TRIBUTE VENTURE: Former KTRK TV anchorman Mark Garay has launched a video firm marketed through funeral homes. PAGE 2A

HOUSTON BUSINESS JOURNAL

Strictly Houston. Strictly Business.

Vol. 39 No. 22 Week of October 10–16, 2008 houston.bizjournals.com 100 Pages, 3 Sections $2.95

FOCUS: BANKING & FINANCE

Safeguard financial data from foxes in henhouse

Some studies have shown that internal threats comprise 60 percent to 80 percent of all security threats, says Craig Mullins, corporate technologist for Sugar Land-based NEON Enterprise Software.

"*The most typical security threat* comes from a disgruntled or malevolent current or ex-employee who has valid access to the mainframe," he says. "Auditing is the best way to find an unauthorized access emanating from an authorized user."

SECURITY

FROM PAGE 13B

When considering data protection practices, financial institutions should first look at the data stored in their database systems, Mullins says. Once data is secured, in order to be accessible, both data and metadata must be classified and organized.

"This is a requirement, because only in doing so can banks determine which data applies to which regulations — and therefore, which controls and what type of data protection measures are required for the data," he says.

Additionally, data should be retained for longer periods of time, creating a need for archiving, and it must be recoverable in the event of logical or physical errors.

He stresses that a bank's reputation, brand and market share can take a steep dive if it experiences any breach in data security.

The most highly visible regulations affecting financial institutions include Sarbanes-Oxley, and Payment Card Industry Data Security Standard.

• **Sarbanes-Oxley Act of 2002.** The most familiar to the average American, SOX was put in place to regulate corporations to reduce fraud and conflicts of interest, improve disclosure and financial reporting and strengthen confidence in public accounting.

"Section 404 of this act, the one giving IT shops the most problems, specifies that the chief financial officer must do more than simply vow that the company's finances are accurate; he must guarantee the accuracy of the processes used to add up the numbers," Mullins says.

• **Payment Card Industry Data Security Standard.** PCI DSS was developed by major credit card companies to help prevent fraud, hacking and other security issues.

"A company processing, storing, or transmitting credit card numbers must be PCI DSS compliant — or it risks losing the ability to process credit card transactions. Given the availability and high-volume concerns of payment card transactions, this information is typically stored in a mainframe database," he explains.

'The most typical security threat comes from a disgruntled or malevolent current or ex-employee who has valid access to the mainframe.'

Craig Mullins
NEON Enterprise Software

"Bank executives must ensure their databases are protected such that only properly authorized entities have access to only the specific data they need in order to do their jobs — and to be able to prove this," he says. "Tracking who did what to which piece of data and when they did it is important because there are many threats to data security."

Data access auditing, sometimes simply called database auditing, can track the use of database resources and authority.

But as with any technology, there are multiple considerations before implementation, he adds.

The first step, he says, is to make a list of regulations to be complied with based on the types of data the institution holds. This "compliance roadmap" should determine what level of data access auditing is required, with input from an internal auditing group. A good database access auditing solution should answer several questions:

- Who accessed the data?
- At what date and time was the access?
- What program or client software was used to access the data?
- From what location was the request issued?
- What command was issued to access the data?
- Was the request successful; and if so, how many rows of data were retrieved?
- If the request was a modification, what data was changed? (A before and after image of the change should be accessible.)

"When choosing a solution, consider one that delivers pre-canned compliance reports," he suggests. ■