EXECUTIVE SUMMARY

As organizations dramatically scale up the amount of data moving across their systems and business units, the risk of data breaches and abuse grows.

Many organizations are managing more than a petabyte of data, which gets copied and proliferated for purposes of development, testing and backup. While data centers may have safeguards and best practices in place to protect data, there are no guarantees of whether other departments, business partners, or outsourced environments have the same rules and protocols.

There are also measures that need to be taken to safeguard data from internal abuse; however, preventing privileged users from negligence or malfeasance is a serious challenge.

These enterprise data security challenges, and more, are highlighted in a new survey of 350 data managers and professionals by the Independent Oracle Users Group. The survey was underwritten by Oracle Corporation and conducted by Unisphere Research, a division of Information Today, Inc.

The survey covered progress within three key areas of database security:

1. **Prevention:** Encryption, masking, privileged user controls.
2. **Detection:** Activity monitoring, network logging, database firewalls, auditing.
3. **Administration:** Database lifecycle and configuration management.

Survey respondents hold a variety of job roles and represent a wide range of organization sizes and industry verticals. The largest number of respondents is represented by database administrators (38%), followed by director/manager of IT. More than one-fourth work for very large organizations with more than 10,000 employees.

The majority come from IT service providers, financial services, education, and government agencies. (See Figures 43–46 for demographic detail.)

The following findings highlight the importance of data security issues

- Though corporate data security budgets are increasing this year, they still have room to grow to reach previous year's spending. More than half of respondents say their organizations still do not have, or are unaware of, data security plans to help address contingencies as they arise. Additionally, *human error* has beat out *internal hackers* or *unauthorized users* as the biggest security risk.
- Many organizations have multiple copies of sensitive, unencrypted production data moving both within and outside their enterprise, increasing the risk of data breaches. Less than a third of respondents encrypt all sensitive data on disk or in motion. More than three-fifths of respondents send actual copies of enterprise production data to other sites inside and outside the enterprise.
- A majority of respondents actively collect native database audits, but there has not been an appreciable increase in the implementation of automated tools for comprehensive auditing and reporting across all databases in the enterprise. In addition, this monitoring is sporadic—most would not know if their data had been breached or corrupted by an insider.
- There may be a great deal of attention and due diligence when it comes to auditing or monitoring database systems for unauthorized access or tampering with records, but perhaps the best—and least employed—strategy is prevention. Only about a third of respondents say they are able to prevent privileged users from abusing data, and most do not have or are not aware of ways to prevent the downloading of sensitive data to spreadsheets or other ad hoc tools.
- While data security audits can help track abuses after they happen, few respondents conduct such audits on a frequent basis. More companies are moving to centralized repositories to manage audit information.

Respondents also discussed where they see data security vulnerabilities within their organizations.

> "The sheer number of systems and databases…with business units operating like [a] standalone business, is a challenge for us. Plus, processes and controls are not yet consistent across the enterprise."
>
> *—Analyst, Mid-Sized Manufacturer*

> "Management does not assign enough time for creating monitoring and testing suites; it cares more about increasing the customer base."
>
> *—Chief Information Officer, Services Company*

> "I don't believe management sees data as vulnerable. As long as there are no reports from higher-seated users, they think everything is performing ideally. At this point, the most pressing risks are in the developers/testers themselves and the lack of knowledge concerning the data structure/architecture on the database—and even infrastructure—they are working with."
>
> *—Database Administrator, Consulting Firm*

Despite growing threats and enterprise data security risks, organizations that do implement appropriate detective, preventive, and administrative safeguards are seeing significant results.

Closing the Security Gap: 2012 IOUG Enterprise 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/About_Us#Unisphere. Unisphere Media, 630 Central Avenue, Murray Hill, New Providence, NJ 07974; 908-795-3701, Email: Tom@dbta.com, Web: www.dbta.com.*

Data collection and analysis performed with SurveyMethods.