# Communicating With Sam

## Modernizing Security and Recoverability

*Sam Johnston*

**Question:**

*Our company has used the iSeries platform since the late 1980s. We have developed our own applications and maintained them. For many years our business has been relatively unchanged, while the iSeries has been very stable and thus application changes have been relatively few. However, we have recently consolidated multiple iSeries severs onto a logically partitioned machine and integrated a Windows application server. In the future we are looking at integrating Linux applications. The rate of change is increasing and we feel that we need to review our legacy applications to ensure we are following best practices in security and recoverability. We also want to make sure we have incorporated the latest enhancements in the operating system into our applications and operational processes. Our IT organization has never faced the prospect of such a dynamic environment, and is generally not well equipped to manage the potential pace of change. What can we do to ensure that we respond to the business needs without creating chaos?*

**Answer:**

It is not uncommon to hear your scenario. Many companies have benefited from the iSeries legendary Hardware and Software reliability. This reliability is so good that many CEO's and other senior managers outside IT assume it will always be this way and no investment is required in the iSeries operational environment and processes. We know this is not true. The real issue is that IT systems are becoming more complex and more integral to business performance than ever before. This puts pressure on IT to achieve higher levels of application availability and reduce any planned or unplanned outages. However, there are limits to the improvements that can be achieved without significant investment in redundant hardware, OS, High Availability software, application enhancements, and of course operational processes.

Given that your applications have changed little for sometime, while your business has become increasingly dynamic, then clearly you are in need of a modernization project for both the applications and processes. The key success factors are not uncommon or different to any other project – appropriate investments in capital and resources, coupled with a strong executive sponsor to ensure cross-department synergy and co-operation. Assuming these factors are in place, tactically they will need to be supported with a strong, flexible foundation for your software management strategy.

The first step is to ensure that you have well documented programming standards and processes in place. You will need an auditable process in place for code promotion to the production environment; that is complied with, understood and agreed upon by all Development, Production and Computer Operations staff.

This process would include documentation of the required steps used for development, testing, user acceptance and promotion to the Production environment within your company. You should also establish the security requirements for each step to ensure a smooth and timely transition to production.

Many companies have limited controls over development that are often not effective due to the lack of strict processes coupled with weak documentation. This allows application objects to be promoted into production with insufficient security or testing. It is not uncommon to observe objects running in the production environment from development libraries. This should not be allowed and can quickly lead to a chaotic environment. The result is that no one will know which objects are required for production and it can impact which objects are actually saved impairing recovery capabilities.

To ensure processes are followed and enforced you may want to invest in an application to manage the process for you. Having this type of software in place to automate the development management process will improve development productivity. Just as important it will protect the production environment by minimizing mistakes, simplifying managing multiple versions and protecting developers' work.

Object level security needs to be designed into the application as part of the development project. Without object level security you are highly exposed to data theft, corruption, and any accidental deletion, change or modification of private and/or confidential data. For example, during a hardware consolidation project we performed for a customer, we observed that print files of payroll jobs were on the system and accessible to anyone. These files contained employee pay information, account numbers, payroll amounts for individuals, and other sensitive information such as their social insurance numbers. We have all heard about the disgruntled employee that distributed payroll information, and it crucial that your development processes don't inadvertently make it easier to do so.

Access to Objects is the means of gaining access to business data. Each object on the system needs to have the proper level of security tied to it so that it is acces-

sible to only those people within the organization that should have access. A company's use of data can make them successful and provide them a competitive advantage. Your company like other companies has data that is personal and confidential. Unauthorized access to this data could harm employees, customers, supply partners or the company if put into the wrong hands.

Today's Open database industry standard has created more and more ways for people to access data. No longer is data secure by menu options. You need object level security to protect against rogue ODBC, FTP, TFTP, JDBC transactions and to stop unauthorized people from accessing privileged confidential data.

Governments are now starting to take a firm hand and demanding data protection and integrity via privacy legislation such as the Health Information Privacy Act, Personal Information Privacy Act, not to mention corporate governance initiatives such as the United States' Sarbanes-Oxley.

In the near future it is possible that companies without a strong security process in place will lose business and partners due to the way laws are written. The laws are written so that if a company does business with a company that is deemed NON-compliant, than that company is also judged NON-compliant, regardless of how much money or time the company has spent trying to become compliant. Therefore, companies that are compliant will seek business partners that are also compliant and these companies will be required to conform to annual Security Audits, Change Control Audits and have formal Disaster Recovery processes in place with associated test documentation.

To determine the most appropriate strategy for your organization, the first step is to conduct a Recovery Needs Workshop. This is a session conducted with IT and the Key Business Process Owners. In order to develop a disaster recovery plan for the company, IT must understand the critical business processes and map them to the IT processes. The Recovery Time Objective and Recovery Point Objective for each process must be established and agreed to by the Business Process Owners. This will allow IT to develop a disaster recovery plan, and implement technology and processes that support the business needs. You won't be able to cost justify your Recovery Plan, without identifying the business risks, process needs and the priorities.

With the knowledge obtained from the Recovery Needs Workshop it will be possible to recommend a technical solution that meets the business needs at a price that is justifiable. Availability economics are simple - the faster the recovery time and the closer to the last transaction the more it will cost, usually increasing on an exponential rather granular scale. The key issue is to get the right level of recovery and test it regularly to ensure staff is experienced with the process. The key to justification of recovery is to be certain it will meet expectations, so if you don't document, train and regularly test the process you can be fairly certain that the expense will never be justified regardless of size.

Ultimately, achieving high levels of availability or business continuity requires considerable effort in Application Development, Security and Recovery Processes. All elements are linked and interdependent, requiring a life cycle management approach. The starting point is always sound business practices and procedures, supported with automation tools to reduce or eliminate the potential for human error. Change management tools deliver the silver bullet in this effort by complimenting strong business practices with structure, allowing organizations to improve productivity through compliance, while ensuring that approval is pushed to the right level. TUG




***Sam Johnston*** *is a partner and Chief Technology Officer of Intesys Network Communications Ltd., providing value-added networking and e-commerce solutions to the iSeries community. He can be reached at (416) 438-0002 or via email at sjohnston@intesys-ncl.com.* *Any TUG member wishing to submit a question to Sam can forward their typewritten material to the TUG office, or to Intesys. The deadline for our next issue is Friday February 11, 2005.*