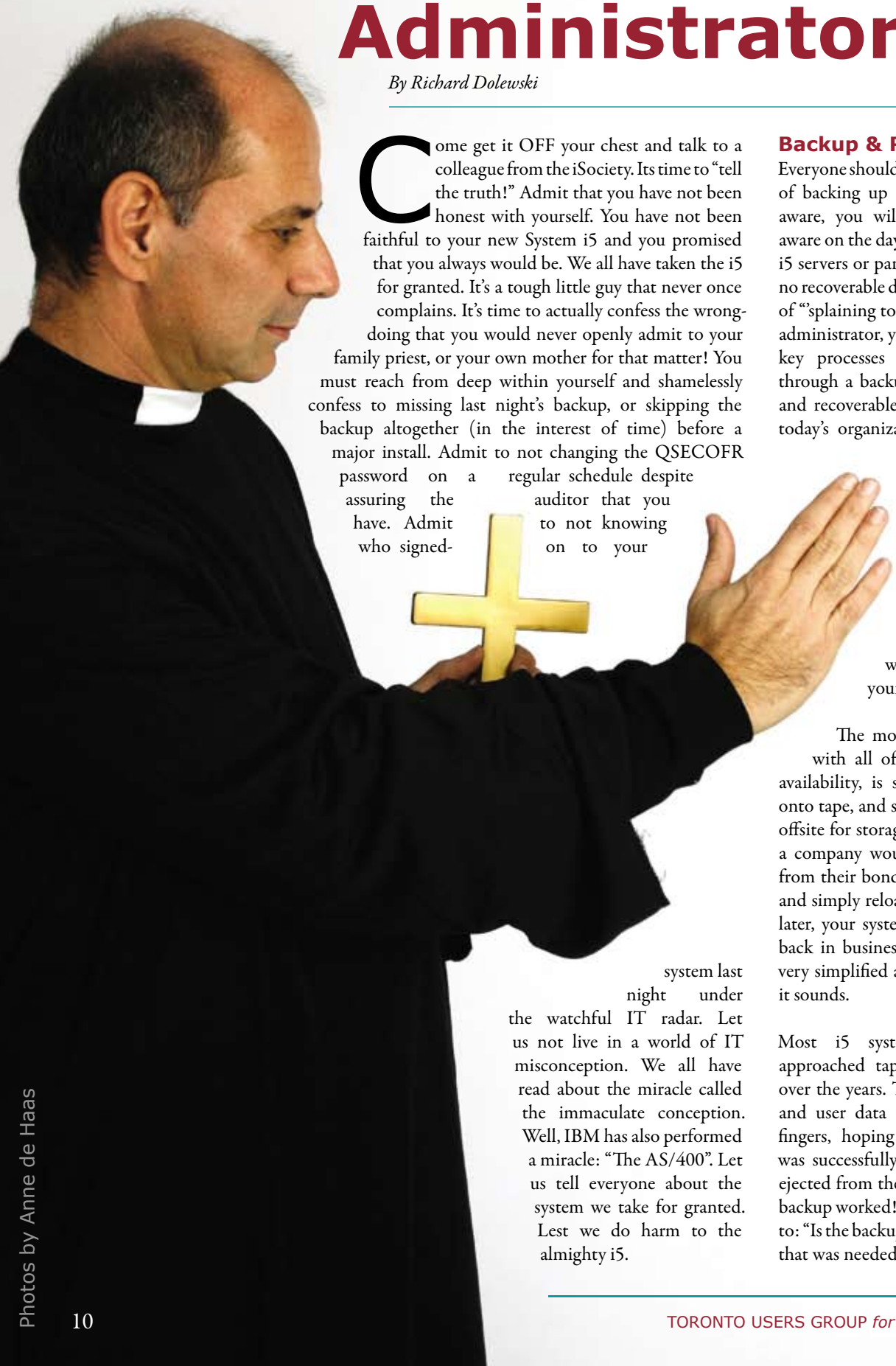
Confessions of a System Administrator

By Richard Dolewski



Come get it OFF your chest and talk to a colleague from the iSociety. Its time to "tell the truth!" Admit that you have not been honest with yourself. You have not been faithful to your new System i5 and you promised that you always would be. We all have taken the i5 for granted. It's a tough little guy that never once complains. It's time to actually confess the wrong-doing that you would never openly admit to your family priest, or your own mother for that matter! You must reach from deep within yourself and shamelessly confess to missing last night's backup, or skipping the backup altogether (in the interest of time) before a major install. Admit to not changing the QSECOFR password on a regular schedule despite assuring the auditor that you have. Admit to not knowing who signed-on to your system last night under the watchful IT radar. Let us not live in a world of IT misconception. We all have read about the miracle called the immaculate conception. Well, IBM has also performed a miracle: "The AS/400". Let us tell everyone about the system we take for granted. Lest we do harm to the almighty i5.

Backup & Recoverability

Everyone should be aware of the importance of backing up critical data. If you aren't aware, you will likely become painfully aware on the day after one of your iSeries or i5 servers or partitions crashes and there is no recoverable data. Then you will have a lot of "'splaining to do Lucy!" As an i5 system administrator, you need to bring all of your key processes and procedures together through a backup solution that is reliable and recoverable. Data is the backbone of today's organizations. Information is our corporations' most valuable asset, therefore, immediate recovery and access to data after an outage is the key to business survival. When data is lost or damaged or simply unavailable, it negatively impacts—and worse—completely halts your business.

The most common method, even with all of this pressure for systems availability, is still to first back up data onto tape, and second send the tape media offsite for storage. In the event of data loss, a company would recall the tape(s) back from their bonded offsite storage provider, and simply reload the server. A day or two later, your system is restored and you are back in business. As you all know this is very simplified and it is sure not as easy as it sounds.

Most i5 system administrators have approached tape backups the same way over the years. They backed up the system and user data to tape and crossed their fingers, hoping that the backup process was successfully completed. The tape was ejected from the tape drive and voila—the backup worked! No thought was ever given to: "Is the backup complete?" "Is everything that was needed to be backed up to recover

Photos by Anne de Haas

every component of the i5 server actually backed up?" We would go about our way in hopes that no one ever asked for a restore. It became an accepted not-so-best practice. Confess away that your backups may be incomplete!

Everyone knows about the potential problems of backing up to tape, but no one said much about it. Backup had become an IT internal little secret. "Backups ran fine... I never hear about any issues!"

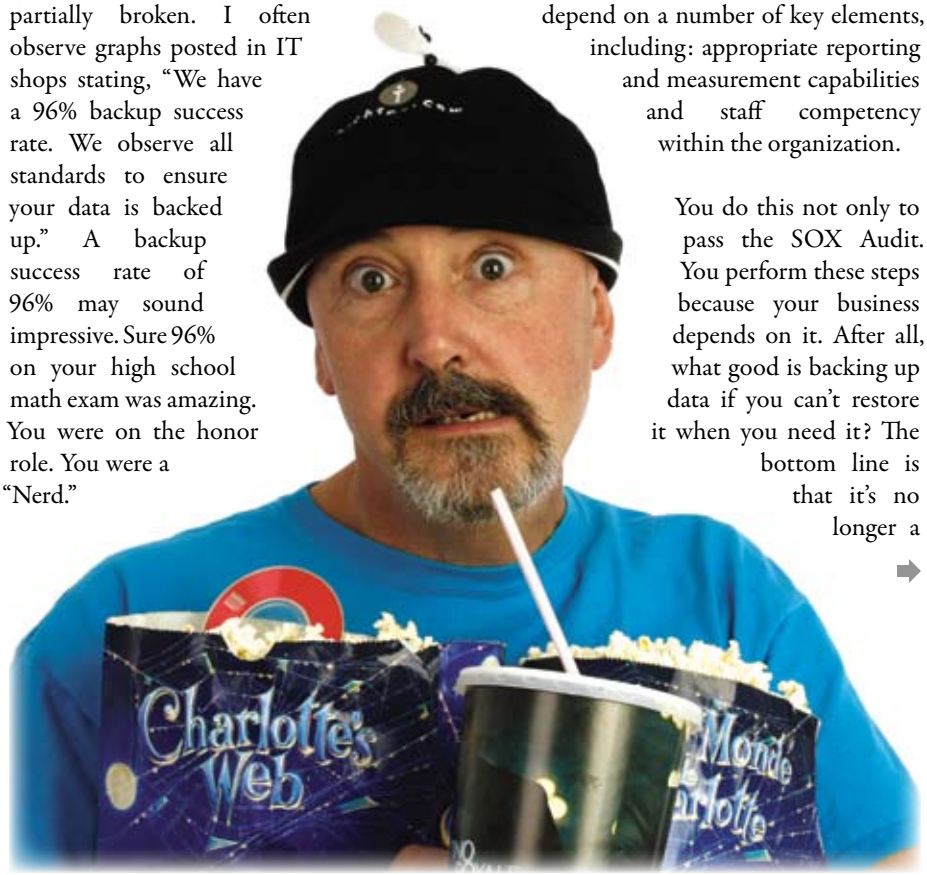
The key element to maintaining compliance and avoiding recovery issues is to stay on top of it. Having a process in place means a lot more than simply signing your name to it. With a sign-off, the process implies correctness. It means you have adhered to all the necessary steps in verifying the process as fully complete. That means 100% complete. This is especially important as it pertains to your backups. 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, "We have a 96% backup success rate. We observe all standards to ensure your data is backed up." A backup success rate of 96% may sound impressive. Sure 96% on your high school math exam was amazing. You were on the honor role. You were a "Nerd."

In real life though, this implies failure! This means that 4% of the time the Server isn't backed up on any given night. On a yearly calendar, there are 14 days when you have an incomplete backup. This means 14 days/year you will not be able to recovery the system in its entirety. Is this acceptable to your business? This number gets padded as well. Examples include: (1) "13 objects not saved" — "Oh we always get this message...its no big deal." (2) "Backup is signed off as successful." Was the backup really successful? This is not a half-full or half-empty discussion. You need 100%!

Back up 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. 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 backup 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 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



See "Confessions — The Movie", playing at a TUG MoM near you on Jan, 24

question of if data can be restored, but how quickly it can be recovered and how much data loss your own 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. By meeting audit compliance means you are demonstrating Disaster Recovery preparedness. Preparedness is all about being "recovery minded", not about being over-cautious or simply signing on the dotted line, as in: "The backup ran OK so now I meet SOX compliance !"

Tape Backups For All Systems

PROS:

- Easy to run
- Easy to manage – BRMS
- Easy to Automate – BRMS
- Today's High Speed and High Capacity reduced backup windows
- Capacity of today's tapes reduces number of tapes
- Virtual tape libraries V5R4 solution

Cons:

- Media errors
- Seldom validated
- Time to restore at Hotsite in a disaster
- Loss of data because backup only runs once per day

Backup & Recovery Best Practices

As the complexity of our systems increases, compliance proficiencies now demand that IT become accountable to both the users and to the business. The Sarbanes-Oxley Act provides governance that must be adhered to for many organizations today. The Act requires that the procedures used by the IT department must be audited annually to ensure they have internal controls and procedures, and that they are always followed. Disaster Avoidance happens long before a disaster occurs, certainly not after the fact. The backups must be executed on a regular basis and conform to a concise recovery program design. As the system administrator of the iSeries, you must have the ability to restore all of the system's data to a consistent usable state, which minimizes the impact on your applications. That is your primary goal. You should perform a system audit of your backup and recovery program design and verify its completeness.

Tips for meeting Compliance for Backups

1. Develop a Backup & Recovery Plan.
2. Establish a Backup Lifecycle Program.
   - ✓ Success/failure reporting
   - ✓ Problem analysis, resolution, and signoff
   - ✓ Examine backups exceeding 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—backup monitoring
4. Have a Hot-Box for vital records
5. Initiate a process to identify orphan data
6. Automate your backup process
7. Integrate your backups into change control process.

Security—Masked Confessions

How many of you know of gaps in your security implementation and convince yourself that nothing bad will never happen to you? "I simply have no time to properly secure all access to the system." "It was good enough for the external auditors, it must be good enough for me" Would you confess after the fact that you knew all these years that the security implementation was incomplete? Probably not!

If your system security were breached at your company, would you even know? While the risk of a security breach is high, the good news is that there are many ways for companies to mitigate the risks and

provide a safe controlled access to their critical data. Data security is the protection of the company's information assets from accidental or unauthorized access. Security consists of safeguards built into the system to help achieve control over devices, data, and programs. Security prevents unauthorized use of data and also helps protect the integrity of the system.

The most important action that must be taken for an effective information security program is the formulation of a company wide security policy outlining the protection of information. Do you have a written Security Policy? ... "What, we just finally wrote a Disaster Recovery Plan and now you what a security policy as well?" Security policies are fundamental to any security effort as they outline your management expectations for system security and guidelines for the different users that access the system.

The areas covered by the security policy should include general security policies and expectations of conduct, physical security, logical security access, application security, and application development security. Specifically to the i5, security policies should include architecture specific settings and configurations. The standards must include the recommended settings for system values, security related network attributes, auditing, and user profiles. The standards must also include guidelines for naming of user profiles and authorization lists as well as guideline for securing objects.

Anne de Haas

RD: "If your security were breached, would you even know?"

Auditing

How many of you examine the system for security events from the night before or have monitoring in place to proactively notify you on a timely basis? Do you even have the audit journal turned on? Tell the truth. "Oh that. I shut it down as it consumes too much CPU and eats up all my disk." You cannot review what you do not record or audit. The primary tool for event auditing on your i5 is the audit journal. The journal function is to record all security specific related events based on parameters you supply with the QAUDLVL system value. The journal function is also very useful for auditing specific types of activities on a system-wide basis, including the capability to audit specific user or object activity.

Auditing is important as it provides the ability to check for inappropriate behavior and gather data for regulatory and forensic purposes should it be required. In order to fulfill these objectives, auditing must be turned on with processes for proper analysis and storage of receivers in place.

Assuming an i5/OS breach, here is the information required:

- ✓ i5/OS audit journal receivers
- ✓ Job logs
- ✓ History logs
- ✓ Exit point software network access reports (e.g., FTP, ODBC accesses)
- ✓ Application level – history and audit logs
- ✓ Job Accounting history
- ✓ Network access logging
- ✓ Physical security reports

An audit trail can provide an excellent starting point to allow for a review of a system's security. However, it's not the preferred approach to be investigating security problems after they have occurred. The operating system comes with the IBM security toolkit. This extensive package for security reporting could be setup to run various batch jobs on a nightly and/or weekly basis. Select queries can be written against the audit journal to work with messaging software to warn of extensive violations.

Absolution

I find it amusing to discover all of the little secrets that go on it many IT shops today. Things happen daily and we simply accept them as part of the norm or ASSume no one will notice. If the computer room walls could talk! It's time for everyone to step forward and confess—not to the wrong-doing— rather, to the lack of doing. Stand up and say "Thou shall not abuse the System i5." Now don't you feel better? For you must clear your IBM soul before you see the lights (SRC lights, that is.) TUG

Richard Dolewski *(a certified systems integration specialist and disaster recovery planner) is Vice President for Technical and Contingency Services with Mid-Range. See a more detailed bio and an abstract of Richard's upcoming TUG MoM presentation on Page 8 ("The Agenda").*

Bloorview KIDS REHAB

Bloorview Kids Rehab is Ontario's largest children's rehabilitation facility. It is located in Toronto, Ontario, Canada. It was founded in 1899, by a group of community-minded women who met in Toronto to discuss the creation of a "Home for Incurable Children". As of 2005, the Centre provides hospital care, outpatient clinics, an integrated kindergarten school programme, assistive technology services and community outreach activities to about 6,500 children and youth with disabilities and their families each year. It is associated with the Faculty of Medicine at the University of Toronto. Prior to 2006, the centre was called the Bloorview MacMillan Children's Centre.

L-R: Richard Dolewski, Valerie McMurty, Wende Boddy, and Rakesh Tripathi (Presentation of a cheque from TUG to Bloorview Kids Rehab. Many thanks to the players and sponsors who raised this money at the TUG Annual Golf Tournament!)