EXECUTIVE SUMMARY

Information security is top of mind for all organizations today. Companies recognize that there are severe repercussions to ignoring or undervaluing data security, and most are increasing their investment in security and putting in place measures to protect their information. But are those measures sufficient? And, do those measures really provide the safeguards organizations think they do? According to this year's survey of 430 members of the Independent Oracle Users Group (IOUG), the answer to both of these questions is "no," leaving organizations more at risk than they are aware. This study of IOUG members' information security practices was first conducted in 2008, and then again in 2009.

This year's survey,[1] conducted in May 2010 by Unisphere Research, a division of Information Today, Inc., and sponsored by Oracle Corporation, uncovered the following troubling findings:

- Fewer than 30 percent of respondents are encrypting personally identifiable information in all their databases. Although slightly up from last year, this finding is startling given the number of existing data privacy and protection mandates that specifically call for data-at-rest encryption.
- Close to two out of five of respondents' organizations ship live production data out to development teams and outside parties. However, more than one-third admit that the data is unprotected, or don't know if it is protected. In many cases, the data consists of sensitive or confidential information.
- Three out of four organizations do not have a means to prevent privileged database users from reading or tampering with HR, financial or other business application data in their databases. Many of those who responded that they could "prevent" such activity indicated that they did so by relying on auditing and recovery process, and were reacting rather than preventing.
- In fact, two out of three respondents admit that they could not actually detect or prove that their database administrators and other privileged database users were not abusing their privileges.
- However, database administrators and other IT professionals aren't the only people that can compromise data security from the inside. An end user with common desktop tools can also gain unauthorized direct access to sensitive data in the databases. Close to half of respondents say that this either could happen in their organizations, or that they don't know if it could.
- Almost 64 percent indicate that they either do not monitor database activity, do so on an ad hoc basis, or don't know if anyone is monitoring. Less than one-third of those monitoring are watching sensitive data reads and writes. As a result, 40 percent of respondents indicate that they are unsure as to how long it would take them to detect and correct unauthorized changes to their data or their databases.
- Overall, two-thirds of companies either expect a data security incident they will have to deal with in the next 12 months, or simply don't know what to expect.

What is the greatest risk? "Our greatest risk is probably that of a rogue employee running amok," says one respondent. "We'd know about it soon enough, but it might be too late to avoid serious damage." This is a sentiment echoed by many other respondents.

Some data managers feel that their data is secure mainly because databases are not connected to the Internet—a false comfort that may lead to a rude awakening, especially considering that a majority of organizations admit that they do not apply Critical Patch Updates intended to address security vulnerabilities in a timely manner, or take steps to ensure that all their Internet-facing applications are not subject to SQL injection attacks.

On the following pages, the detailed survey results are presented by key areas: data privacy, access control, activity monitoring and auditing, and operational security.

[1] The survey consisted of email messages to IOUG members directing them to a Web-based survey instrument. Respondents were encouraged to provide open-ended responses to further explore the nature of their data security adoption strategies.

2010 IOUG Data Security Survey *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.