Disaster Recovery Best Practices Start with Backup Compliance

By Richard Dolewski

Let's examine the most critical process in disaster recovery planning: our backups. No recovery is possible without saving the data in the first place. Disaster avoidance happens long before a disaster occurs, certainly not after the fact.

The System i (iSeries/400) backup process is a critical function to ensure business continuity for the system. The backups must be executed on a regular basis and must conform to strict controls. As the system administrator for your System i, you must have the ability to restore all of its data to a consistent usable state, thereby minimizing the impact to your business.

A Word on Compliance

As the complexity of our systems increases, compliance proficiencies demand that IT become accountable to both the users and to the business. The Sarbanes-Oxley (SOX) Act mandates governance for many of today's organizations. This act requires that procedures are executed routinely by System i system administrators. All must be audited annually to ensure that internal controls and procedures are always followed. A commonly used framework in the IT industry is CobiT (Control Objectives for Information and related Technology). To achieve this standard, IT departments are adopting a best practices framework in computing services to ensure they achieve these audit requirements.

The following are tips for meeting CobiT Compliance for Backups:

1. Develop a backup and recovery plan.
2. Establish a backup lifecycle program, that includes:
   - Success/failure reporting
   - Problem analysis, resolution, and signoff
   - Examination of backups which exceed backup window
   - Tape handling and library management
   - Bonded offsite tape storage
   - Weekly, monthly, and long-term backups
   - Archived data
   - Planned review of backup polices
   - Recovery testing and verification
3. Review backup logs daily.
4. Have a hot-box for vital records.
5. Have a process to identify orphan data.
6. Automate your backup process.
7. Integrate backups into a change control process.

"I Never Hear About Any Backup Issues"

The key element to maintaining compliance and avoiding recovery issues is to stay on top of your backups. Having a process in place means a lot more than simply signing your name. Your signature implies correctness, and means that you've adhered to all the necessary steps in verifying that the process is 100% complete. If the backups are incomplete or flawed prior to a disaster, then the disaster recovery plan simply will not work.

Many backup solutions are partially broken. I often observe graphs posted in IT shops stating that the department has a 97% backup success rate. This rate may sound impressive—sure, 97% on your high school math exam was amazing. You were on the honor role. But in the world of backups, this implies failure! It means that 3% of the time, the server or entire data center isn't backed up on any given night. On a yearly calendar, you have incomplete backups on 12 days. This means 12 days per year that you wouldn't be able to recovery your data. Is this acceptable to your business? This number gets padded as well. **Examples include:** "13 objects not saved. Oh, we always get this message… it's no big deal," you say, and sign off that the backup was successful. But was it successful? This is not a half full or half empty discussion. You need 100%!

Backup strategies reflect the critical nature of the data. A system outage should make you reflect on the methods used in backing up the data and how long it would take to restore that data—if at all.

Customize Your Backups

Always build your backup strategy based on your recovery needs. By determining what data needs to be protected, you can create and maintain a reliable backup system for your organization. Such a system will ensure a successful recovery from a disaster. Many best practices seem basic, but accomplishing them isn't always easy. They depend on a number of key elements, including appropriate reporting and measurement capabilities, and staff competency within the organization.

You do all this not only to pass the SOX audit; you perform these steps because your business depends on it. After all, what good is backing up data if you can't restore it when you need it? The bottom line is that it's no longer a question of whether data can be restored, but how quickly it can be recovered and how much data loss your organization can tolerate. It's about making sure that recovery time objectives (RTO) and recovery point objectives (RPO) match the true value of data at any given point during the business data lifecycle.

Make PR Part of Your Plan

Many companies have documented disaster recovery plans in place. We've all tested and re-tested our plans to ensure that every step is properly documented. Equally important, our recovery strategies are indeed complete for a successful recovery with minimal loss of data and downtime.

But have you considered the media attention you may get following a disaster? Are you prepared to face the press and the TV cameras when a disaster strikes? Who from your organization will face the reporters, and what will they say? More importantly, how will they say it? The last thing you want to see is your computer operator on the national news giving his opinions of what just happened. "It's a death trap in there," or "Nobody warned us," or "We never planned for anything like this," or worst of all, "We will never recover from this."

The moral: Don't let an unqualified employee share his or her fifteen minutes of fame in front of the cameras, or you'll be dealing with a public relations disaster as well as your planned disaster recovery.

Is Your Company Prepared for the Microphone?

There are several steps you can take to prepare pre-selected members of your recovery team to work with the media. Keep in mind that we have ourselves to blame for bad press, not the media. We are all thirsty for up-to-the-minute live information. And the media likes to report on the bad news versus the good news. So here are some very important things to consider:

1. It's important to decide in advance exactly who will speak to the media. Always assign one primary spokesperson and one alternate. When more then one person communicates with the media, it can create some inconsistencies in your story. That is the last thing you want to do.
2. Journalists tend to seek out the worst possible prognosis for your company. However, it doesn't have to be a picture of total gloom and doom. The savvy spokesperson should learn how to quickly turn around the very negative questions and reiterate their own positive comments and what the company has already done to improve the situation.
3. Practice this role just as you would your technical recovery. There are agencies available that will give you the "lights, camera, action" practice run, and even include a dozen microphones pressed up against you to train you in handling this type of pressure. This should be part of every passive disaster recovery test.
4. Answer all questions as directly and briefly as you can in a positive manner. Example: "Yes, we had a disaster and we are in the process of recovering all our mission critical systems… and yes, we will be serving our customers tomorrow."
5. Never lie… end of story.

It's inevitable that the public will hear your story; this is beyond your control. What you can control is how they hear it and the negative information the media may report.

Meeting audit compliance means you're observing disaster recovery preparedness. Preparedness is all about being recovery minded, not about being overly cautious or simply signing on the dotted line. CC

Richard Dolewski *is a certified systems integration specialist and disaster recovery planner. As Vice President for technical and contingency services provided by Mid-Range, he has extensive experience in disaster recovery planning, backup & recovery program design, and high availability. Contact Richard at rdolewski@midrange.ca*