



## CONTENTS:

A Word From Dan: Exposure	2
Check Please	3
John Still: Keeping Your Firmware Firm	4
Education Seminars	7
Richard Dolewski: DR	8
Paul Oh: Tivoli Tips	10
Robot/SCHEDULE 10	11
Mid-Range Help	12

©Copyright 2007  
**Mid-Range  
Computer Group Inc.**  
All rights reserved

Send subscription requests to:  
Mid-Range, 34 Riviera Drive,  
Markham, Ontario,  
Canada L3R 5M1

Web site: [www.midrange.ca](http://www.midrange.ca)  
Phone: 905-940-1814  
Toll Free: 800-668-6470

**Editor-in-Chief**  
Dan Duffy

**Managing Editor**  
Zdy Orlinski

**Technical Editor**  
Richard Dolewski

**Art Director**  
Vaughn Dragland

**Contributors**  
John Still  
Richard Dolewski  
Paul Oh

**Editorial Assistant**  
Laurel Hall

IBM®, the IBM logo, System i5™, i5/OS®, iSeries™, p5™, AIX®, pSeries™, AS/400™, and Websphere® are trademarks or registered trademarks of **IBM Corporation** in the US, Canada, and other countries. Trademarks of other companies appear for identification purposes only and are property of their respective owners.

Design & Pre-press Services:  
**Eclipse Technologies Inc.**  
416-622-8789  
[www.e-clipse.ca](http://www.e-clipse.ca)

Printing & Binding:  
**Amanda Graphics Ltd.**  
416-497-0500  
[www.amandagraphics.com](http://www.amandagraphics.com)

Distribution:  
**Grants Mailing Services Inc.**  
905-624-9082  
[www.grants-mailing.ca](http://www.grants-mailing.ca)

Canada Post / Eclipse  
Publications Mail Agreement  
Number 40907015

Current Circulation: 5,000

ISSN: 1718-858X

Printed in Canada



# A Word From Dan ...

## “Exposure”

“...The condition of being unprotected... the condition of being at risk of financial loss .....”

Over exposure is bad for film. It's bad for you and your company data too. Companies lose data in a variety of ways. A great deal of data loss is preventable if companies stick to the basics. (See “Check Please” on page 3 for a list of the basics.) Banks, mutual fund companies, retailers, courier companies and governments are losing data in various ways. That's not good. Companies have a fiduciary duty to protect their data. It's not an option.

### What should you do?

#### 1. Lock It Up:

In other words restrict access to it in the first place.

- Who has passwords?
- To which applications and to which data?
- Are you compliant with your security policies?
- Do you even have a security policy?
- Do you have to go as far as biometric (thumbprint, retinal scan etc.?)



#### 2. Back It Up:

Get the right data backed up to the right media, consistently!

- Check your backups.
- There is only one way to do that.
- Restore them. Or at least try to restore them.
- Do a disaster recovery test.



#### 3. Scramble It Up:

Encrypt Your Data

- Software encryption?
- Hardware encryption?
- Both?
- It depends on your situation and set up.



No one is perfect, and sometimes data does get lost. The press has been full of stories lately about various types of corporate data loss.

### But losing data is not the worst of it...

The big question is: does the lost data get exposed? i.e., does it see the light of day or can it be seen by those who shouldn't have their eyes anywhere near it?

What's worse than losing data is losing data that is readable and accessible because it is not encrypted. While losing data is still embarrassing, the cost of losing it is reduced exponentially if it is encrypted. If it is encrypted the chances of it being read, accessed or used for nefarious means are almost zero.

### Losing data can affect your company.

Losing data and having it fall into the wrong hands can affect your brand. Your brand is your company to a great degree. The initial cost of the loss is trivial compared to the loss of confidence in your brand.

Take stock of where you are when it comes to data exposure. A little bit of prevention goes a long way.

It may save your brand and your company and you'll never be forced to wear that extremely unflattering hat.

**M-R**

*Dan Duffy*

Daniel T. Duffy,  
President, Mid-Range

Protect IT. Protect IP. Protect Your Brand.™



“Get Your Picture On The Front Page. All Press Is Good Press.” ... **NOT!**

Check please.



Since 1988

- |                                     |   |           |
|-------------------------------------|---|-----------|
| Disaster Recovery Plan              | ✓ | Completed |
| Disaster Recovery Test              | ✓ | Completed |
| Disaster Recovery Hot Site          | ✓ | Completed |
| Security Audit                      | ✓ | Completed |
| Back Up & Recovery Audit            | ✓ | Completed |
| Encryption Implementation           | ✓ | Completed |
| Infrastructure Simplification       | ✓ | Completed |
| Hosting / Co-location / Outsourcing | ✓ | Completed |

# Keep Your Firmware Firm

By John Still

**S**o the new year rolled around, spring is almost here, and you are wondering why you can't get your belt done up in the same notch as you did a few months ago. Maybe all of those second helpings on cold winter evenings weren't such a good idea after all. Instead of tossing out all those fitness club flyers you get in the mail, you are actually starting to read them because you know you have to do something quick before you need a bigger belt altogether.

We've all been told before that regular exercise is the key to a healthy body and spirit. The same holds true for your System i5. Still, many shops adopt the "if it ain't broke, don't fix it" attitude. Sadly, these are the systems that end up in the emergency room for "unscheduled" maintenance.

Implementing a maintenance strategy for your i5 will help you stay out of the emergency room and, to be honest, just makes good business sense. Would you rather have short, scheduled outages for maintenance, or unscheduled, middle of the day scrambles with panic calls to IBM support and users lighting up your help desk lines?

## Recommendations for Server Maintenance

When it comes to server maintenance, IBM recommends the following:

1. Keep your server on a supported release level.
2. Stay current with the latest available fix packages:
  - Cumulative PTF Packages
  - HIPER Group PTFs
  - Database Group PTFs
  - Other Group PTFs as related to your environment
  - HMC and server firmware fixes

Most shops I have visited tend to stay on supported release levels. Falling behind in OS levels could make for more complicated (and costly) upgrades in the future as you may have to do an interim upgrade before you can get to the new release level. If you get to the point where you are running an unsupported release, getting help after your system crashed will be difficult. IBM's technical support databases are always pushing the information on the unsupported releases out to make room for the APARS and Knowledge Base documents for the supported releases. You might find a hit doing a Google search on the error code...maybe. If you find yourself in this position, contact us here at Mid-Range and we will do our best to help resolve the problem. Helping you put together a strategy to get to the latest release and fix levels would be our top priority.

Staying current with the latest available fix packages may be desirable but for most shops, having to IPL their system with a frequency that matches IBM's PTF updates is just not possible. As far as Cumulative PTFs and other Group PTF packages, I think a quarterly maintenance schedule is sufficient.

The High Impact and Pervasive Problems (HIPER) bulletin lists new PTFs every week. Again, finding a weekly maintenance window to stay current with the HIPER bulletin is nearly impossible for most. I would still recommend all shops subscribe to this bulletin and review it for any critical issues that have been dis-



covered. You may see something that may impact your business...a defective PTF or a DASD microcode patch. In fact, the most recent HIPER bulletins have listed PTFs required to handle the changes this year to Daylight Saving Time. By all means, schedule time to take care of these issues. Scheduled versus unscheduled is always the better way to go. You can subscribe to the HIPER bulletin at no charge. Just send an email to [hiper@ca.ibm.com](mailto:hiper@ca.ibm.com) and include your IBM customer number.

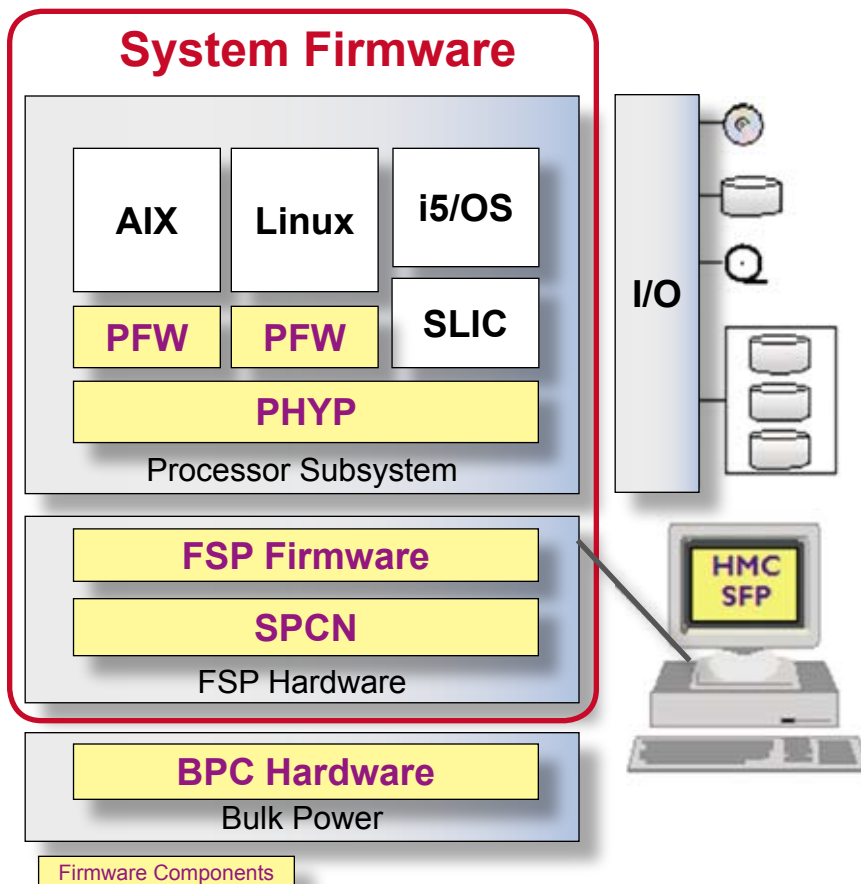
### What is firmware?

Now, assuming you have been a good little IT manager and have kept your iSeries on a current OS level and you have also been diligent by applying PTFs on a quarterly basis, along comes a shiny new System i5 into your shop. How does this change your maintenance strategy? The introduction of the Hardware Management Console (HMC) and i5 firmware will require some minor but important adjustments.

Let us first discuss the concept of firmware as this is something new that was introduced with the i5 hardware lineup. The simple definition of firmware is it is low level software that controls the system hardware.

As you can see in this diagram, firmware on the System i5 is more complex than the simple definition leads you to believe. Here is a brief description of each of the firmware components:

- **FSP** is the Flexible Service Processor firmware. This provides diagnostics, initialization, configuration, run-time error detection, and correction.
- **PHYP** is the Power Hypervisor firmware. Based



on the iSeries hypervisor, this provides VLAN, virtual I/O, and subprocessor partitioning support.

- **PFW** is the Partition Firmware that supports the pSeries Power Architecture Platform Requirements+ (PAPR+) interface.
- **HMC** is the Hardware Management Console firmware. This provides converged platform configuration, management, and services.
- **SPCN** is the System Power Control Network firmware. This interfaces with bulk power for power monitoring and control.
- **BPC** is the Bulk Power Control firmware that controls each bulk power unit in CEC and towers. This firmware is specific to the i595 system.

firmware will fix known problems with these components, add new function, and keep the server and HMC operating at their peak.

### Firmware Update Policy

There are many ways to order firmware for your System i5. You can use an HMC, order a CD, use the SNDPTFORD command from a green screen, or go to the Fix Central web site. Before you do this however, you need to know what the firmware update policy is set to on your server. If your system is not controlled by an HMC, the firmware update policy is set to "Operating System". This simply means that you would order the Firmware fix as you would any other PTF using the SNDPTFORD command or through Fix Central. Firmware fixes and updates are also included in Cumulative PTF packages and HIPER Group PTFs...when you load and apply these, you are also applying firmware fixes.

The only other setting for the firmware update policy is "HMC". If your server is controlled by an HMC

As with OS and System Licensed Internal Code (SLIC) PTFs, updating

*John Still is the Director of Technology & Systems Integration with Mid-Range Computer Group Inc. He can be reached at 905-940-1814, 800-668-6470, or via email at [johns@midrange.ca](mailto:johns@midrange.ca).*

## ... firmware

this is the default setting. You could change the setting to “Operating System” but you would also have to designate a “Service Partition” to act as the vehicle for loading and applying the fixes. If you only have a single partition, this is not a problem. When you have multiple partitions, this is not recommended since applying Cumulative or HIPER PTFs on the Service Partition that has firmware fixes included **WILL** force a shutdown of the entire System i5 as firmware fixes are applied. If you are not prepared, this could mean abnormal shutdowns of all your partitions. You have more control over this when the HMC manages the firmware.

How can you tell if LIC is HMC managed or operating system managed on your i5? One way is to try to start the HMC’s **Change Internal Code Wizard**:

- Click on Licensed Internal Code Maintenance on the HMC’s Navigation area
- In the contents area, click on Licensed Internal Code Updates.

- Select Change Licensed Internal Code for the Current Release.

You will receive the message *“The requested action is not allowed. One or more targets are configured for LIC updates through the operating system.”* if the operating system has LIC update control.

The only way to change this setting is through the Advanced System Management Interface (ASMI) which you access from the Service Applications menu on the HMC or by using the updlic command from the HMC command line interface.

### What Firmware Fixes are Available?

Now that you know what your firmware update policy is set to, you can go to IBM’s Recommended Fixes site and see what firmware fixes are available:

[http://www-912.ibm.com/s\\_dir/slkbase.nsf/recommendedfixes](http://www-912.ibm.com/s_dir/slkbase.nsf/recommendedfixes)

Select the OS level you are running, and then select the Server Firmware link base on the setting

of the firmware update policy. Note - if your firmware update policy is set to Operating System and you are running V5R3 OS, you will need to know if your SLIC level is V5R3 or V5R3M5 as the firmware fixes are different. Type DSPSFWRSC on a command line and press enter. Press F11 and you will see the installed release level of the SLIC.

It is important to note that in most cases the HMC code level needs to be updated to the most recent level prior to updating firmware. Fortunately, the HMC code can be updated without disrupting running partitions and usually takes less than an hour to complete. HMC code can be ordered directly from the HMC if it is on a public network with access to the Internet. You can also order CDs from the Recommended Fixes or Fix Central sites.

To determine the current level of HMC code, click the help tab at the top of the HMC GUI screen and then select “About HMC”.

To determine the current level of firmware installed using an HMC, click on Licensed Internal Code Maintenance on the HMC’s Navigation area:

- In the contents area, click on Licensed Internal Code Updates.
- Select Change Licensed Internal Code for the Current Release.
- Select the managed system (your i5).
- Select View System Information and click OK.
- Select None for the LIC repository and click OK.

For servers without an HMC you need to sign on to System Service Tools (STRSST) then select the following:

- 1. Start a service tool
- 4. Display/alter dump
- 1. Display/alter storage
- 2. Licensed Internal Code (LIC) data
- 14. Advanced analysis
- Put a 1 next to Flashlevels and press enter



IBM® System i™ family

- Press enter again to see the installed level of firmware

### Fixpacks VS Releases

There are two options available to change the firmware running on your server:

1. Upgrade to a new release. This is always a disruptive process as the i5 will be shutdown, powered off, and then reactivated again.

2. Update the existing Firmware running on the system. Updates are also called "Fixpacks". If your system is managed by an HMC and the Firmware Update Policy is set to "HMC", updating the existing Firmware will in most cases be a concurrent process that will not disrupt partition operations. The instructions for the Firmware update will indicate if the process will be disruptive or not. Remember, if your system is not managed by an HMC or if your Firmware Update Policy is set to "Operating System", installing Fixpacks will always be a disruptive process so you will need to plan accordingly.

If the firmware instructions indicate the process will be disruptive, do a normal shutdown on all your partitions. Once the partitions are in a powered off state, proceed with the firmware upgrade or update.

On an HMC managed system, go to the Licensed Internal Code Updates section on the HMC to install Firmware. Take the option to "Upgrade Licensed Internal Code to a new release" task for release updates or "Change Licensed Internal Code for the current release" task if you are installing a Fixpack.

Once the upgrade has completed, you can right click on each of your partitions, activate them, and resume operations. That's all there is to it.

### In a Nutshell

Planned versus unplanned, scheduled versus unscheduled... this is the mantra. In the meantime, where did I put all those fitness club flyers?

**M-R**



### Blade Rage

*Blade Server Technology*

**Length:** 1 day  
**Scheduled:** April 17, 2007  
**Registration:** 8:30  
**Course Time:** 9:00 - 12:00  
**Price:** Free

**Instructor:** Paul Oh

#### Topics Covered:

- IBM Virtual Fabric
- Architecture, Application Solutions & Consolidation
- Virtualization
- Live-Demo

RSVP: lhall@midrange.ca



### TSM Seminar

*Tivoli Storage Manager 5.4*

**Length:** 1 day  
**Scheduled:** April 26, 2007  
**Registration:** 8:30  
**Course Time:** 9:00 - 12:00  
**Price:** Free

**Instructor:** Paul Oh

#### Topics Covered:

- New Features
- New Functions
- New Capabilities
- Backup Set Enhancements
- Live-Demo

RSVP: lhall@midrange.ca



### Installing a New Release of OS/400 V5R3 - V5R4

*Moving Your System i Operating System From One Release to the Next*

**Length:** 1 day  
**Scheduled:** May 10, 2007  
**Registration:** 8:30  
**Course Time:** 9:00 - 17:00  
**Price:** \$795

**Instructor:** Richard Dolewski

#### Course Abstract:

This one day course covers the basics. Learn and understand what needs to be done on your system prior to taking this big step. Systems preparation and the technical procedures will be reviewed to ensure a successful implementation. Students will go through a step-by-step Operating System upgrade process in the classroom. Plenty of helpful tips to ensure you are running come Monday morning.



### System i - BRMS

*Backup, Recovery, and Media Services on System i*

**Length:** 2 days  
**Scheduled:** May 23 & 24, 2007  
**Registration:** 8:30  
**Course Time:** 9:00 - 17:00  
**Price:** \$795

**Instructor:** Richard Dolewski

#### Course Abstract:

Learn about BACKUP and Recovery Media Services (BRMS). One stop tool to manage your backup, recovery, and media management in stand-alone or multiple i5 systems at a single site or across the network. Prerequisite: Student must be familiar with the OS/400 standard save and restore commands.



### System i - Administration

*Understanding Your System i*

**Length:** 2 days  
**Scheduled:** May 30 & 31, 2007  
**Registration:** 8:30  
**Course Time:** 9:00 - 17:00  
**Price:** \$795

**Instructor:** Richard Dolewski

#### Course Abstract:

This 2 day course is directed at individuals looking to enhance their understanding of System i administration and systems management best practices. The student will be given a detailed overview of the unique aspects of the System i architecture. These sessions are hands on and cover the typical day-to-day required of a System i administrator. Upon the completion of this course the student will be able to perform PTF management and understand the System i IPL process. The native save & restore functions in the operating system and best practices for reviewing logs will also be covered. In addition the student will learn about system values and how they control the system's operation.



Location: 34 Riviera Drive, Markham, On. L3R 5M1  
 Register @: educate@midrange.ca

# 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 policies
  - 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 roll. 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 recover 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 infor-

mation. 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 than 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. 

**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](mailto:rdolewski@midrange.ca)

## Question: Switch Blades? Answer: Yes. Can you?

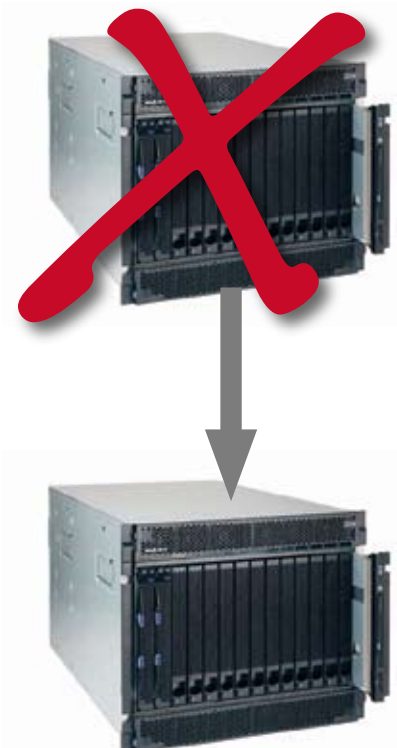
Blade server technology is evolving. More options. More networking capabilities. More density. More of your company data in one place.

With so many of your applications running on your blade servers have you thought about what you could do without them?

If the answer is, "not a whole lot" then it is time to do a test, a disaster recovery test.

Mid-Range offers the complete line up of IBM Servers including IBM Blade Servers in our raised floor disaster recovery hot sites. We also offer replication services with NSI Double Take™ and other methodologies to protect and recover your systems.

Contact [rdolewski@midrange.ca](mailto:rdolewski@midrange.ca) or 905-940-1814 or 800-668-6470 to set up a test date.



# Tivoli Tips

By Paul Oh

Ever been asked to keep monthly backups for seven years? Are SOX, Bill 198, and auditors driving up your archiving requirements? Is your data growing? These common IT challenges can better be addressed with the newly released Tivoli Storage Manager 5.4 (Jan 26, 2007 GA). Specifically TSM 5.4 has made great enhancements in the functionality of "Backup Set" which can be effectively used for long-term archiving.

## What is a TSM Backup Set?

A TSM Backup Set is a snapshot copy of TSM data that is created for archival purposes. A Backup Set uses only the number of days for retention

IBM **Tivoli** software

and is independent of the regular TSM incremental Backup versioning scheme. This makes Backup Set a great alternative to TSM Archive for monthly and yearly backups.

TSM Archive can still be used for long term storage but presents the following challenges: It adds tremendous overhead to the TSM database and requires all filespaces to be specified in a TSM schedule. In contrast TSM 5.4 Backup Set offers the following benefits:

- ✧ Improved Backup Set individual file and directory restore capability in TSM 5.4. No need to restore the entire Backup Set contents as was the case in earlier versions of TSM.



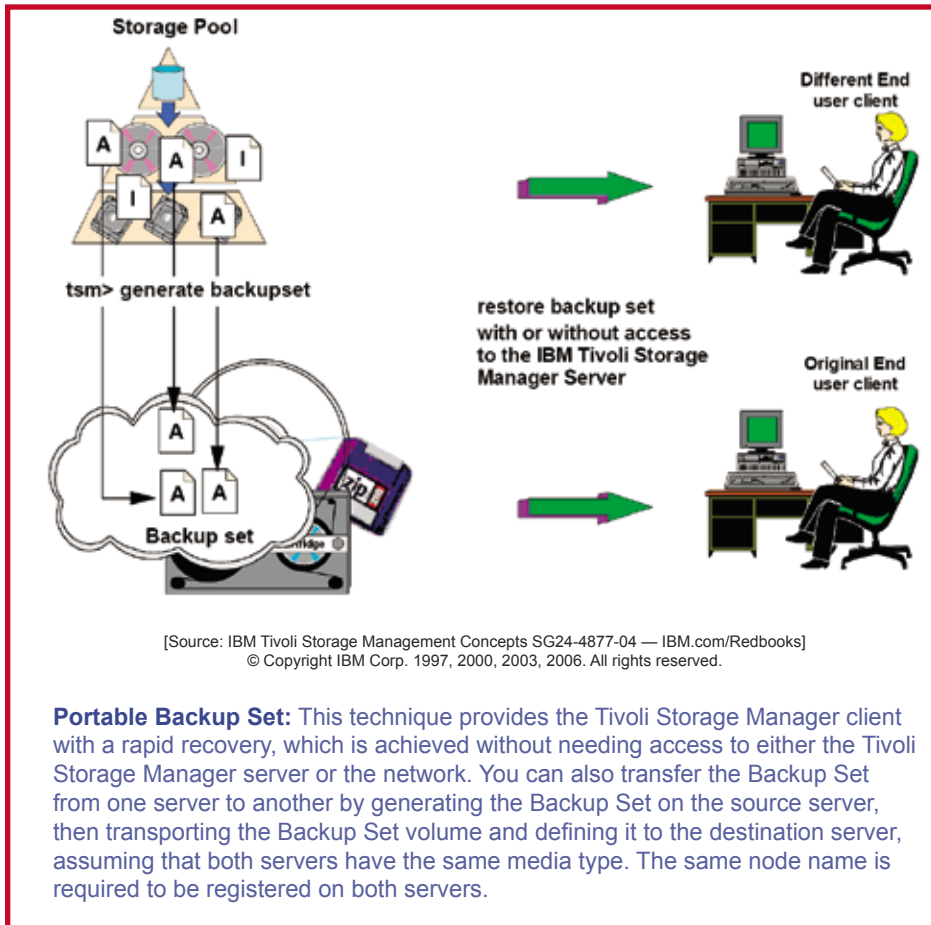
*Paul Oh is TSM/ADSM certified with over 10 years of experience. He is currently a member of the TSM 6.1 Advisory Council and has participated in past Advisory Councils and Beta programs for TSM.*

- ✧ Ability to create multiple server backups to one Backup Set tape in TSM 5.4 (assuming it fits in one tape). Previously a Backup Set was created per server or file space resulting in partially full and wasted tapes; for example archiving 15 servers would have required 15+ tapes prior to TSM 5.4.

- ✧ Ability to create a point-in-time Backup Set in TSM 5.4. This feature was first introduced in TSM Express last year and has finally made it into TSM. A point-in-time Backup Set allows you to create a Backup Set snapshot from last Saturday assuming your TSM Backup copygroup retention parameters meet this length of time.

- ✧ Individual files in a Backup Set do not require separate entries in the TSM database because the entire Backup Set is tracked as a single entity.

For more information contact Mid-Range at 905-940-1814, or 800-668-6470. **M-R**



**Portable Backup Set:** This technique provides the Tivoli Storage Manager client with a rapid recovery, which is achieved without needing access to either the Tivoli Storage Manager server or the network. You can also transfer the Backup Set from one server to another by generating the Backup Set on the source server, then transporting the Backup Set volume and defining it to the destination server, assuming that both servers have the same media type. The same node name is required to be registered on both servers.

# Announcing Robot/SCHEDULE® 10.0

## New PC Interface! New Job Schedule Tools!

### Control Your Job Schedule From Your PC

Robot/SCHEDULE, the world's most popular job scheduler for the IBM® System i™, brings a new look and feel to job scheduling with the Robot/SCHEDULE Explorer. Use the Explorer's point-and-click user interface to manage your entire job schedule, with direct access to every Robot/SCHEDULE tool and job schedule option. With complete job schedule control at your fingertips, you're more efficient and save valuable time. Display a job's details, create new jobs, make schedule changes—all with just a click—directly from your PC!

### Get A Real-Time View Of Your Jobs

With Robot/SCHEDULE's Schedule Activity Monitor™ (SAM™), you see all the job schedule action right from your PC. SAM shows you every job on your system—forecasted, running, waiting, completed, failed—on a single display. Color-coded icons show which jobs are running and which have been submitted.

Let SAM help you eliminate job schedule errors and meet—or exceed—your Service Level Agreements.

### Discover New Ways To Create And Display Jobs

Robot/SCHEDULE's Job Creation Wizard walks you through the job creation process with on-screen prompts. Create a job, define its run schedule, and run the job—in just seconds. Display your job graphically with the new Job Schedule Blueprint™. The Blueprint shows job details and the relationships between jobs. Use it to find gaps in your schedule and see how schedule changes will affect your jobs before you apply them.

Call us today at **1-800-328-1000** for a **FREE** Robot/SCHEDULE Information Kit. Or, visit our Web site at [www.helpsystems.com](http://www.helpsystems.com) to download a **FREE** 30-day trial.

**NEW!**

**Version  
10.0**





Managed Services  
Hosting  
Outsourcing  
System Management  
System Monitoring  
Security and Compliance  
High Availability  
Back Up and Recovery  
Disaster Recovery Plans  
Disaster Recovery Tests  
Disaster Recovery Hot Sites  
ERP Implementation Services  
ERP Project Management Services  
IBM Servers, Storage, and Middleware



Since 1988

800-668-6470 • 905-940-1814 • [www.midrange.ca](http://www.midrange.ca)

Copyright © 2007 Mid-Range Computer Group Inc. All rights reserved.  
MID-RANGE and the Mid-Range logo are trademarks of Mid-Range Computer Group Inc. All other marks are intellectual property of their respective owners.