Retrospect

Planning for Disaster Recovery

A Retrospect Partner Best Practices Document

Aspects of disaster preparedness

Considering disaster recovery and what it means for a computer system (for example, being able to perform a bare-metal restore after a hard drive failure) is quite narrow in scope compared to thinking about disaster preparedness for an entire business, that is, ensuring that a business can be up and running again shortly after a fire, flood, theft or other circumstance. Questions that include, "Where will the employees meet and work," and, "How will we provide computers without waiting on an insurance company to mail a check," are valid concerns for developing a plan to come out of a disastrous situation on top.

Incorporating disaster preparedness planning into your services

Disaster preparedness is indeed so broad and complex a subject that entire businesses have been built around providing such services. Although outlining the tasks necessary to emulate such businesses is beyond the scope of this document, one thing is clear: IT service providers are in the best position to get their customers thinking about what must be done to ensure the survival of their business, and to provide services around ensuring ongoing IT functions.

At the very least, if even just to protect yourself and your business from unexpected data loss when working on customers' systems, you should have a comprehensive backup and recovery plan in place for each of your customers. Make such a plan a requirement, and in it detail:

- Initial planning and implementation
- Day-to-day management (running backups and restores, checking email notifications)
- Periodic maintenance and testing (archiving, verifying partial and complete restores)
- Reassessment as needed (system capacity, performance, technology, methodology, etc.)

The tasks listed above provide significant services revenue over time, and somewhere between 70-90% of a backup and recovery process can be duplicated from one client's environment to another, making it a mostly repeatable process. Decide what works, then set your clients (and yourself!) up for success.

Backup and disaster recovery plan best practices

Create and formalize a plan

We recommend that you formalize a backup and recovery plan for each of your clients. It should include things like your service-level agreement with response times that you can meet, what is your responsibility and what is theirs, measurements for success, and what ongoing services will be provided.

Offsite backup storage and recovery

Local backups are the best first line of defense against data loss, but it's critical to get at least one copy of an organization's data stored safely offsite, preferably at a location removed by several miles. Here are some things to consider regarding offsite backups:

- What data must be backed-up offsite? Can any data—such as cache files—be excluded?
- Should the data be encrypted?
- Where will the offsite data be stored?

- How will it get there? (Options: cloud backups, physical transportation of backup media)
- Who will be responsible for transporting physical media offsite?
- When will we have access to the physical media if we need it?
- At what interval will the offsite storage be updated?
- How long will older data be archived?

Build your system recovery toolbox

Every IT services provider should maintain an arsenal of useful tools. At a minimum, have the following ready at all times:

- Burn a Retrospect Emergency Recovery Disc for Windows systems.
    - Best when licensed with the Retrospect Dissimilar Hardware Restore add-on
    - Be aware of specific hardware requirements (like RAID and network HBAs)
- Create a bootable Tools Disk for OS X systems.
    - Include the Retrospect application, engine, and client
    - Add favorite Mac utilities (Disk Warrior, Tech Tool Pro, etc.)
- If any offsite backups are stored on tape, be sure you will be able to promptly source a drive to read those tapes, should the main tape backup drive become unusable for any reason.
- Make sure that you have access to any necessary passwords and keys! If the Post-it™ note containing your Backup Set password was under the keyboard* and just burned up with the rest of the office, you'll be in trouble without that password stored safely elsewhere!

Test, test, test

Even carefully considered disaster recovery plans need to be tested. Few things are more painful than discovering that things aren't working as expected when you're running a critical restore. Retrospect's design includes a unique data verification method that actually uses the same routines as when it runs a restore. That's great for ensuring that backup data is readable and exactly matches the original data, but successfully testing a proper restore is always the best way to maintain confidence in the system.

Put in place a plan to test restores at least quarterly for each of your clients. When you perform such testing, there are several tests that should not be overlooked:

- Search for and restore a file
- Restore a folder to a previous point in time
- Restore an entire volume and ensure that it boots, applications run as expected, etc.
- Check critical business application function (accounting, email, etc.) following a restore
- Restore from offsite backups

Besides ensuring the reliability of the backup system, testing restores gets you in front of your clients on a regular basis and maintains *their confidence in you*. It's a win-win procedure.

Start immediately; perfect over time

Whatever you do, don't wait to get your clients started with offsite backups until you have crafted the perfect plan. Get something offsite NOW. By their very nature, disasters both natural and man-made are difficult to predict or prevent. It's best to get at least one copy of your customers' backups stored safely offsite immediately. Then you can contemplate and implement over time a system that will provide a level of service that best meets your clients' situations and needs.

* Retrospect, Inc. does not condone storing passwords in anything less than a safe and secure manner.