TUG MoM REVIEW

THE JANUARY 2007 MEETING OF MEMBERS

By Jay Burford and Stephen Bingham

It was cold! The winds were blustery! But were the TUG members deterred by the daunting weather? No, we were not! We parked in the warmth of the underground parking lot at the Living Arts Centre Mississauga. Then we received an even warmer reception from the TUG "meeting and greeting" team: **Wende Boddy**, **Loretta Dryer**, and **Harry Hastilow**. What a way to start an evening of fun, friendship, and education! And later it was spiced up with a movie and even some "movie confessions".

The great turnout, despite the inclement weather, was a strong indication of the interest in the evening's two topics: "i5 Availability" and "DR & Security Confessions—The Movie". TUG President **Léo Lefebvre** welcomed everyone and advised the attendees that there would be a draw during the TUG Business Session, after the dinner break. He then introduced our first speaker, **Chris Hird**, President of Shield Advanced Solutions, who also works closely with Blair Technology Solutions Inc., to do a presentation on i5 Availability.

Photos by Léo Lefebvre

Afternoon speaker Chris Hird

Jay Burford

Stephen Bingham

i5 Availability

Chris provided a brief history on the tools provided on the AS/400 since its inception in 1988. Chris has been actively involved in the development of products such as JobqGenie, SPM Manager, CD Generator and FTP Manager. His presentation included a reference to a number of White Papers that are either currently available or else coming out shortly.

Chris likes to "think outside-the-box!" and CHEAP! He discussed "Remote Journaling & Recovery" and noted that while many people attempt to use this process as one method of HA, it is NOT really High Availability.

In V5R1, IBM introduced virtual optical and has now released Virtual Tape with V5R4. Both have the advantage of speed but have DASD considerations. As Chris explained, there are options to consider. Backing up to a virtual image, either Optical or Tape saves the time during the initial backup and avoids potential media errors that can interfere with your batch run. In the tests run by Blair Technology, they found no difference in speed between virtual optical and virtual tape.

Since virtual tape allows you to specify your tape type, you have more flexibility in the size of the image file, resulting in the need to change virtual images fewer times, if at all.

As Chris mentioned earlier, they specialize in "outside-the-box thinking". A great example of this is Remote DASD and an automated FTP process. Whether you

choose a LINUX FTP Server or an Intel Server, the cost of DASD is inexpensive and dropping. You can currently get a terabyte (TB) of disk for less than $800. Add a DVD/CD writer that supports the *UDF format and you are set.

Backup your files to a virtual optical image, then FTP the image file to the FTP server, and delete the image file from the i5 on successful completion of the file transfer. This eliminates the need to have all of the virtual images on the i5 at one time, reducing DASD limitations. Once the FTP images are on the FTP server, they can be written to CD.

You can use these images in one of two ways to recover your system. FTP them back from the server or restore them from your CD using the optical drive. Chris explained that a full system backup and recovery could be done using this method. NOTE: i5 OS (LIC) must be installed for a full recovery.

Léo Lefebvre

Chris Hird — "thinkig out-of-the-box," at the January TUG meeting

In V5R4, IBM introduced something called "WATCH Commands". These are monitors that allow you to monitor any message queue or even a job log for specific messages and take appropriate action automatically. These commands are used in the above process to monitor for error messages.

© The 5th Wave, www.the5thwave.com

Chris went on to discuss some possibilities for the next stage of optical backup, by saving to optical only with the use of some techniques for journal receiver storage, remote storage management and object replication.

He closed with the recommendations to keep looking for alternative methods. As IBM constantly gives us more access to the operating system, there are more options available to us if we just keep "thinking outside-the-box".

The MoM

During the break we all enjoyed an excellent hot buffet dinner while everyone took the opportunity to say hello to friends and acquaintances. Prior to the second presentation, Léo gave us a further update on the special MoM on May 30th (which is one week later than usual. Our special guest presenter will be **Randall Munson**, the winner of multiple "Gold Medals" as a speaker at COMMON.

Léo then introduced our IBM Liaison **Stephen Quan** to give us an update on the upcoming elections of Directors on the TUG Board. Stephen opened by explaining the positive experience and how much he has enjoyed working with the Board for the last two years. (Details on page 28.) Next, Director **Glenn Gundermann** invited us to attend TEC '007 on April 17th to the 19th. See Glenn's article on page 18 for details.

Glenn and Wende then distributed the Door Prizes: First there were two '007 Editions of

the "Scene-it" Game, kindly donated by **Alkarim Sachedina** and the Mattel Corporation. Then we had a draw for a $50 certificate to be used towards the purchase of a registration for the upcoming TUG TEC '007. Please see the "Lucky Winners" article under "*TUG NOTES*" on Page 28 for the names of the winners.

DR & Security Confessions - the Movie

Richard Dolewski opened the second session by providing bowls of popcorn for all the attendees (movie patrons?) and asked the question: "What is a Disaster?" He then told us that the Federal Emergency Management Agency (FEMA) in the U.S. recorded over 100 weather related disasters in 2005 and 82 in 2006. He also talked about some of the additional major hydro outages here in Ontario including some that were unrelated to weather. He pointed out that while many of us believe that these situations are covered in our Disaster Recovery (DR) plans we should possibly look again. For instance: Where will you get the fuel to run your backup generators when the power outages last beyond the limits of your fuel supply and the pumps cannot be used without power?

He talked about IT "secrets" (perhaps dirty secrets?) in your DR plan: Is it a REAL plan (written, tested, and published) or something in someone's mind or on the back of a napkin? Do we know who has the plan? Are they ALWAYS available? He pointed out that "only 76% of today's businesses have fully documented Disaster Recovery Plans."; "38% NEVER test their plan"; and that "30% will NEVER work in a Disaster"!

He advised us on the outcome of a poor or incomplete plan, as well as some of the requirements for a good plan. One of the most important issues when you begin a plan is to ensure that you have defined and prioritized the Business Objectives and aligned the IT capabilities with these needs in order to "Minimize the gap between Business Requirements and IT Deliverables". He later emphasized the responsibly of IT to ask the tough questions to ensure that management **really** understands the impact on the business that could ensue in the case of a disaster. i.e., "could they really afford the disruptions that have been negotiated?" He suggested some open-ended questions that might uncover the real needs of the business and therefore of the DR Plan. Some examples were: Did management understand the reality of recovery time objectives; the impact of a possible loss of a day's orders; or the inability of the warehouse that is functioning in another location being unable to ship product due to system unavailability?

You then need to categorize your servers for recovery. The typical breakdown is 60% critical immediately for recovery, 20% necessary but recovery may be delayed, and the remaining 20% may not be required at all during a disaster. This allows you to center your efforts on the all-important 60%. For many companies it is imperative that

Léo Lefebvre

they include e-mail in this review, as it has become a "mission critical" part of many businesses. In addition, Richard pointed out that e-mail should be considered a High Availability (H/A) application.

Next you need to understand that "Backup = Recovery". Richard stated that of the companies that perform regular backups 42% are incomplete, and that 21% of the iSeries/400 and 36% of the Intel installations are unrecoverable using these backups. He went on to provide various backup pros and cons, and some save/restore strategies including some pitfalls and some horror stories. He also emphasized the impact of the Sarbanes-Oxley (SOX) requirements on backup and recovery requirements. He pointed out that some companies are "proud" of their 97% backup success rate, with only a 3% failure rate. They don't seem to equate this percentage with 12 days per year of NO Backups. NOT GOOD – If Murphy's Law occurs, what happens when a disaster strikes after one of those 12 days?

Léo Lefebvre

Evening speaker Richard Dolewski

He then discussed keeping "a clean house". You need to look at your computer room environment including temperature, humidity and airflow, data security and tape and backup device maintenance. Power supplies and their backups are especially important. There needs to be redundancy on your power supplies and on your "RAID5 or RAID6" setups.

Another mistake that many companies make is keeping their backup material on site. If you do, as Richard says, "... your company is toast!" Do your backups daily and get them stored safely off-site. If you use encryption, as is becoming more of a requirement due to SOX etc., ask yourself some questions: Who has the password? Where do they have it? Onsite? Offsite? How do you get it if there is a disaster?


Léo Lefebvre

Who would have thought about the computer console being strategic to the DR plan? We all did after Richard's real life stories (horror movies?). One company spent the money to develop DR Plans for their multi-million dollar business and then tried to save a few dollars by using an old, previously discarded console. Another used a high-end server as a console but couldn't find the required CDs to load the software for the iSeries. Another found the CDs but couldn't find the required "key". You must have a dedicated system console, properly maintained, configured with the proper, up-to-date hardware requirements, and all the latest required software for iSeries Access and Microsoft needs.

Richard stressed the importance of testing your plan REGULARLY — passively and actively. He then provided some comparisons of various versions of Continuous Availability and High Availability (H/A) and concerns when developing your DR Plan.

Next came a discussion of Security, including security for both your production and test data. You also need security for your backups. Passwords and user profiles need to be "managed" to ensure that they are current and protected. TCP/IP applications, autostarts, application architecture, the inappropriate use of special authorities, and control tables may all provide unexpected access to vital data. You must administer these areas and check them regularly. You must also supervise the authorization that has been given to your users. Do individuals have too much authority? Are there super users? Was a new user given a prior employee's authorizations when they took over a job, even if they didn't have the knowledge, the need, or the experience required? Do you close down a profile immediately when someone leaves the company?

Richard then discussed auditing the system. You should have your audit journals turned on. If you don't, how do you know who deleted or changed a file—perhaps inappropriately. You may need to have the audit journals turned on in order to meet changing government or professional regulations.

He pointed out that while you may think good security costs a lot — ***Poor security costs so much more***. The cost of lost data could have a severe impact on your business. Some of the repercussions could include the public perception of your company, legal action under privacy laws, stock valuation, loss of trade secrets, loss of business, litigation, and even loss of employment.

Richard then described the actions we should take when there is a security breach in order to supply the forensic information required. He advised us to save a substantial list of audit journals, job and history logs, access and physical security reports. He also suggested that we do not purge our audit journals after 7 days, or even 30 days. We should save them to tape, as they may be required for "proof" of a security breach or in the case of one company that he assisted, of an ongoing theft. He followed with a discussion of data preservation for the i5/OS, data retention for the i5/OS, as well as buying and implementing the best security applications that are available. Encryption for laptops, hard drives, backup tapes, CDs, memory sticks, PDAs, Black-Berrys etc. was recommended.

In closing we were warned to "Err on the Side of Caution" and that it was extremely important for the IT community to be prepared. TUG