



For the Complete Technology & Database Professional

IOUG DATA SECURITY 2009: BUDGET PRESSURES LEAD TO INCREASED RISKS

The 2009 IOUG Data Security Report

By Joseph McKendrick, Research Analyst
Produced by Unisphere Research, a division of Information Today, Inc.
September 2009

Sponsored by **ORACLE®**

Produced by



TABLE OF CONTENTS

<i>Executive Summary Key Findings</i>	3
<i>The State of Data Enterprise Security—2009</i>	5
<i>Risky Data Concerns</i>	12
<i>Data Off Premise</i>	15
<i>Super Users</i>	18
<i>Data Encryption Issues</i>	20
<i>Sensitive Data in Non-Production Environments</i>	24
<i>Monitoring and Auditing</i>	27
<i>Demographics</i>	32

IOUG Data Security 2009: Budget Pressures Lead to Increased Risks was produced by Unisphere Research and sponsored by Oracle. Unisphere Research is the market research unit of Unisphere Media, a Division of Information Today, Inc., publishers of Database Trends and Applications magazine and the 5 Minute Briefing newsletters. To review abstracts of our past reports, visit www.dbta.com/research. Unisphere Media, 229 Main Street, Chatham, NJ 07928. Tel: 973-665-1120, Fax: 973-665-1124, Email: Tom@dbta.com, Web: www.dbta.com.

Join the IOUG—If you're not already an IOUG member and would like to continue receiving key information like this, visit the IOUG at w3.ioug.org/join/today for information on how to join this dynamic user community for Oracle applications and database professionals.

Data collection and analysis performed with SurveyMethods.

EXECUTIVE SUMMARY

Since the last IOUG survey on “data insecurity” was conducted in September 2008, there has been an unrelenting stream of publicly reported data breach incidents within companies and public sector organizations.

For example, in March, a major telecom reported that a former employee sold or otherwise provided account data on thousands of companies to a third party without permission. During the same month, the New York Police Department reported that a civilian employee of the department's pension fund was accused of stealing eight tapes containing the Social Security numbers and direct-deposit information for 80,000 current and retired officers. An employee at the billing vendor for the city of Chicago's ambulance service had a laptop stolen, which contained patient names, addresses and Social Security numbers, impacting up to 63,000 people. Also this year, a third-party consulting services firm working on behalf of a major financial services firm reported that one of its employees was burglarized, and that a computer, which contained the names and Social Security numbers of current and former financial advisors and some applicants for employment, was stolen. An oil company reported that a former employee stole employee data, including Social Security numbers.

What do these incidents have in common? They all involved data that fell into the hands of insiders or contractors, without security mechanisms to safeguard it or in some cases the means to detect the incident until the perpetrators were arrested. Despite these risks, companies have made little headway in improving the security of data that's stored, managed, or transported across their enterprises, according to the results of a new survey among members of the Independent Oracle Users Group (IOUG).

In July and August of 2009, Unisphere Research conducted a study for the IOUG to address these challenges, and more. The survey was announced via an email notification to the IOUG membership list, which directed participants to a web-based survey instrument. A total of 316 responses were collected by the survey deadline.

Survey respondents oversaw complex and multiple database sites, many with large volumes of data. Forty-two percent of those surveyed manage greater than 100 databases, and 20 percent manage in excess of 500 databases.

Of the 316 respondents to the survey, 54 percent indicated they are database administrators, eight percent identified themselves as analysts, eight percent as IT managers, seven percent as developers, and the remaining 23 percent said they hold a variety of titles, including that of consultant, architect, and project manager.

Respondents came from a fairly even split among company sizes. About a third, 32 percent, came from large organizations with more than 10,000 employees, and more than a third, 37 percent, represented employers with 1,000 to 10,000 employees. In addition, 29 percent are with smaller to medium-size firms with 1,000 or fewer people. By industry, 15 percent came from the IT services and consulting sector, and 14 percent represented government organizations. Another 11 percent were with educational organizations. (For more information on the demographics of this survey, see Figures 30 through 33 at the end of this report.)

This survey explored a number of data risks, including the ability to enforce and monitor who has access to data, especially privileged users, media protection for data at rest and in transit, the secure configuration of the databases which house enterprise data, and the use of sensitive data in “non-production” settings, such as testing. Finally, the survey examined the regulatory compliance and auditing practices around data and databases.

Key findings include the following:

- There has been a 50 percent increase in data breaches since last year and growing wariness of the potential for data security problems. However, the uncertain economic climate over the past year has put a damper on the availability of funding and staff time to address these issues. There is pressure to do more with less and unfortunately in many cases less is actually being done. Only 28 percent of respondents reported receiving additional funding for their data security budgets—down a third from a year ago.
- Managers see internal threats—such as access by unauthorized users—as more pressing than external hackers or viruses. Potential abuse of access privileges by IT staff also ranked highly as a perceived security issue. One out of four cited lack of management commitment and lax procedures as exposing their data to risk.
- Outsourcing of database administration, development and testing functions has increased by up to 40 percent over the past year. More outsourcing and off-shoring without adequate security has also resulted in organizations unintentionally taking on more risk.
- Most organizations do not have mechanisms in place to prevent database administrators and other privileged database users from reading or tampering with sensitive information in financial, HR, or other business applications. Most are still unable to even detect such breaches or incidents.
- Awareness of the importance of data encryption is up, but fewer companies are actively applying encryption across all their data assets, whether data is at rest or in motion. A third even ship live unencrypted production data offsite.

IOUG Data Security 2009: Budget Pressures Lead to Increased Risks was produced by Unisphere Research and sponsored by Oracle. Unisphere Research is the market research unit of Unisphere Media, a Division of Information Today, Inc., publishers of Database Trends and Applications magazine and the 5 Minute Briefing newsletters. To review abstracts of our past reports, visit www.dbta.com/research. Unisphere Media, 229 Main Street, Chatham, NJ 07928. Tel: 973-665-1120, Fax: 973-665-1124, Email: Tom@dbta.com, Web: www.dbta.com.

Join the IOUG—If you're not already an IOUG member and would like to continue receiving key information like this, visit the IOUG at w3.ioug.org/join/today for information on how to join this dynamic user community for Oracle applications and database professionals.

Data collection and analysis performed with SurveyMethods.

- Close to half of organizations employ actual production data within non-production environments, thereby exposing this information in unsecured settings. To make matters worse, there has been a decline in companies “de-identifying” such sensitive data.
- Overall, corporate management is complacent about data security. Efforts to address data security are still ad hoc, and not part of an overall database security strategy or plan. Companies are not keeping up with the need to monitor for potential risks. More monitoring tends to be ad hoc or on the fly, versus more organized or automated systematic approaches.

The slippage in the level of security being applied to data may be beyond respondents’ immediate control, or even the control of companies caught in the grip of the economic downturn. However, in some cases, more education may make the difference. In comments provided with the surveys, a number cited the general complacency among their companies’ management toward these security vulnerabilities. “In general, just lax procedures for auditing and also, encryption of database backups,” said one respondent.

On the following pages is an overview of the scope of the risks companies face with the security of data environments.

THE STATE OF ENTERPRISE DATA SECURITY—2009

There has been a 50 percent increase in data breaches since last year, and widespread concern over continued vulnerability. However, the uncertain economic climate over the past year has put a damper on the availability of funding and staff time to address security issues.

Respondents to this survey represent data professionals and managers who play a role, either directly or indirectly, in the data security of their organizations. For the most part, respondents said the database managers and professionals within their companies are directly responsible for database security, and a majority of respondents to this survey, 91 percent, have a role in securing their data environments. When comparing the results to the 2008 survey, it's notable that there is an increased focus on data and database security across the board—shifting to systems management and development groups. (See Figures 1 and 2.)

About nine percent of respondents reported that over the past year their companies' data has been breached, compromised, or tampered with—a 50 percent increase from the previous survey (six percent). In addition, more than one out of five respondents remained concerned about potential data breaches or incidents within the next 12 months. (See Figures 3 and 4.)

While companies put a high priority on security, the current economic climate seems to have put a damper on security-related spending, the survey finds. About 28 percent reported that IT security-related spending has increased, down from 41 percent in last year's survey. About 13 percent said spending has actually decreased, a three-fold jump. (See Figure 5.) Larger companies

(defined in this survey as having more than 5,000 employees) were more likely than their smaller counterparts (500 or fewer employees) to have cut security spending, 16 percent versus 10 percent.

Despite a tightening of budgets, companies appear to remain supportive of data security initiatives. A majority of respondents, 52 percent, said that database security is a “high” IT security priority at their companies—about the same level as a year ago. (See Figure 6.)

The larger the company, the more likely database security is a high priority. Close to three out of five of large companies rank database security as a top priority, versus 37 percent of the smallest organizations. (See Figure 7.)

However, it's notable that 35 percent either have few or no databases securely configured, or simply don't know. This is up from 32 percent a year ago. (See Figure 8.)

A lack of tools, and a continued reliance on manual, ad hoc approaches to data security, may be hampering data security efforts. Only one out of four respondents reported that they consider their data assets to be securely configured, which is statistically unchanged from last year's survey.

Enterprises tend to be complex and multi-siloed. Thus, there appears to be less awareness of where sensitive data may be residing throughout the enterprise. Again, the economic climate—with tight budgets, overstretched staffs and a lack of tools—may have slowed down security efforts. While half of the respondents reported knowing where this data is, this is down from 60 percent in last year's survey. (See Figure 9.)

***IOUG Data Security 2009: Budget Pressures Lead to Increased Risks** was produced by Unisphere Research and sponsored by Oracle. Unisphere Research is the market research unit of Unisphere Media, a Division of Information Today, Inc., publishers of Database Trends and Applications magazine and the 5 Minute Briefing newsletters. To review abstracts of our past reports, visit www.dbta.com/research. Unisphere Media, 229 Main Street, Chatham, NJ 07928. Tel: 973-665-1120, Fax: 973-665-1124, Email: Tom@dbta.com, Web: www.dbta.com.*

Join the IOUG—If you're not already an IOUG member and would like to continue receiving key information like this, visit the IOUG at w3.ioug.org/join/today for information on how to join this dynamic user community for Oracle applications and database professionals.

Data collection and analysis performed with SurveyMethods.