



Michelle Haskin, vice president and application specialist, says SpiritBank adopted a data-encryption program partly to preserve customer confidence.

PHOTO BY JOHN BARNETT

A S P I R I T O F

Protection

SpiritBank goes beyond regulations to avoid a data-loss nightmare **BY JIM UTSLER**

I wrote an article about encryption recently, starting it off with scary stories and statistics about lost and stolen data tapes. It sent a shiver up even my spine, thinking that my highly personal and confidential information might fall into the hands of some dirty-deed doer who would steal my identity and buy a new car on my credit. (If it does happen, I hope they at least get a hybrid.)

Unfortunately, those stories are still creeping up in the press, and SpiritBank is one financial institution that isn't taking chances. Indeed, SpiritBank has taken rigorous steps,

using BOSaNOVA's Q3 storage encryption appliance, to help ensure the security of its customers' information.

A Scary Thing

The Tulsa, Okla.-based SpiritBank has been in business for more than 90 years, and remarkably, it's still family owned (third generation). In these days of banking mergers and acquisitions, that's quite an accomplishment—and one that's paid off. The bank has 350 employees working in its headquarters and its 18 branches, which are in 12 markets in a mix of metropolitan and rural locations.

“If we lose a tape, we lose a tape. All we have to do is buy a new one.”

— Michelle Haskin, vice president and application specialist, SpiritBank

Following a path along I-44 in Oklahoma, the commercial bank operates in large cities such as Tulsa and Oklahoma City and smaller burgs such as Bristow and Cushing. “Because of this, we have a pretty diverse customer base,” says Michelle Haskin, vice president and application specialist with SpiritBank.

Running quietly in the background are two IBM* System i* servers, including a production 520 and a backup 820 (soon to be upgraded to a 520). The bank also has an IBM System Storage* Ultrium* 3 3580 tape drive for its daily, weekly and monthly tape backups. And, as with most financial institutions, it has several vendor-supplied banking applications, most notably Cardinal/400 from Cardinal Software. “That’s our primary app,” Haskin says.

SpiritBank was sending tape off into the wild in clear text before deciding to encrypt all offsite-bound tapes. The daily backups would go with a bank employee to one of the bank’s branches and be sealed in a vault. If the company needed to send tapes to the Cardinal office in Parsons, Tenn., to troubleshoot or diagnose problems, it did so via commercial carriers.

In both cases, however, the possibility that a tape might get lost or stolen always existed, opening the bank up to possible liability—and the potential for customer revolt.

“A loss of customer confidence would have as big an impact as any fine would, maybe even more,” Haskin says. “Once you lose that confidence, you can never get it back.” Although it had never misplaced a tape, it decided it didn’t want to take any chances, especially given data thieves’ increasing sophistication.

“Five or 10 years ago, that wasn’t really a concern. It was too expensive for people to purchase the proper tape drives and there was not nearly the number of conversion utilities back then that are available now,” Haskin says. “In addition, you had to have a System i server to read the tapes. Now, you can actually buy a tape drive off of eBay, hook it up to your PC and use conversion utilities to read a tape that was created on the System i server. In fact, you can find a video of someone proving just how easy it is on the BOSaNOVA Web site. It’s a very scary thing.”

Unfortunately, according to Haskin, many banks still don’t recognize the threat—or if they do, they haven’t taken any steps to address it. In fact, she says, “I’ve been in the data-processing area in the banking industry for 25 years, and sending tapes offsite in clear text was an accepted industry practice. It wasn’t until probably a year ago that you even heard people talking about the necessity of encrypting tapes. And even now, many companies, banks and financial institutions continue to send tapes via mail or shipping companies. And just because you have a tracking number doesn’t mean a tape won’t fall off the back of a truck.”

Reading the Headlines

Though the banking industry is getting closer to developing regulations that would require banks to encrypt their tapes, the only banking regulation so far regarding lost tapes is that the institution would be held financially liable for the lost data and must notify customers of the loss. Haskin says she fully expects “in the near future that encryption will be part of that regulation—or at the very minimum, be highly recommended by examiners.”

Already, there’s movement in that direction. The Gramm-Leach-Bliley (GLB) Act, for example, has set encryption guidelines for financial institutions, such as requiring them to at least consider whether “encryption of electronic customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access,” is appropriate. GLB also suggests that if financial institutions think encryption might be beneficial in their particular cases, they must implement it.



CUSTOMER: SpiritBank
HEADQUARTERS: Tulsa, Okla.
BUSINESS: Commercial bank
HARDWARE: An IBM System i 520, an IBM System i 820 (soon to be upgraded to another 520) and BOSaNOVA’s Q3 storage encryption appliance
SOFTWARE: BOSaNOVA’s Q3 storage encryption

appliance setup software and Cardinal/400 from Cardinal Software
CHALLENGE: Making sure the data on its backup tapes is secure
SOLUTION: Using BOSaNOVA’s Q3 storage encryption appliance to securely encrypt backup tapes to be taken offsite

Although there are no direct calls yet for encryption in the financial services industry, it's sure to be mandated at some point. To its credit, SpiritBank decided not to wait for that mandate. It instead determined that the "risk wasn't worth the cost justification," Haskin says. In response, the bank brought its technology-steering committee, security officer and technology department together to chart a new safe-data course.

After assessing its own system vulnerabilities, SpiritBank found its most glaring problems were the unencrypted tapes. "Even though our daily backups were going only 10 miles to a vault in one of our branches, a lot can happen over the course of that trip," Haskin says.

SpiritBank began looking at several software and hardware encryption solutions. In the end, it decided that the hardware route was the best way to go, assigning the encryption load to an appliance that would sit between the server and the tape drive, avoiding any potential server-performance hits. Additionally, Haskin remarks, "A hardware solution wouldn't require us to make any changes to our backup script. Everything would simply run as it always had,"

After reviewing several options, SpiritBank asked BOSaNOVA for more information about the Q3 storage encryption appliance and eventually requested a demo model for testing. The entire testing procedure, according to Haskin, took only about an hour. This included installing the appliance, restarting the 820 and configuring the Q3 box on a PC. After running a backup on the 820, the company loaded the tape into the 520, which didn't have a Q3 box attached to it and was unable to read the tape. "It was terrific," Haskin recalls.

Secure and Flexible

Based on the success of that test, SpiritBank's technology-steering

committee approved the purchase of two Q3 units, one for the production 520 and the other for the backup 820. Once the Q3 devices arrived, it took only 30 minutes to put them into production, including installation, configuration, testing and then going live. "They were really easy to install," Haskin says. "You load a

program on a PC and set the encryption key—and that's pretty much it."

One important benefit of the Q3 solution was that the devices are married to the encrypted tapes they create, so even if another Q3 device is brought into the data center and attached to the System i platform, and an encrypted

tape is loaded, the tape still can't be read. This is true even if someone has the encryption key, because each Q3 device has a unique embedded chip that must match the associated data on the tape it encrypted.

As an added safeguard, BOSaNOVA supplies two chips for each Q3 device.

Should users experience any problems with the original chip, they can simply install the backup chip and continue backing up as they had in the past. SpiritBank keeps the spare chips for its two Q3 units in separate vaults at two locations, ensuring even greater data security.

As of now, SpiritBank uses only one of the Q3 units, for its production server. When it replaces the 820 with the new 520, it will begin full box-to-box replication. (Because the 820 is maxed out, Haskin says, it's used only to back up specific files. The company works with a disaster-recovery site in Texas to make sure it can recover from a system failure.) When complete replication between the System i boxes begins, the bank will create two sets of backup tapes, each protected by the encryption capabilities of the BOSaNOVA Q3 solution.

If the production box were to go down, SpiritBank can move the production Q3 to the backup box and load data from the tapes encrypted on the production system. SpiritBank can even take the production Q3 to its disaster-recovery site and restore from the production tapes there. If the disaster includes the Q3 device, Haskin can use the backup chip in a new Q3 box and still successfully recover. "This system is very secure, but also very flexible," she says.

Sit Back and Relax

SpiritBank isn't taking any chances, thanks to its encryption scheme, which comes due in large part to BOSaNOVA's Q3 storage encryption appliance. "If we lose a tape, we lose a tape," Haskin says. "All we have to do is buy a new one."

SpiritBank can now send its tapes wherever it wants, without worrying about an open truck door or a determined hacker. And when the banking industry finally gets around to regulating the use of encryption, SpiritBank can simply sit back and relax as other companies scramble to obtain compliance. Now part of its spirit is a spirit of protection. 



Jim Utsler, IBM Systems Magazine *senior writer*, has been covering technology for more than a decade. Jim can be reached at jutsler@msptechmedia.com.