expectations? The IT team at another insurance company learned the hard way.

At the time the company lost its Lotus Notes server, expectations were that the service would be back online within one hour. Unfortunately, the IT team had never tested its ability to recover the server, nor did it have the necessary secondary hardware, software, or data to quickly perform a complete operating system recovery. As a result, the team severely underestimated the actual recovery time.

The business owners, understandably upset, had to recruit third-party consultants to help with the recovery, causing the internal IT team to lose a great deal of credibility. The moral of this story: establish, verify, and document your RTOs—commit to them and communicate them—and test, test, and retest your data protection plan.

Five Keys to a Successful Backup and Recovery Program

1. Treat your backup and recovery plan as a living tool—own it, update it, prioritize it.
2. Establish and communicate real-world RTOs.
3. Prepare an audit toolkit.
4. Expand your capabilities by partnering with your IT services provider.
5. Test, test, test.

Best Practice #3: Rigorous Audit Preparation

To pass a regulatory audit, you must prepare at least one month in advance. Ensure that your data retention and encryption policies comply with industry regulations. Verify that your backup and recovery plan is up to date. Test your ability to recover data and document the results. When you walk into the audit, make sure you have a fully stocked audit toolkit that includes your plan, passwords, and recovery tools.

During the audit, you'll have to demonstrate your data recovery plan—how you recover specific files and folders, move data offsite, and recover data from that offsite location—and provide a copy of that plan. The auditor will verify that your offsite backup location and data retention scheme meet regulatory standards and that you can meet your RTOs.

Real-Life Lessons in Backup & Recovery

How to Pass an Audit with Flying Colors

A recent audit of a bank demonstrates the value of being prepared.

The IT team was required to show how the bank's data was backed up offsite. The team verified the data encryption policy and demonstrated the process to access the backup data. Finally, it demonstrated file restores at multiple retention points (last month and last quarter)—and easily passed the audit.

Best Practice #4: A Recovery Team with a Deep Bench

Data recovery is a team effort. Assign a primary owner to put the recovery plan in motion, but don't put your organization at risk by relying on one person to perform it. Expand the team and guarantee that multiple people within your organization know what to do in case of disaster.

You can build the extended team from your own IT organization or bring in outside experts. One advantage of using an outside vendor is that they won't be subject to the onsite stresses of an outage, allowing them to better focus on a rapid recovery. Task your vendor with designing your backup and recovery solution and you'll know the vendor's support team will be prepared to bring it's insider's knowledge to bear in an emergency.

Real-Life Lessons in Backup & Recovery

The Right Team Is First to Recover

Consider the example of a small bank affected by Hurricane Katrina.

The bank had decided to forego tape backups, sending its data directly to an offsite location out of the region. When the storm hit, the bank's business was taken offline but its IT team was able to get to a location that had Internet access. With the help of its backup service provider, the team rebuilt its IT environment in a remote data center in Atlanta.

Because the team had collaborated with its provider well in advance of the catastrophe, the bank was prepared and had the resources it needed to recover. It was one of the first businesses to be up and running in the New Orleans area after Hurricane Katrina.

How EVault Can Help

EVault®, founded in 1997, is the industry's most experienced cloud backup service provider. Our data protection platform was built from the ground up to deliver optimal performance in a distributed environment: efficient bandwidth usage, minimal storage footprints, end-to-end security, and more. We offer cloud-connected™ deployment—spanning onsite and cloud locations—so you get fast onsite backups and recoveries with reliable offsite disaster protection.

Together with our partners, we are with you every step of the way. We can help guide your deployment, service your everyday operations, and act as first responder when things really go wrong. In fact, we're the only truly full-service backup and recovery provider—no other vendor can match our breadth of solutions or level of service.

Consider EVault Managed Services....

To ensure a successful backup and recovery program, many EVault customers choose the EVault Managed Services option. You get a dedicated team of experts that will learn your business and then help construct a data protection strategy tailored to your needs. The team will manage and monitor your EVault deployment. With regular reporting and consultation sessions, you will know that your backup and recovery plan is accurate and up to date. And if problems occur, you get streamlined support from a team that knows your environment and can help speed your recovery.

EVault Managed Services helps you:

- Build a comprehensive, living data protection plan, based on real-life objectives your team can stand behind
- Get ready to pass audits
- Expand your recovery team so you can meet your SLAs—on time, every time

...And Start with a Free Assessment

EVault Managed Services can get you started with a data protection assessment that reviews your infrastructure and recovery plans. We'll help you establish appropriate RTOs for mission-critical systems and applications. Then, if you choose to work with us, our team can design and implement a customized data protection solution and test it end-to-end for all systems under contract. You'll receive a fully documented plan—covering environment and recovery requirements, recovery steps, and disaster recovery test results—that you can share with auditors.

Take the Next Step

To learn about how EVault can help you implement a successful backup and recovery program, call us at 1.877.901.DATA (3282), email us at concierge@evault.com, or visit us at www.evault.com.

EVault®

Headquarters | 201 3rd Street | Suite 400 | San Francisco, CA 94103 | 877.901.DATA (3282) | **www.evault.com**
Netherlands (EMEA HQ) +31 (0) 73 648 1400 | **France** +33 (0) 1 55 27 35 24 | **UK** +44 (0) 1932 445 370

2012.08.0016_WP (updated 09/05/2012)