Mullins Consulting, Inc.

Return to Home Page

October 10-16, 2008

HOUSTON BUSINESS JOURNAL

Safeguarding Financial Data from the Foxes in the Henhouse

By Craig S. Mullins

Regulatory compliance has become a critical aspect of the IT landscape, and is a special consideration for financial institutions that house sensitive data. More and more regulations are being passed that dictate increased effort be exerted to better secure and protect the accuracy and privacy of mainframe data.

The most valuable enterprise data is typically stored within a mainframe database, so financial institutions must implement more robust auditing capabilities into their mainframe environments. Reputation, brand and market share can take a steep dive if a bank experiences any breach in data security. Auditing access to data is the first step towards preventing and handling data breaches.

The Regulatory Environment

There are many regulations that impact data protection and auditing requirements. The highly visible regulations that affect financial institutions include Sarbanes-Oxley (SOX) and Payment Card Industry Data Security Standard (PCI DSS).

SOX, the most familiar to the average American, 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 CFO must do more than simply vow that the company's finances are accurate; he or she must guarantee the accuracy of the processes used to add up the numbers.

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 they risk 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.

Simply put, 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.

Tracking who did what to which piece of data, and when they did it, is important because there are many threats to data security. External agents trying to compromise security and access company data are rightly viewed as a threat to security. But industry studies have shown that the majority of security threats are internal – within an organization. Indeed, some studies have shown that internal threats comprise 60 to 80 percent of all security threats. The most typical security threat comes from a disgruntled or malevolent current or ex-employee that has valid access to the mainframe. Auditing is the best way to find an unauthorized access emanating from an authorized user.

Tactics for Compliance

So how can financial institutions ensure they are in compliance with these regulations (and others)? Data access auditing, sometimes simply called database auditing, can track the use of database resources and authority. Each audited database operation produces an audit trail of information. The audit trail will show which database objects were impacted, what the operation was, who performed the operation, and when it occurred. This comprehensive audit trail of database operations produced can be maintained over time to show in-depth analysis of access and modification patterns against data in the mainframe.

But as with any technology, there are multiple considerations to understand and deliberate upon before implementation. The first step is to make a list of the regulations to be complied with, based on the types of data your institution holds. After you have created a compliance roadmap, determine what level of data access auditing is required, with input from an internal auditing group. A good database access auditing solution should answer at least the following questions:

1. Who accessed the data?
2. At what date and time was the access?
3. What program or client software was used to access the data?
4. From what location was the request issued?
5. What command was issued to access the data?
6. Was the request successful; and if so, how many rows of data were retrieved?
7. 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. For example, if you are looking to comply with PCI DSS, a database auditing solution that delivers out-of-the-box PCI reports will shorten your implementation timeline.

Ensuring compliance with tedious government and industry regulations is a daunting task. This, along with the growing need to protect databases from the increasing online and internal threats to sensitive data has resulted in financial executives being asked to be more personally responsible for the safety of corporate data. Data access auditing solutions can help financial institutions meet growing requirements safely and proactively.

From Houston Business Journal), October 2008.

Home.