

JOURNALSTAR | Security solution makes headlines



CLIENT SUCCESS STORY



Illinois' largest downstate newspaper protects its systems and data from the "danger" inside

No internal user had ever compromised security at the Peoria *Journal Star*, downstate Illinois' largest daily newspaper, but Information Systems Manager John Snider wasn't about to let it happen on his watch. He took a proactive approach to protect the organization (and its data) from harm, working with Advanced System Designs to install security software on the newspaper's iSeries server.

"It's my responsibility to protect our systems and data," Snider says. "If one person gets into the data and causes problems, that's what people will remember. Before we installed this software, there was a big opportunity for someone—intentionally or unintentionally—to get into our systems and alter or delete data. We decided we could not just ignore the risk and hope the problem wouldn't happen to us."

Understanding the risks posed by internal users

New technologies have made it possible for organizations to share data with remote users, business partners, customers, and others, and there are hundreds of ways to allow access to iSeries data—increasing the need for organizations to rethink their security strategies. Interestingly, while most security news revolves around hackers and the dangers they present organizations from the outside, a majority of security breaches happen by accident—from the inside. Internal users like employees, business partners, and suppliers often have direct access to mission-critical applications and data. While most of these trusted users don't have malicious intent when they access an organization's applications or data, some do—and others may inadvertently cause problems simply by accessing or changing information.





“I am very confident with the solution ASD helped us implement and encourage others to explore similar solutions. If you don’t, your data is at risk of being compromised. Anyone with a PC attached to your server can do damage, whether they mean to or not.”

Journal Star
Information Systems Manager
John Snider

Alan White, a principal at ASD, likes to use an analogy of the castle and the moat to explain internal security issues. “Most organizations have built their moat (a firewall) to keep outside invaders out. But most don’t have any idea what’s going on inside their castle. What data are employees accessing and possibly manipulating, intentionally or unintentionally? Payroll records, financial statements, you name it—these are the kinds of things you don’t want everyone in your organization looking at or changing.”

That was Snider’s biggest concern. “Everyone hears about hackers, but it’s the people inside your organization who get into a file or a database and don’t know what they’re doing who can be the most dangerous,” he says. “It wasn’t vindictive use I was worried about. It was the accidental use—the oops, I just deleted a file I wasn’t supposed to.”

Granting (and restricting) access, monitoring use

To protect the *Journal Star* from problems, Snider worked with ASD to install a security product called PowerLock on the newspaper’s iSeries server, which is accessed by approximately 100 users at any one time and runs business applications like billing, accounts receivable, and circulation.

Manufactured by the PowerTech Group, PowerLock allows network administrators like Snider and his staff to grant users access only to the systems or files they need to do their jobs—restricting them from entering others. Administrators can effectively monitor network traffic and ensure the integrity of corporate data. PowerLock’s audit trail feature in particular allows Snider and his staff to monitor use.

“If an employee repeatedly tries to access something they aren’t supposed to, we’ll go talk to them,” Snider explains. “Maybe they really do need access. Maybe not. The important thing is that we know about it and can make an informed decision.”

Snider also liked the easy set-up of the PowerLock product. “ASD came in about a month before the install and captured all our

iSeries’ transactions. They identified each computer and what files and applications it was uploading or downloading. We used that information to grant access to our users before the software went live. When it did, there weren’t any surprises or downtime—everyone automatically had access to the systems and data they needed. We were up and running on day one.”

Another benefit of PowerLock is ease of maintenance. “There are security packages out there that you have to install on every PC. I wanted something that resided on the iSeries box for ease of updating and maintenance,” Snider explains. “Because of that, PowerLock isn’t a high-maintenance product at all—in fact, it’s almost no maintenance.”

Finding the right partner and the right solution

The *Journal Star* has been working with ASD for over a decade, and Snider describes the relationship as a long, successful one. “It was a logical place for me to go because many of the IBM people I grew up with and trusted are now at ASD. And their work on this project was very professional. It was just a piece of cake.

“I am very confident with the solution ASD helped us implement and would encourage others to explore similar solutions. If you don’t, your data is at risk of being compromised. Anyone with a PC attached to your server can do damage, whether they mean to or not.”



Technology People. Business Results.

ASD people are technology people. Experts who understand the breadth of technology solutions available. Consultants who apply that expertise to your specific needs. And partners who care about delivering business results for your organization. For more information or to arrange a meeting, give us a call or visit us at www.asd.net/security.

Our security offerings range from assessment, design, and implementation to product sales and support. A leading provider of security expertise and solutions, we help you protect information, lower communication costs, increase bandwidth and response time, and improve Web server performance.

St. Louis office
866.ASD.9406
or 314.317.9406

Corporate office
877.ASD.4968
or 309.263.7944

Technology spotlight

PowerLock NetworkSecurity. Closes the gap between the access requirements of the networked world and the risk inherent in sharing iSeries data with employees, remote users, and business partners. Protects you from the cost and negative press associated with security breaches by monitoring and controlling who is accessing what, when, and how.

PowerLock SecurityAudit. Allows you to set and manage a sound security policy within your iSeries environment by conducting a comprehensive security analysis to obtain meaningful, accurate results. Lets you review reports at your convenience, configure them with the data you want, and investigate any security concerns that may arise.

PowerLock FlashAudit. Reviews security vulnerability in six major security areas: public authority, networks security, user security, special authority, system security, and system auditing. Recommends corrective action, if necessary.

- Technology**
- People**
- VPN/Firewall
- Authentication
- Spam Control
- Internet Management
- Intrusion Detection
- Audits & Assessments
- Traffic Management
- Security Appliances
- OS Security
- Anti-virus
- Business**
- Results**