Kisco Information Systems

SPECIAL REPORT

Case Study

Affordable IBM Midrange Software that makes you more productive

BYU-Idaho, Opens Doors to Education and Faith, Closes Them to the AS/400

Brigham Young University-Idaho is unique: It endeavors to open the door to the attainment of a higher moral standard as well as an academic one for its 11,000 students. Administrators do not feel however, that while opening the minds of its students, they can afford to leave any unattended openings to their production computing environment.

BYU-Idaho rests its faith in an IBM AS/400 model 730. It hosts an array of applications that you don't come across too often, including programs that manage information on financial aid, scholarships, student data, accounting, alumni, student employment, and placement. By and large, all the applications on BYU-Idaho's AS/400 are custom; all developed and maintained internally. When the school began opening up its environment to support TCP/IP so faculty, administrators and students could access the system from network connected PCs, it became evident, that having the proper authorities on all objects, level 40 security, and applications that could only be accessed through menu's; a scenario that was more than adequate under SNA, would not keep the back doors to the system safely shut over IP. Of particular concern were hundreds of OS/400 Exit Points. Exit Points are places in a program where you can register and insert your own programs and override default application functions. Exit points can be used to call programs, block access to programs, and perform other functions. "In a college environment, some people think they should be able to access data that they shouldn't have access to," states Thaine Robinson, Director if Information Systems at the school.

For more information on SafeNet/400 and other Kisco software solutions, log in at www.kisco.com.

The question they asked themselves was: How do we secure the system given the fact that people are now accessing it via telnet, Client Access and other topologies without changing the individual authorities for every system object? Controlling Client Access alone is a challenge for security managers. Some client/server functions can bypass traditional OS/400 security checking. A PC based database tool, such as Microsoft Access, Query, or Internet Information Server (IIS) can easily access, update, or delete any data file on the AS/400.

OS/400 Security Fell Short

"We felt that with TCP/IP you had to open up your system to the whole world," Robinson states. "We decided to look at additional security measures because we wanted extra security over what OS/400 offered." Although BYU-Idaho's staff of ten RPG developers had extensive experience, the prevailing thought was that the development of software which systematically limited access to their AS/400, in part by blocking a multitude of program exit points, was best left to those who have done it. Ongoing maintenance was a consideration as well. Tara McClellan, Operating Systems Manager and Security Officer for the school's system states, "We felt it was more justifiable to put our time and effort handling the changes and upgrades of our in-house software."

> *"In a college environment, some people think they should be able to access data that they shouldn't have access to."*
>
> Thaine Robinson, IT Director, BYU-Idaho

BYU-Idaho's production computing environment is carefully audited for compliance with security guidelines set forth by their parent organization, The Church of Jesus Christ of Latter-day Saints. Robinson continues, "Most audited environments require that you have separate

development and production machines. You have to be able to check things in and out. We just don't have the resources to separate these environments. Our test machine is our production machine," he states.

Concern soon arose that too much control would make the system difficult to use. "Users need to be able to easily access information, but that information also must be protected. There can only be one way to get to the information. There cannot be two ways to get to it, " says McClellan.

Robinson and members of his staff began to research third party security software solutions and came across SafeNet/400 from New York-based Kisco Information Systems (www.kisco.com). SafeNet/400 offers features that overlay the security tools in OS/400. SafeNet/400 analyzes the system to find all existing security faults, and allows you to selectively block all exit points. SafeNet/400 also monitors activity and report violations and can notify operators of security issues through system or pager messages. The product's object and profile monitors analyze the use of sensitive programs and commands and produces a comprehensive list of a specific profile's activities.

BYU-Idaho's technicians installed a trial version of SafeNet/400 and ran the logging feature for a week to get a picture of who was accessing the system from network connections and what objects they were trying to access. With details in hand, they locked down their server functions (SafeNet/400 controls over 40 OS/400 Servers) using the product's Access Controls. Each server can be configured for no restrictions, just logging, restricted by user, restricted by user and object, or disabled. Although SafeNet/400 is shipped with a default configuration, McClellan comments that she has slightly modified the way they handle Client Access.

Robinson liked the fact that SafeNet/400 was proactive. When it detects an access violation, the illegal access attempt is rejected. In addition to alerting security officer profiles, the product automatically sends a message to the user stating that the operation has been blocked.

Today, BYU-Idaho's production computing environment is more secure that it has ever been. McClellan is religious when it comes to security. "I run exception reports once or twice a week depending on the time of the year. It's kind of interesting--as students get familiar FTP and Telnet I often see an increase in unauthorized activity. I can find out from SafeNet/400 if there have been attempts to access the 400 and what their IP address is. Then I can identify the building, room, machine and who was actually logged on. We strictly monitor the 400 and the network," she says.

Also occasionally caught in the lair are their programmers. Sometimes they're not properly authorized to access all the things needed for an Ad Hoc file transfer for example. With SafeNet/400, if an access denial occurs inadvertently, McClellan can easily determine what object or file the user didn't have authorization to update the rules immediately. "When there's an issue, I'll call the programmer and sometimes they're a little foggy on what happened. They say they double click on something. One example of this occurred with Operations Navigator, which is used a lot by programmers. When we first installed it, I was getting all kinds of errors from three of them. It turns out that they were just exploring the new tool," she states.

Security Improves Audits

McClellan comments that SafeNet/400 is easy to maintain; An important consideration with all that she is responsible for. "Whenever a new operating system or application program release becomes available that includes Client/Server functions, all we do is get in touch with Kisco." *"Our audits have been very good lately,"* she states. "With SafeNet400 we catch things before they happen. It has had a very positive impact. It lets us know what's going on, and that our back door is intact."

Kisco Information Systems

7 Church St.
Saranac Lake, NY 12982
(518) 897-5002
Fax: (518) 897-5002
www.kisco.com
sales@kisco.com