IOUG
independent oracle users group

For the Complete Technology & Database Professional

DBA–SECURITY SUPERHERO

2014 IOUG ENTERPRISE DATA SECURITY SURVEY

By Joseph McKendrick, Research Analyst
Produced by Unisphere Research,
a Division of Information Today, Inc.
October 2014

Sponsored by

ORACLE

Produced by

UNISPHERE RESEARCH

TABLE OF CONTENTS

DBA—SECURITY SUPERHERO, 2014 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.*

EXECUTIVE SUMMARY

"With great power comes great responsibility"
—Francois-Marie Arouet (Voltaire)

When it comes to data security, today's enterprises are under assault as they never have been before. This year's Russian hacker breach by "CyberVor" was the most visible example of sensitive data falling into the wrong hands, but this incident was only one of many—the news never stops.

The world needs a hero to step forward. In fact, it needs many heroes with the power and knowledge to step forth and do something about this problem. Database administrators are in the right place, at the right time.

Data security has evolved into a top business challenge. The challenge continues to grow and the villains are taking advantage of lax preventive and detective measures.

In many ways, it has become an enterprise-wide challenge in search of leadership. Senior executives are only too painfully aware of what's at stake for their businesses, but often don't know how to approach the challenge. This is an opportunity for database administrators and security professionals to work together, take a leadership role, and move the enterprise to take action.

Who else can we look to as stewards of sensitive intellectual property, personally identifiable and protected health information? Who else has the privileges bestowed upon them to manage and administer this sensitive data? Our heroes, the database administrators have the knowledge and education to secure sensitive data on behalf of organizations and citizens of the known universe.

Now is the time for database administrators and security professionals to lead their companies to ensure data privacy, protect against insider threats, and address regulatory compliance.

As we do each year, the Independent Oracle Users Group (IOUG) surveys a wide range of database security and IT professionals responsible for security, and examines the current state of enterprise data security. By using this data, our desire is for readers to educate their executives and gain consensus with the security team to drive a data security strategy with actionable objectives.

Underwritten by Oracle Corporation and conducted by Unisphere Research, a division of Information Today, Inc., the report summarizes the findings from a survey of 353 IOUG data managers and professionals.

Key highlights include the following:

- Enterprises recognize that data risks come from within, and continue to increase funding. However, close to half still release production data to outside parties, and more than one-fifth report sensitive data is still vulnerable to breaches.
- Two-fifths of respondents admit they are not fully aware of where all the sensitive data in their organizations is kept. Those taking proactive measures to lock down data and render it useless to outsiders are still in the minority. Relatively few have safeguards against accidental or intentional staff abuse.
- Organizations are still not doing enough to monitor their data assets or keep tabs on super-users. Only about one-third can prove abuse of data assets. In a world where stolen data can be distributed globally within seconds," two-thirds of managers estimate that it would take a matter of days to remediate a breach, or simply don't know what length of time would be involved.
- Data security audits still remain few and far between. Only one-sixth review their data assets on at least a monthly basis.

As the data shows, data security is not something respondents take lightly. Yet, it's an ongoing, evolving challenge to protect the growing amounts of information on which enterprises rely. While many organizations in the survey have been spared of major incidents so far, it pays to stay vigilant. As one respondent put it: "You have to assume it's going to happen someday. Luck favors the prepared."

Within today's enterprises, no other type of professional is better equipped or more knowledgeable to deal with data security than database professionals.These are the individuals who understand where the risks are, and how these risks can ultimately affect their organizations. In an era in which information is the most precious resource powering business, database professionals can take a leadership role in helping to prepare and protect these assets. Preparation and education is a role experienced data managers and professionals are ready to take on in their enterprises.

Survey respondents hold a variety of job roles and represent a wide range of organization types, sizes, and industry verticals. The largest segment of respondents, 44%, hold the title of database administrator, followed by director or manager. One-third work for very large organizations with more than 10,000 employees. By industry sector, the majority of respondents come from IT service providers, government, education, financial services, and manufacturing. (See Figures 33–36 at the end of this report for more detailed demographic information on job titles, company sizes, and industry groups.)

DBA—SECURITY SUPERHERO, 2014 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.*

RISK FACTORS AND EDUCATING THE BUSINESS

Enterprises recognize that data risks come from within, and continue to increase funding. However, close to half still release production data to outside parties, and more than one-fifth report sensitive data is still vulnerable to breaches.

IT and data managers have opportunities to educate their businesses on where the primary threats are, and how to mitigate. The need is urgent; the 2014 survey shows that organizations are more willing to face the fact that they may experience a data breach in the next 12 months. More respondents believe the likelihood of a data breach is inevitable since the survey was first conducted in 2008 (more applies to the number of respondents, not relative inevitability), from 20% who believed a data breach was "somewhat likely" or "inevitable" to 34% now. (See Figure 1.)

IT managers and professionals recognize that every organization needs to prepare for the possibility of a breach. As one respondent put it: "With the advent of new ways and implementation and collection of more data, it is inevitable that the data will be breached, not 'if,' but 'when.'"

"There are multiple players in multiple databases that leaves an opening for a dishonest employee, unhappy vendor or an outside hacker getting in," says another respondent. "The most sensitive data is protected by multiple layers of protection, but still there is a possibility that there may be a breach at some time in the future."

Still, a number of survey respondents indicated that they felt their data was safe because it was locked behind corporate firewalls, or wasn't connected in any way to outside networks. As will be discussed throughout this report, this does not provide protection against insider abuse or breaches. As a respondent put it: "It only takes one bad egg" among the workforce or contractors to put data at risk.

It appears most organizations have been lucky so far. Overall, as has been the case in years past, only six percent say they were aware of a data breach within their enterprises, with another 23% admitting they simply aren't aware if any may have taken place. (See Figure 2.) Respondents from mid-size companies were most likely to be aware of data breaches. (See Figure 3.)

Data security is a difficult issue to report, even in a confidential survey, and even more often is difficult to be sure of, as observed by one respondent.

> *'We cannot be certain there has been no silent breach. There is no evidence we have detected of breach or corruption. But picturing yourself as highly unlikely to be breached we feel is like wearing a 'kick-me' sign on your backside.'*

There are numerous costs associated with a data security breach. Such costs include direct, indirect and opportunity costs, including lost business, customer churn, customer acquisition activities, and lost brand reputation. According to the latest figures from the Ponemon Institute, the estimated average cost of a data breach is now $3.5 million per incident, a 15% increase over the 2013 figures.[1]

Many enterprises are also subject to potential fines and penalties levied under a number of government regulatory mandates. These mandates also result in additional reporting requirements. Data management mandates and regulations affect most companies in this survey, including the Sarbanes-Oxley Act, local and state regulations, and HIPAA HITECH. (See Figure 4.)

While there is a great deal of concern about the threat of outside hackers, insider threats remain the most foremost problem. The Target data breach of 2013, for example, occurred because of an outside hacking, but it was a trusted contractor that unintentionally opened up the gates. Many data breaches—even those coming from outside—are the result of carelessness, unclear or non-existent policies, or inside vulnerabilities, either in data centers or among third-party partners. And in the eyes of IT managers and professionals, these vulnerabilities are only increasing as time goes on.

As this survey shows, human error is still seen as the greatest risk to enterprise data, cited by 81%—up from 77% last year (rated as a "high" to "medium" threat by IT managers). This is followed by fear of inside hacks—65%, up from 63% last year, 57% in 2010.

Risks also are rising across other areas of vulnerability, survey respondents point out. For example, 54% are now concerned about abuse of access privileges by their own IT staff—up from 48% a year ago. More than half, 53%, say that malicious code and viruses entering their systems are a threat—up from 38% just two years ago. (See Figure 5.)

When asked about the parts of their systems most vulnerable to security issues, respondents in the survey point to their databases—58% agree that this is where the greatest precautions need to take place. The network is the next most-cited area of potential damage, followed by the server and storage infrastructure. However, these vulnerabilities are not funded according to greatest risk. Most companies pour resources into their networks, followed by servers and databases. Interestingly, a majority say a large amount of resources also go into locking down desktops, though these are seen as less likely to contribute to damage from potential data breaches (See Figure 6.)

Close to half the organizations in the survey are demonstrating a growing commitment—in terms of resources and dollars—to data security efforts. This is unchanged from last year's rate, and

[1] *2014 Cost of Data Breach Study,* The Ponemon Institute, May 2014.

continues the highest levels reported since the first survey in this series was conducted in 2008. (See Figure 7.)

One major area of risk is enterprise business intelligence tools, and increased demands for user access to data. A sizable segment of those surveyed see this as a security vulnerability. Twenty-one percent say data in at least some applications could be exposed. This is slightly less than 26% who feared such a vulnerability a year ago. Interestingly, however, there appears to be less awareness of the problem than a year ago—36% say they don't know the level of vulnerability, compared to 22% a year ago. This may be a reflection of the proliferation of business intelligence tools, particularly as these tools increasingly leverage cloud and mobile platforms. (See Figure 8.)

Often, roles can be confusing. As one respondent put it: "Correct database roles, with user access restricted by role, should ideally result in no unintentionally disclosed data. But occasionally a DBA may misunderstand what is the correct role, or use a generic encompassing role. This is also a challenge with dev/support work tasked out off-shore or to outside consulting groups, where there aren't job titles or identifiable mission statements that DBA can tie roles."

Still, restricting or more closely guarding such access often requires organizational involvement. As one respondent explained: "Some spreadsheets use sign-ons of employees no longer present. When we close those accounts, the users howl, and management makes us re-open them. There's also an "ad hoc" account that many users across the division have access to."

At the root of many enterprise risks is when copies of live production data—which often includes sensitive or personally identifiable information—leave the data center, often going to other parts of the enterprise, such as development shops or backup sites. Often as well, copies of such data may be sent to outside third parties, such as contract development shops. Masking sensitive data in non-production environments, for development, QA and testing, is as important as protecting data in production environments.

Close to half, 45%, of all respondents use copies of production data in non-production environments—unchanged from last year. About one-third, 32%, say they use outdated copies of production data—down from 37%. (See Figure 9.) This is a step in the right direction, however outdated copies can often include data that never becomes outdated, such as names and social security numbers. Complicating the proliferation of production data is the fact that high numbers of data copies are spread across the enterprise. More than two-fifths of survey respondents, 41%, indicate that they have three or more copies of production data across and outside their enterprises—including offsite backups and third-party storage sites. (See Figure 10.) Multiple data copies are most pervasive across mid-size enterprises. (See Figure 11.)

DBA—SECURITY SUPERHERO, 2014 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.*

Figure 1: Predicted Likelihood of a Data Breach Over Next 12 Months

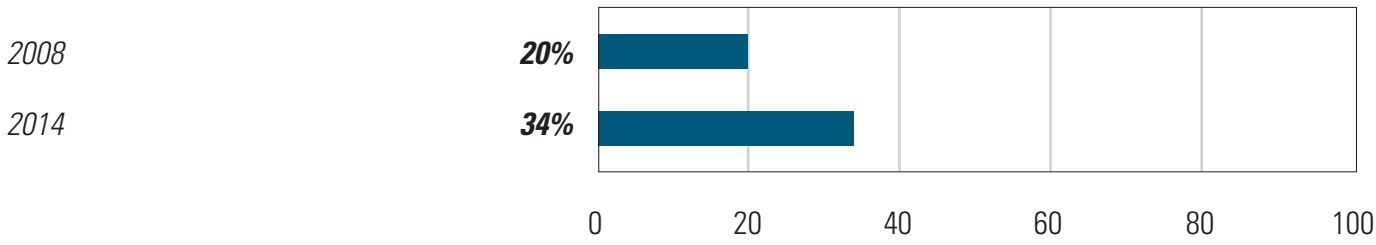


Figure 2: Known Data Breaches over Past Year

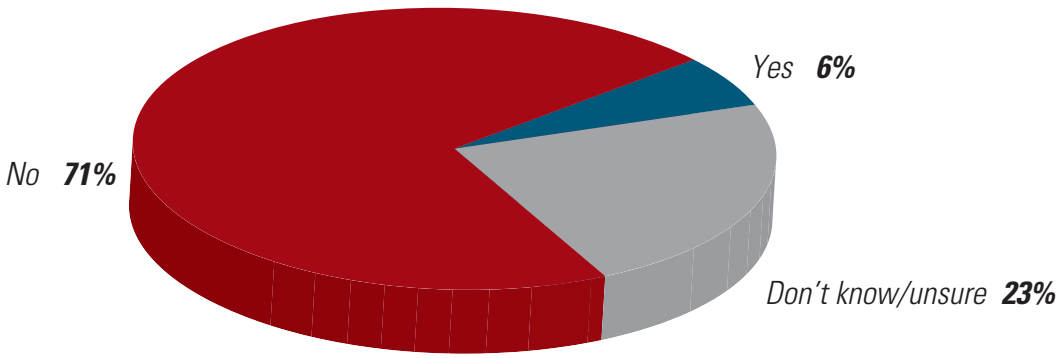
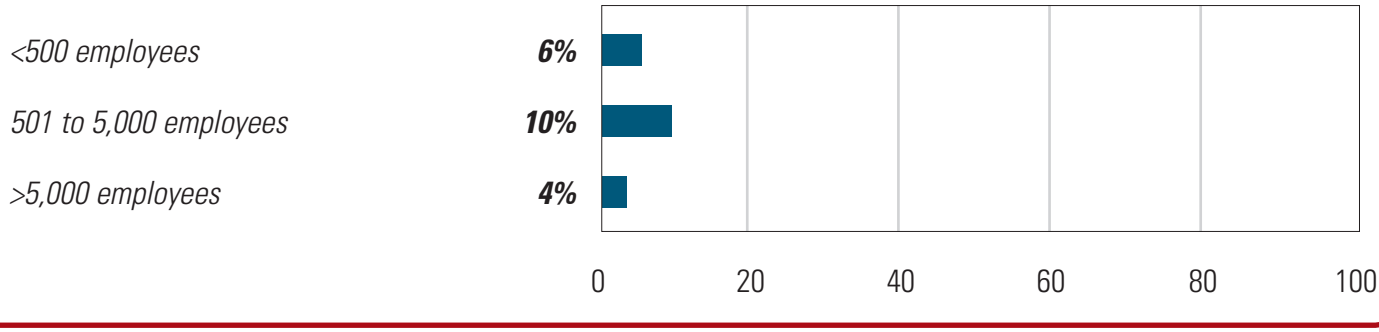


Figure 3: Data Breaches—By Company Size

(Respondents reporting known data breaches within each size category)



DBA—SECURITY SUPERHERO, 2014 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.*

Figure 4: Compliance Mandates

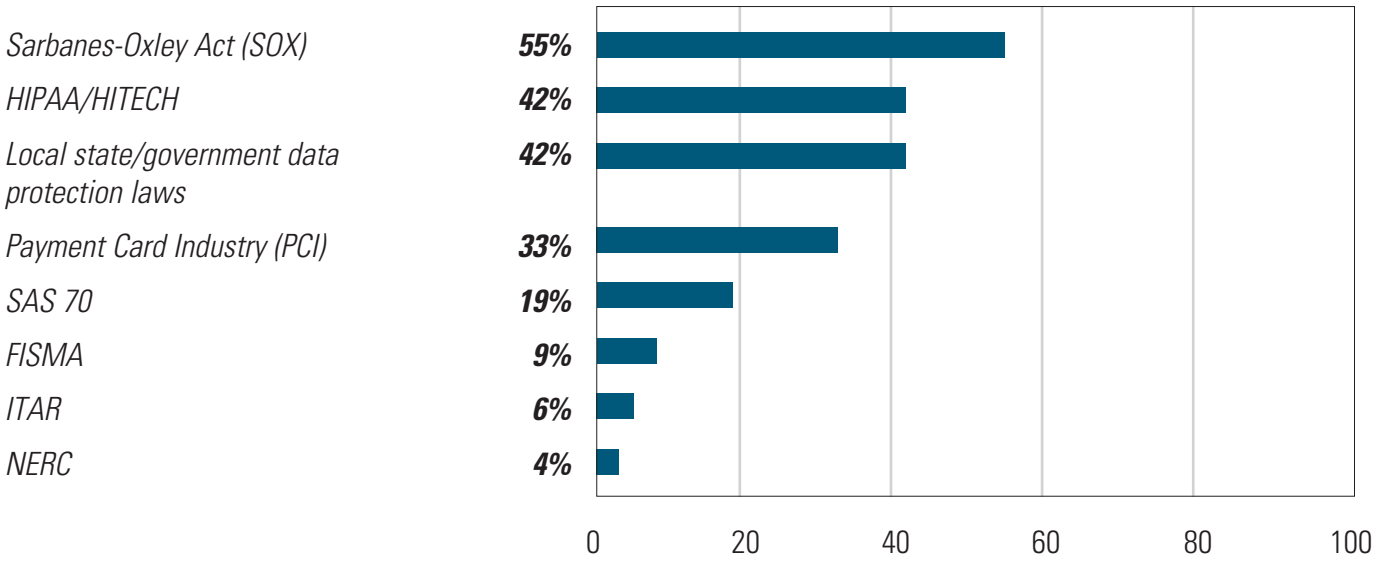


Figure 5: Where the Data Risks Are at This Time

	2010	2013	2014
Human error	—	77%	81%
Internal hackers or unauthorized users	57%	63%	66%
Abuse of privileges by IT staff	48%	48%	54%
Malicious code/viruses	38%	49%	53%
Unprotected web applications	—	44%	52%
Outside hackers	27%	44%	49%
Advanced persistent threat	—	40%	46%
Lack of management commitment/lax procedures	43%	41%	42%
Lack of auditability of access and changes	47%	39%	39%
Loss of hardware or media	39%	38%	38%
Abuse by outside partners/suppliers	25%	32%	35%
Fines/lawsuits	25%	22%	23%

Figure 6: Vulnerabilities versus Priorities

	Greatest vulnerability*	Most resources allocated**
Database	58%	56%
Network	51%	65%
Servers (file, web, email)	48%	57%
Storage	47%	43%
Application	41%	50%
Operating system	40%	51%
Virtual machine	37%	48%
Desktop	33%	53%
Middleware	32%	38%
Mobile devices	16%	21%

** Respondents indicating high levels or maximum potential damage with a breach here.*

*** High/most resources allocated for securing these areas.*

DBA—SECURITY SUPERHERO, 2014 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.*

Figure 7: Year-to-Year Percentages Reporting Increased IT Security Spending

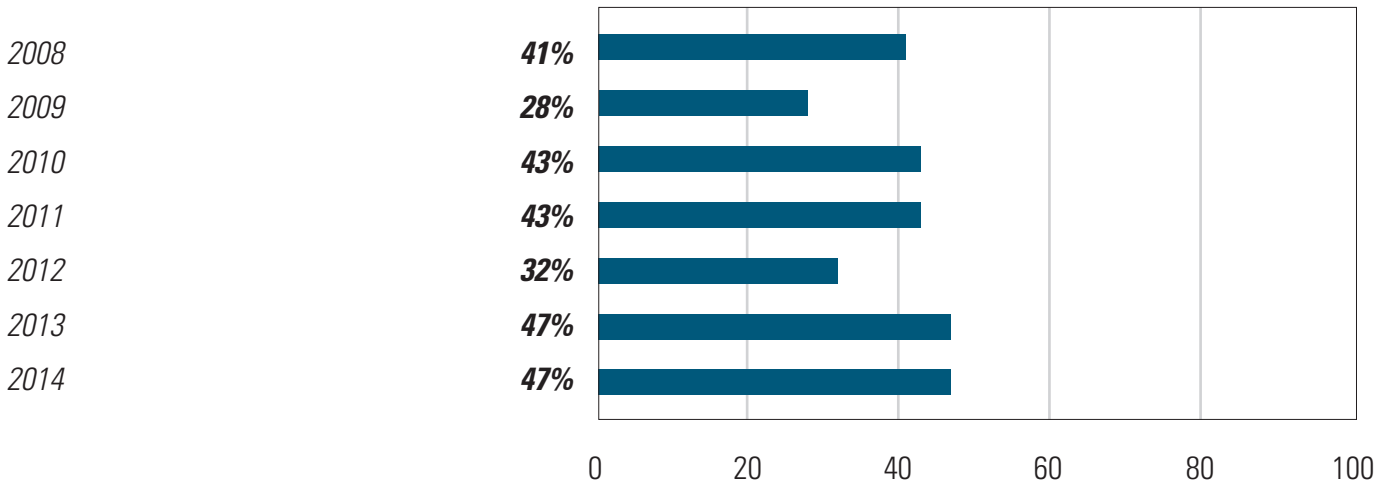
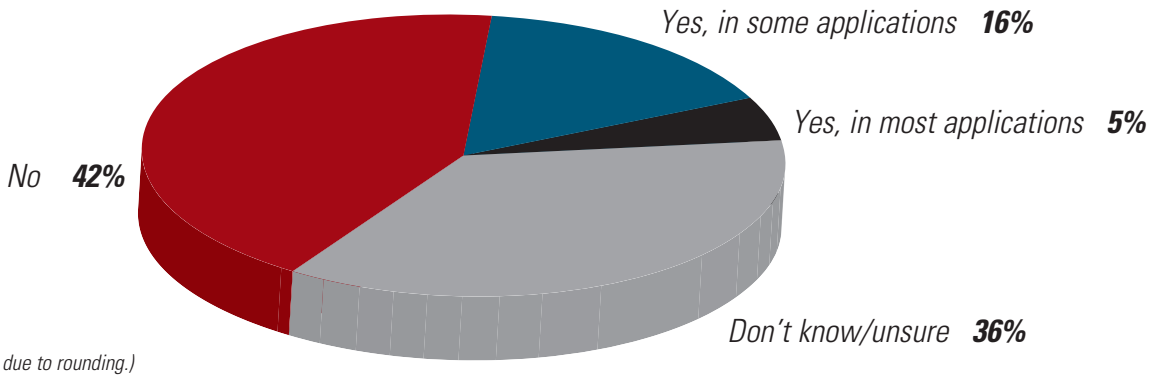


Figure 8: Sensitive Data Unintentionally Disclosed to Enterprise Application/ Business Intelligence Users



(Total does not equal 100% due to rounding.)

DBA—SECURITY SUPERHERO, 2014 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.*

Figure 9: Production Data Used in Non-Production Environments

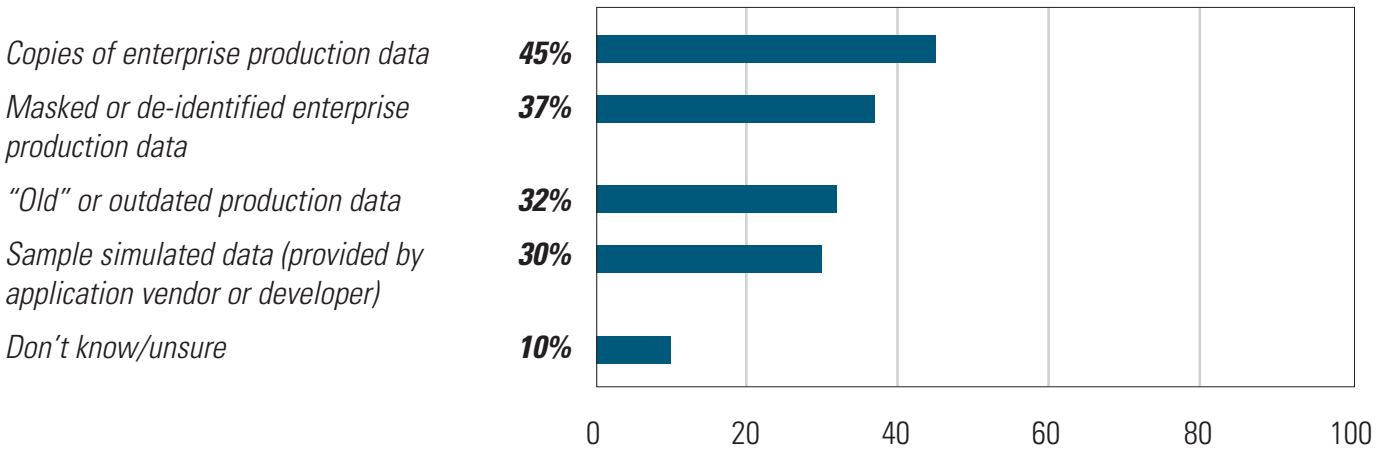


Figure 10: Number of Copies of Production Data

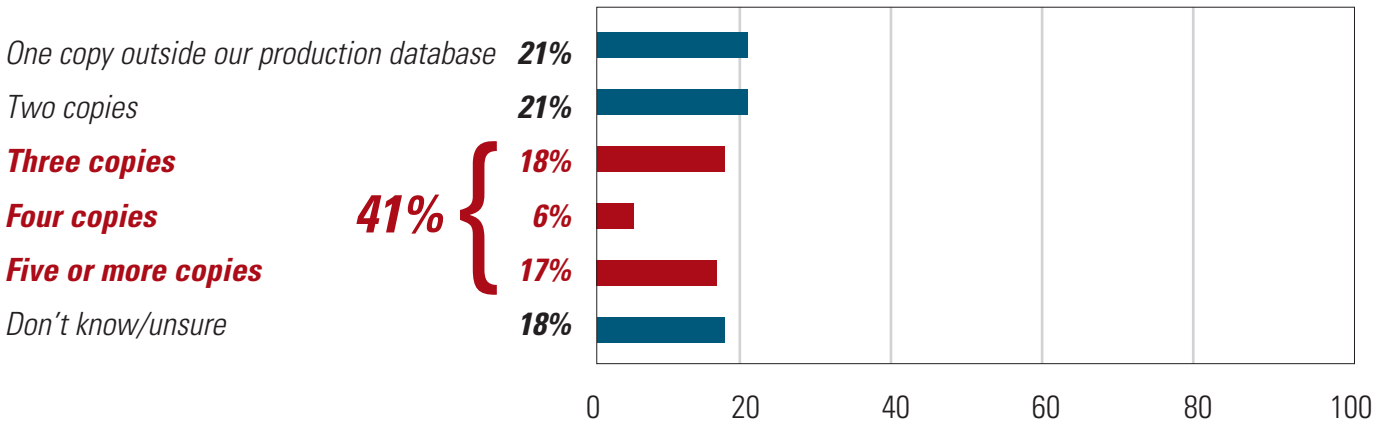
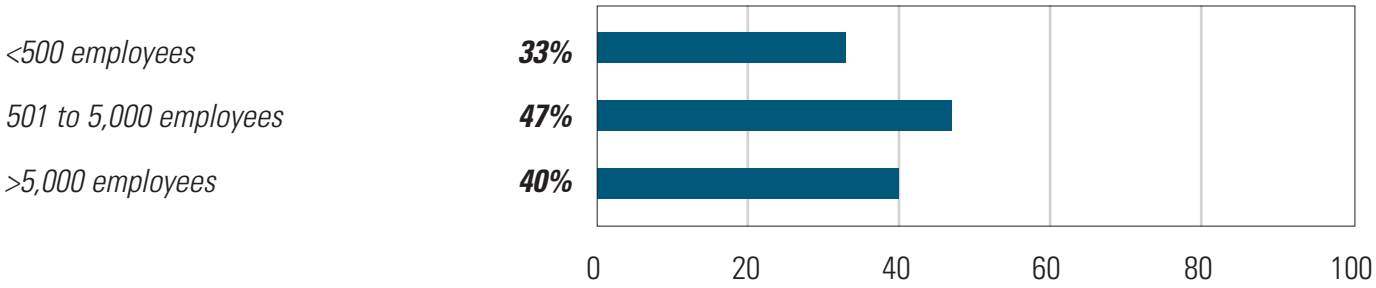


Figure 11: Three or More Copies of Data—By Company Size

(Respondents reporting three or more copies within each size category)



PREVENTIVE CONTROLS

Two-fifths of managers and professionals admit they are not fully aware of where all the sensitive data in their organizations is kept. Those taking proactive measures to lock down data and render it useless to outsiders are still in the minority. Relatively few have safeguards against accidental or intentional staff abuse, and less than one-third have an automated approach to assist their security oversight.

To take the lead in enterprise data security, industry consensus is to follow a defense-in-depth strategy for securing data. The first step is implementing preventive measures, such as encryption, masking, redacting and access controls. The survey finds that these measures are still lacking—as they have been since the first survey in this series was conducted in 2008.

To achieve a robust architecture employing preventive tools, database administrators and security professionals need to understand where sensitive data exists across their organizations. This is often easier said than done, as many organizations have multiple departments with multiple systems. In the current survey, only 61% of respondents claims they know all databases that have sensitive and regulated data. This is down from 70% a year ago, and reflects the increasing complexity of today's enterprise systems, especially with the rise of cloud and digital platforms that may be accessed and managed outside IT's domain. (See Figure 12.) This problem is more acute at larger enterprises, whereas managers and professionals in smaller firms are more likely to be aware of risky data. (See Figure 13.)

The complexity of today's data environments, along with management inertia, may be hampering respondents' abilities to implement full-fledged preventive data protection efforts. About 65% of respondents encrypt data at rest on at least some databases to ensure personally identifiable information is protected—down from 70% in the last survey. An even much lower percentage, 18%, ensure that they have blanket coverage for all key databases in their organization—down significantly from 29% from 2008, the first year this question was asked. (See Figure 14.)

Overall awareness of security measures is down somewhat: The percentage of respondents indicating they "don't know" if measures are taken rose back to 11%—up from 4% last year. The percentage not aware of their security posture declined from 18% in 2008 to 11% in 2012.

Encryption of data at rest is just as likely to be in place at small organizations as it is within large enterprises. (See Figure 15.)

When asked whether organizations are encrypting online or offline backups and exports, a quarter of respondents indicated they do in fact encrypt all data. This is roughly the same as a year ago, but up from 20% in 2008. Overall, a majority of enterprises in the survey, 56%, encrypt at least a portion of database backups. (See Figure 16.)

As indicated previously, 45% of all respondents use copies of production data in non-production environments. Along with encryption, masking sensitive data in non-production database environments, for development, QA and testing, is as important as protecting data in production environments.

Various regulations, such as Payment Card Industry Data Security Standard requirement 3.3, indicate that organizations must redact sensitive data whenever it is displayed. However, 54% either do not, or were not sure whether they were removing sensitive application-layer data. In fact, 11% were not even aware that such a regulation existed. For organizations that say they address this requirement, 16% are using home grown solutions, with another 31% employing third-party or packaged applications. (See Figure 17.)

As discussed in the previous section, human error and internal hacking are two of the most feared security risks, both of which can be limited and even prevented using privilege user access controls. However, close to one-quarter, 71%, have no safeguards or are unsure if they have safeguards to prevent a database administrator or developer from accidentally dropping a table or unintentionally causing harm to critical application databases. (See Figure 18.)

When asked whether organizations could prevent privileged users, such as DBAs, from reading or tampering with sensitive data in business application data, 67% could not, or were unsure. This presents a large issue across the enterprise and should be addressed with privileged user controls. (See Figure 19.)

Data disruptions can occur at many points across today's highly diverse organizations. As one respondent put it: "An unfortunate weakness in our business model are applications which allow and enable elevated access privileges disseminated to technical experts in various departments."

A holistic strategy is often required at multiple levels. "We are currently implementing several security constraints so that data is not directly accessible by any end users and only specific and limited users have access to the databases," says one respondent.

Figure 12: Aware of all Databases With Sensitive or Regulated Information?

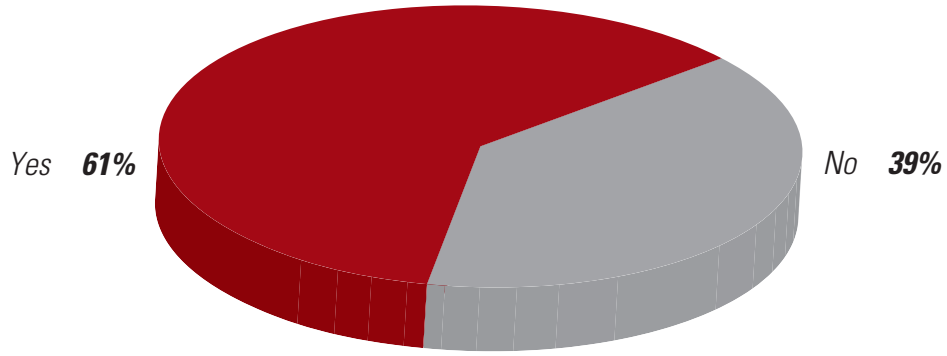


Figure 13: Aware of Sensitive Data in Databases—By Company Size

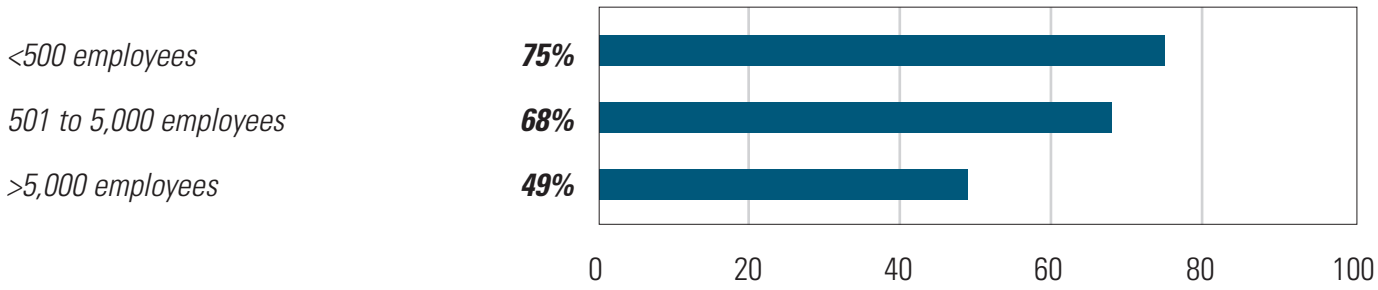


Figure 14: Data at Rest Encryption

	In all databases	In some databases	No	Don't know
2008	29%	28%	25%	18%
2013	20%	50%	26%	4%
2014	18%	47%	24%	11%

DBA—SECURITY SUPERHERO, 2014 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.*

Figure 15: Data at Rest Encryption—By Company Size

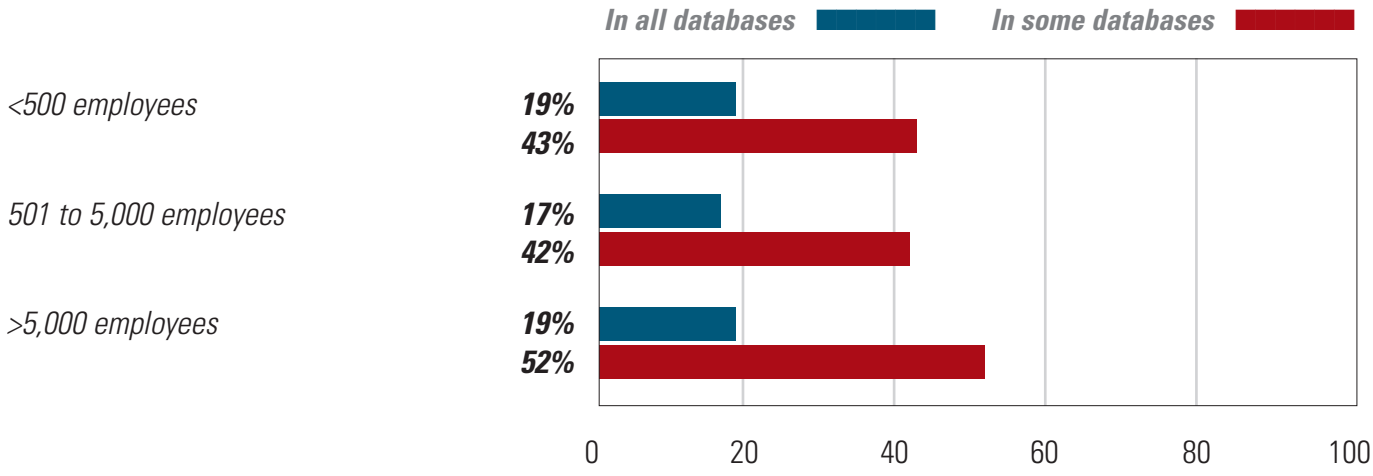


Figure 16: Database Backup and Export Encryption

	In all databases	In some databases	No	Don't know
2008	20%	32%	55%	25%
2013	27%	38%	29%	6%
2014	25%	31%	32%	13%

DBA—SECURITY SUPERHERO, 2014 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.*

Figure 17: How Sensitive Data is Masked to Meet Mandates and Regulations

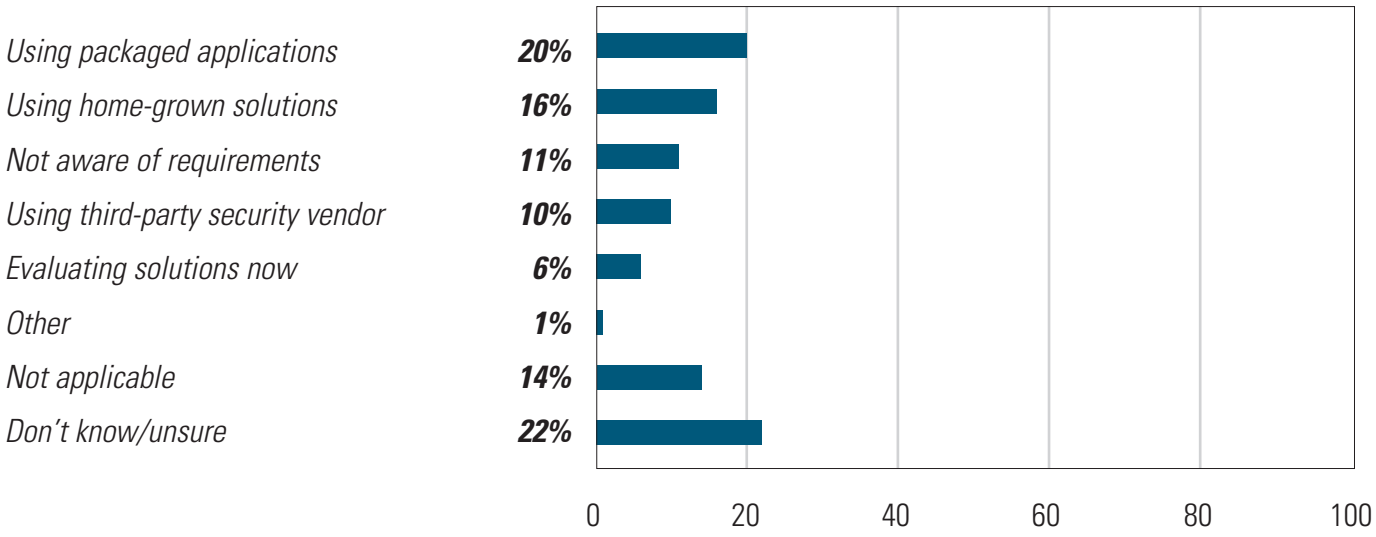
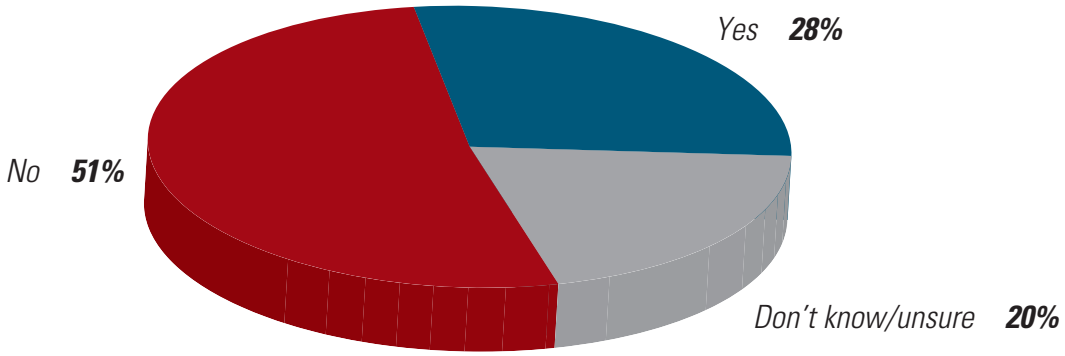


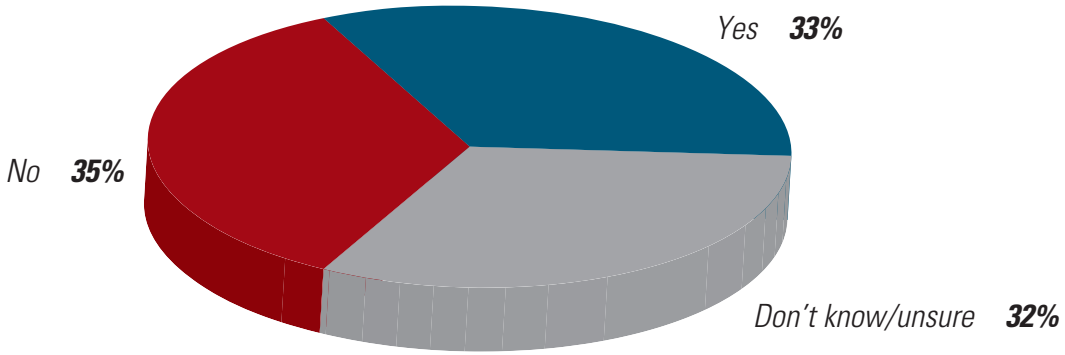
Figure 18: Safeguards Against Accidental Harm to Databases and Applications?



(Total does not equal 100% due to rounding.)

DBA—SECURITY SUPERHERO, 2014 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.*

Figure 19: Able to Prevent Privileged Users from Reading or Tampering with Sensitive Business Information?



DETECTIVE CONTROLS

Organizations are still not doing enough to monitor their data assets or keep tabs on super-users. Only about one-third can prove abuse of data assets. In a world where data can be distributed globally within seconds, two-thirds of managers estimate that it would take a matter of days to remediate a breach, or simply don't know what length of time would be involved.

Preventing cybercriminals from accessing sensitive data should be the foundation of a defense-in-depth strategy, and detective controls provide the forensics that capture characteristics of the attack as they occur. However, there has been little progress in enterprises being able to prove that privileged database users were not abusing their super-user privileges—35% this year, down from 39% a year ago. (See Figure 20.) Likewise, only 35% say they are able to detect unauthorized changes across most databases. (See Figure 21.)

The difficulties in fully securing data against administrator or privileged user abuse was illustrated by one respondent, who noted that "the simplest way is to implement tough security standards so all the DBA accounts get locked out." Of course this is impractical and there must be an appropriate and practical balance between data security and the business.

In today's networked society, data breaches can occur at lightning speed. Unfortunately, the average amount of time to detect and correct security events is increasing. A total of 31% say it would take less than one business day to rectify a breach, down from 37% a year ago and 45% in 2010. Two-thirds say it may take days, or simply don't know how long remediation will last. (See Figures 22 and 23.)

There has been relatively little progress in the percentage of respondents taking measures to guard against direct database network attacks such as SQL injection attacks, considered to be the most common database threat by security experts. In 2010, the first year this question was asked, 35% of respondents had taken steps to prevent these kinds of attacks. This year, 38% report taking such actions. Along with privilege escalation, monitoring database network attacks such as SQL injection attacks is a continuing threat. (See Figure 24.)

Such monitoring requires a broad view across multiple systems, database and applications, a task that is complicated by the complexity of today's IT environments. As one respondent put it: "We educate our developers and QA testers on how to check for SQL injection attacks. Even so, it would be too much to claim we have it covered for all applications across all web platforms."

This does not suggest that respondents have thrown their hands up at the challenge, however. There are many proactive measures underway to keep tabs on security incidents across enterprises. Respondents are taking a number of other measures to address security holes in their data infrastructure, including the monitoring of a range of functions.

About half of enterprises in the survey, 48%, employ tools to help monitor and identify possible anomalies in databases that may suggest suspicious activity. (See Figure 25.) However, only 32% do so on a regular, automated basis, a level that has changed little since the first survey in this series was commissioned six years ago. (See Figure 26.)

The various monitored database activities are highlighted in Figure 27. Unfortunately, less than half of organizations watch for sensitive activities that include database login and logouts, as well as sensitive database table reads and writes. As well, 24% manually monitor their environment, which can be time consuming and error prone, especially within smaller organizations that have limited resources.

Figure 20: Can Prove Privileged Users Were Not Tampering

	2010	2012	2013	2014
Yes	32%	26%	39%	35%
No	39%	48%	43%	43%
Don't know/unsure	28%	25%	19%	22%

Figure 21: Detect Unauthorized Database Changes?

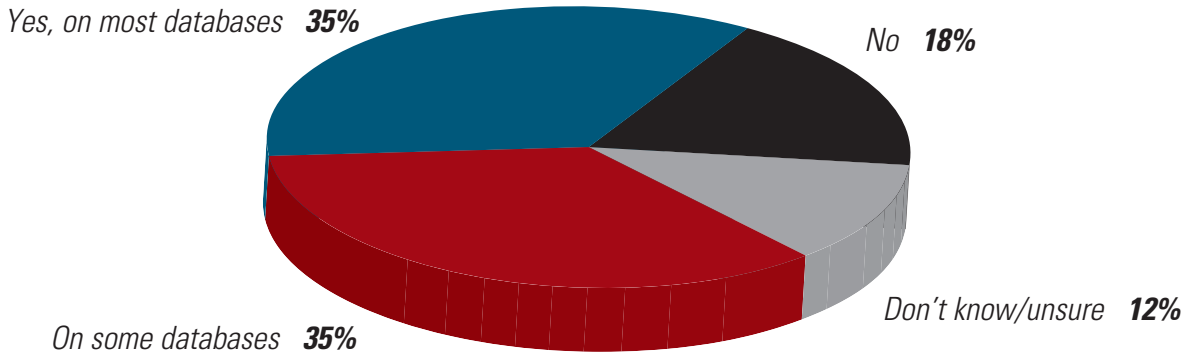


Figure 22: Length of Time to Detect and Correct Unauthorized Database Access or Change

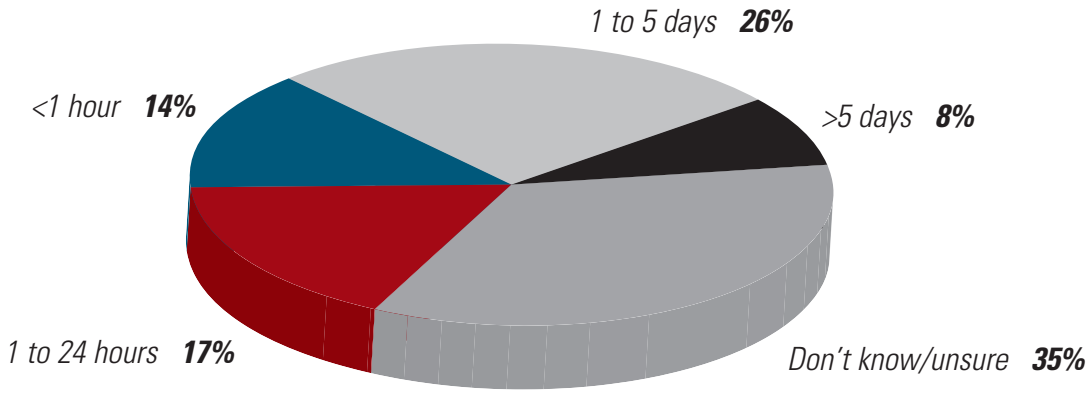


Figure 23: Percentage Respondents Reporting It Would Take Less Than a Day to Detect and Correct Unauthorized Changes

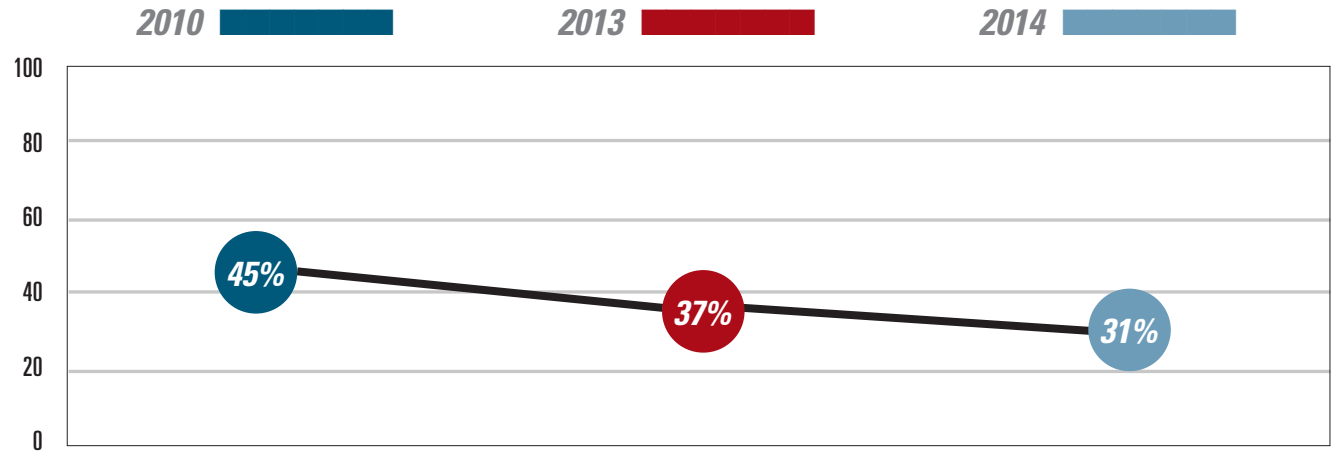


Figure 24: Taken Steps to Prevent SQL Injection Attacks?

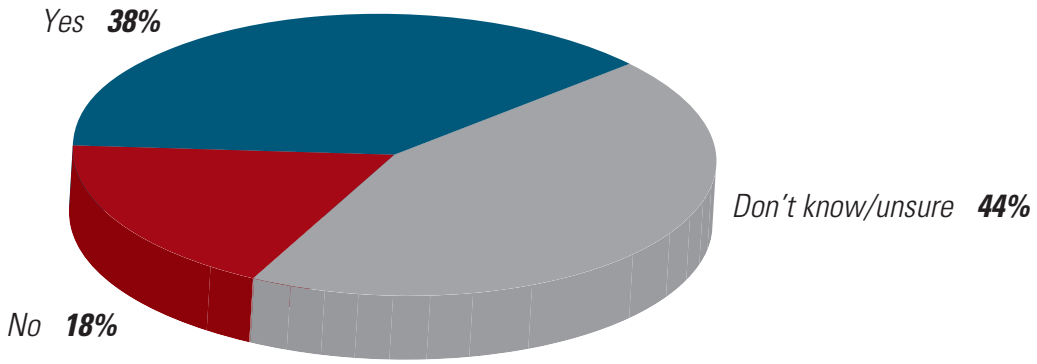


Figure 25: How Data Security Monitoring is Conducted

(For security Issues such as unauthorized access to data or configuration changes)

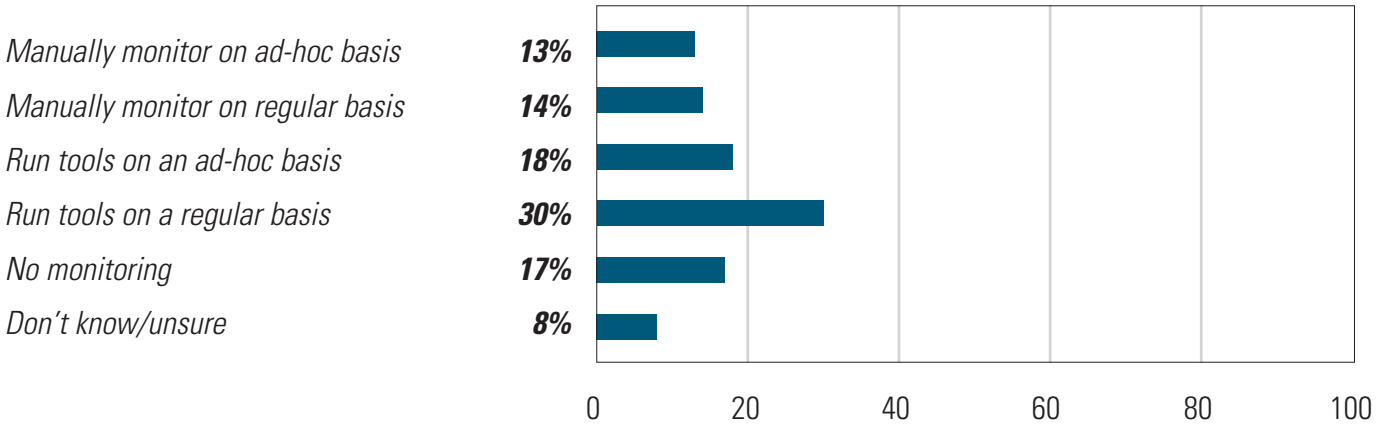
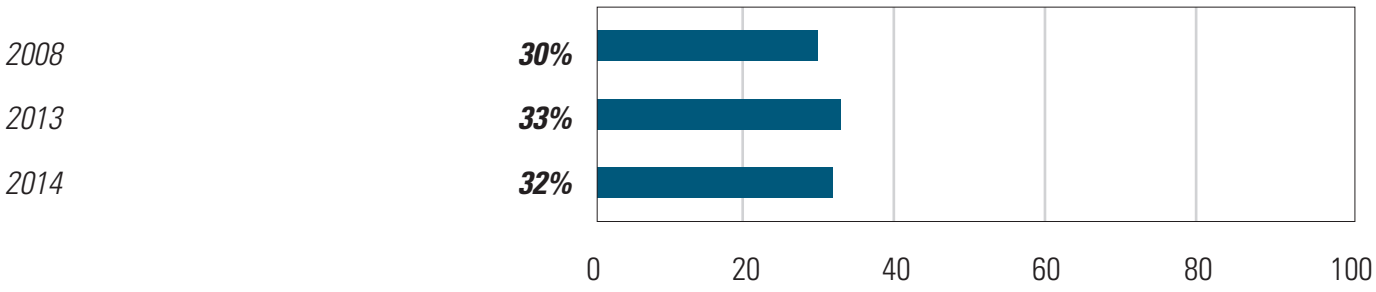
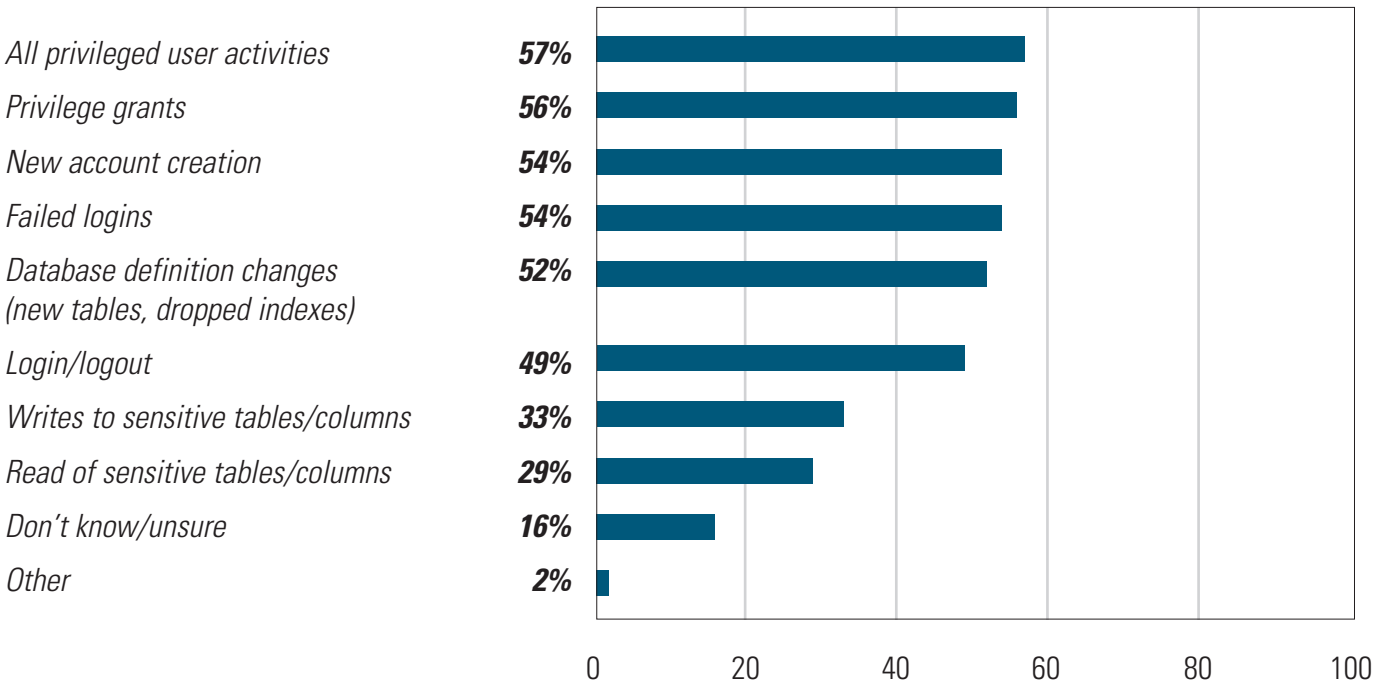


Figure 26: Use of Tools for Data Security Monitoring on a Regular Basis



DBA—SECURITY SUPERHERO, 2014 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.*

Figure 27: Database Activities Monitored



ADMINISTRATIVE CONTROLS

Data security audits still remain few and far between. Only one-sixth review their data assets at least on a monthly basis.

The ability to continually audit and assess evolving data security threats is another area where database managers and security professionals can provide high value to their organizations.

However, the survey indicates that administrative measures to pull and review database activity remains only an occasional activity. After a bump in last year's survey, the percentage of enterprises conducting frequent audits (once a month or more) remains at low, stagnant levels—16%, the same as four years ago, the first time this question was asked. (See Figures 28 and 29.)

There has not been appreciable movement in terms of audits. The percentage saying they "never" conduct security audits or don't know stands at 28%, in line with a year ago (27%), but down from 35% in 2010. While many respondents' enterprises conduct auditing, it is often inconsistent. As one respondent put it: "Extensive Auditing is enabled for the activities performed by all privileged users. These logs will be reviewed time to time."

Additional gauges of administrative controls over data security include the length of time it takes to prepare for a security assessment or audit, compliance with mandates or regulations. This is key to the agility of the data security process. Database security audits can follow an intensive process depending on whether the process is manual or automated. Overall, 26% of respondents say it takes less than one day to prepare for an audit, down from 37% in last year's survey. Enterprises have been slipping backwards on this front, suggesting the increasing complexity and degree of overworked IT staffs that decrease the agility of this process. (See Figure 30.)

One out of eight respondents indicate that recent compliance audits have flagged database security issues at their sites. (See Figure 31.) While data security is an ongoing and pressing concern, only 26% apply Oracle Critical Patches as they are released. (See Figure 32.)

Figure 28: Frequency of Data Security Audits

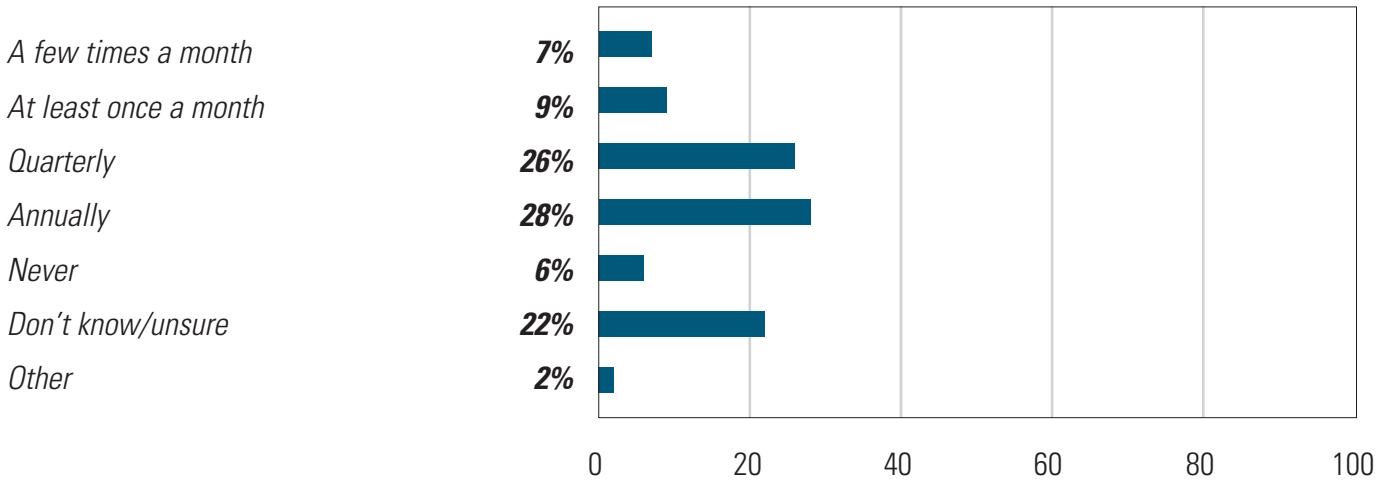


Figure 29: Percentage of Respondents Conducting Frequent Audits

(Multiple times a month to at least once a month)

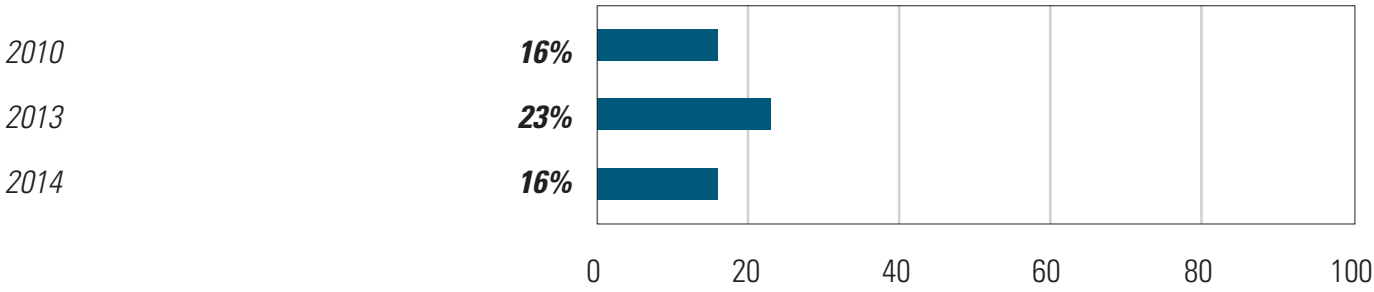


Figure 30: Length of Time to Prepare Database Security Assessment/Audit

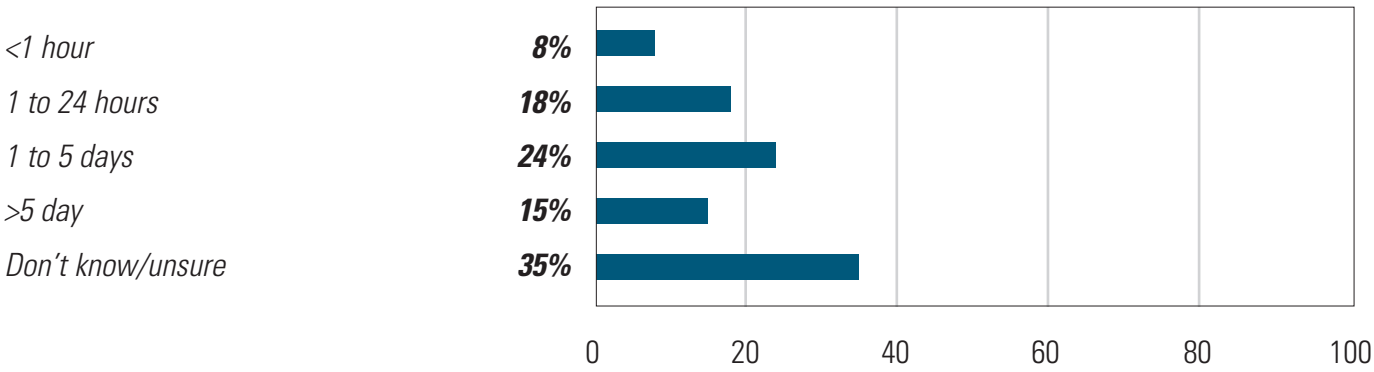
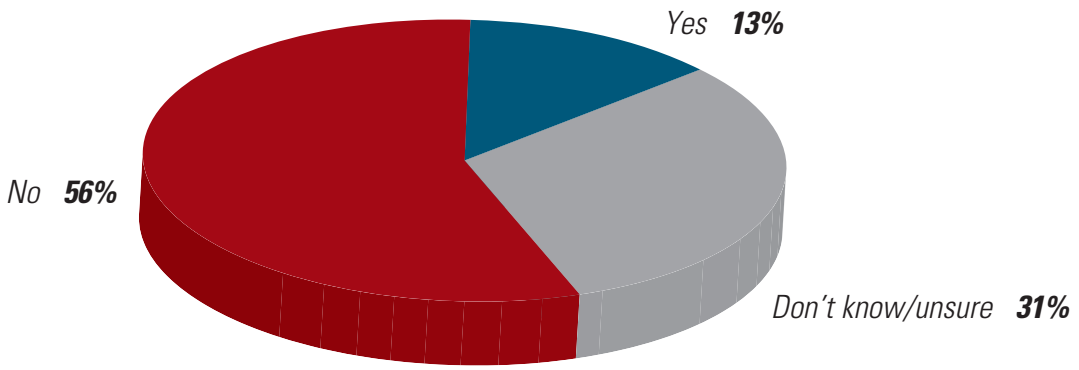
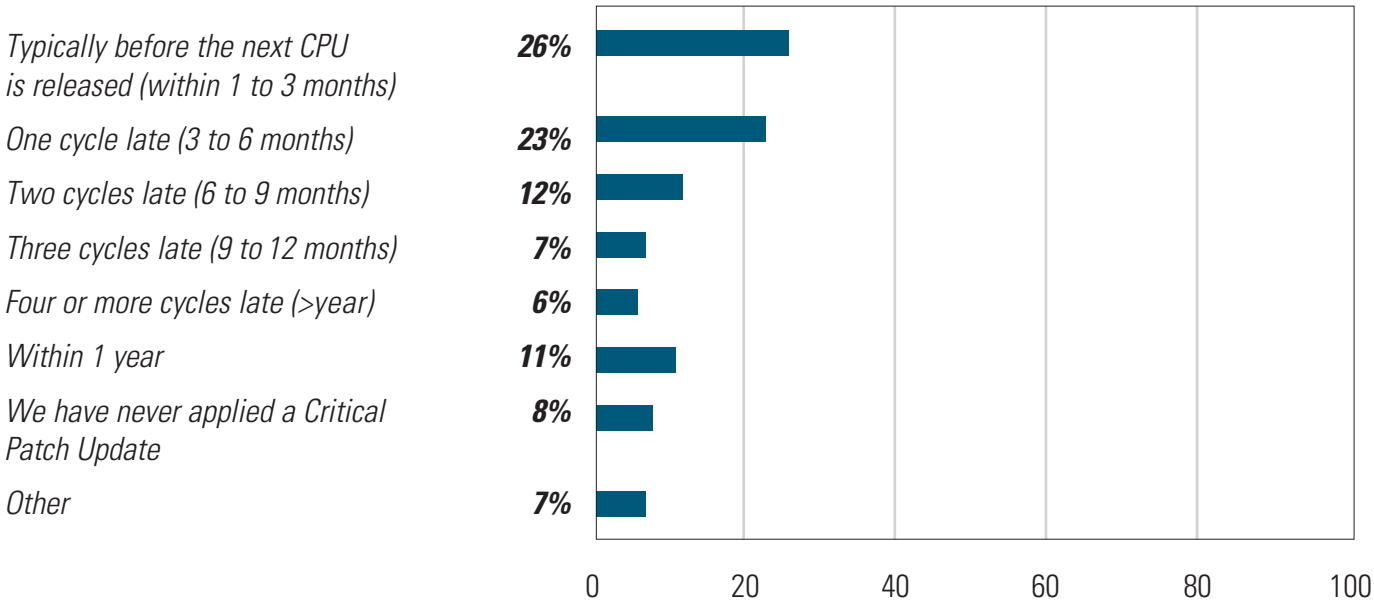


Figure 31: Have Regulatory Compliance Audits Over the Past Months Flagged Any Database Security Issues?



DBA—SECURITY SUPERHERO, 2014 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.*

Figure 32: How Quickly Are Quarterly Oracle Critical Patch Updates Applied to All Databases?



CALL TO ACTION

Data security is not just a technical challenge; it is an enterprise business challenge. Nearly 70% of the IOUG respondents indicate that the database group is responsible for data security within their organization. However, data security is arguably everyone's responsibility. As stewards of sensitive customer and organizational data, it is the database group's responsibility to step forth and educate the business on the mandate to secure data. The superhero DBA must balance service level agreements for performance and availability, with the often-neglected requirements for data security.

Senior executives are only too painfully aware of what's at stake for their businesses, but often don't know how to approach the challenge. This is an opportunity for database administrators and security professionals to work together, take a leadership role, and move the enterprise to take action. The following steps need to be taken:

Understand business leaders' concerns. Communicate with business leaders in order to understand their data challenges and security concerns. Share with them the likelihood of a security breach and learn what they deem as the most sensitive data. Data security is an organizational issue that requires open communications and business involvement.

Educate the business. As the steward of data, a superhero DBA must take a proactive stance, and educate the business about the risks, and how to address those risks.

Use data metrics to make change. It all begins with providing metrics to help leaders prioritize data security versus their other responsibilities. By using the IOUG data security survey results to educate the business, database and security professionals offer substantial evidence of data security's greatest risks and industry trends.

Emphasize prevention. More preventative measures—such as data encryption and redaction—need to be in place in order to stop malicious hackers in their tracks.

Audit and monitor frequently. More auditing and monitoring needs to take place, so malicious acts do not continue unabated for lengthy periods of time. Only 30% of enterprises employ tools and processes to automate scanning for anomalies. New technology on the market relieves many of the manual burdens associated with database monitoring.

Trust, but verify. At some point we need to trust our IT staff; however, we also need to verify they, and the use of their credentials, are trustworthy. Stolen credentials from superusers are a common attack vector. Therefore, it is important to follow the practice of separation of duties and least privilege. Sixty-five percent of organizations could either not prove, or are unsure, whether privileged users were tampering with sensitive data. There needs to be cross-checking of privileged access.

Within today's enterprises, no other type of professional is better equipped or more knowledgeable to deal with data security than database professionals. These superheroes understand where the risks are, and how these risks can ultimately affect their organization. In an era in which information is the most precious resource, database professionals must take a leadership role in helping to prepare and protect these assets. With great power, comes great responsibility.

DBA—SECURITY SUPERHERO, 2014 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.*

DEMOGRAPHICS

Figure 33: Respondents' Organizations—By Number of Employees

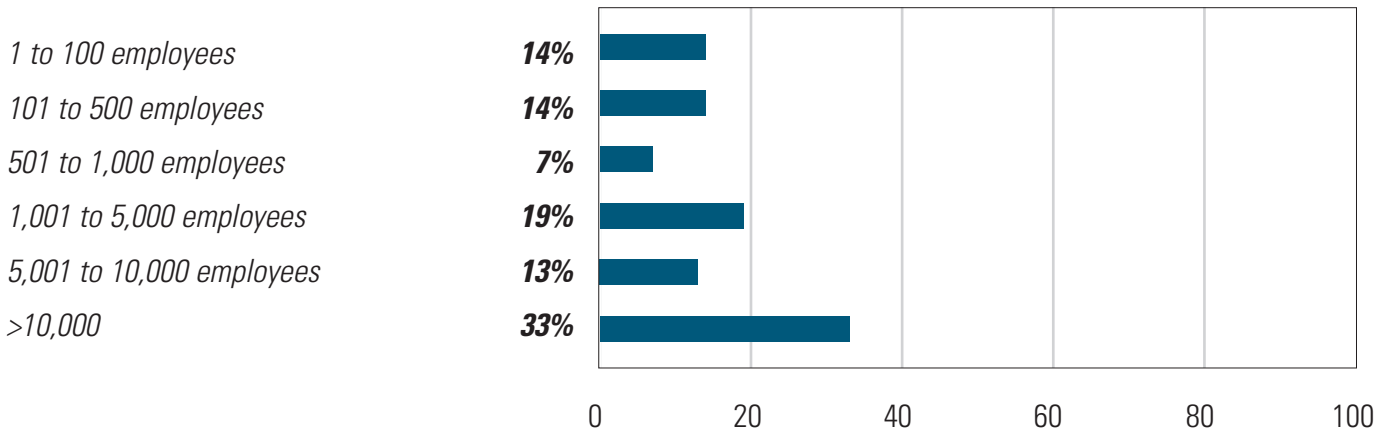


Figure 34: Number of Databases at Respondents' Sites

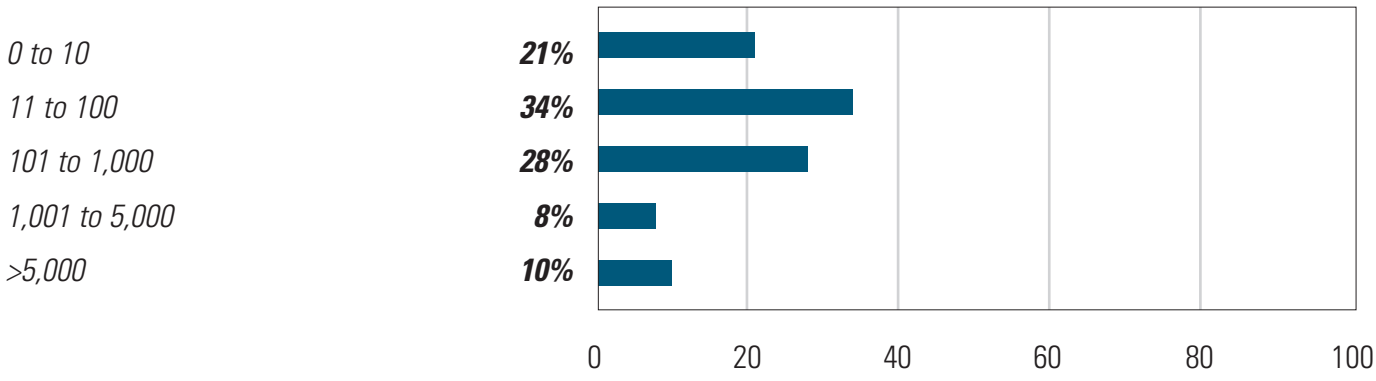


Figure 35: Respondents' Primary Job Titles

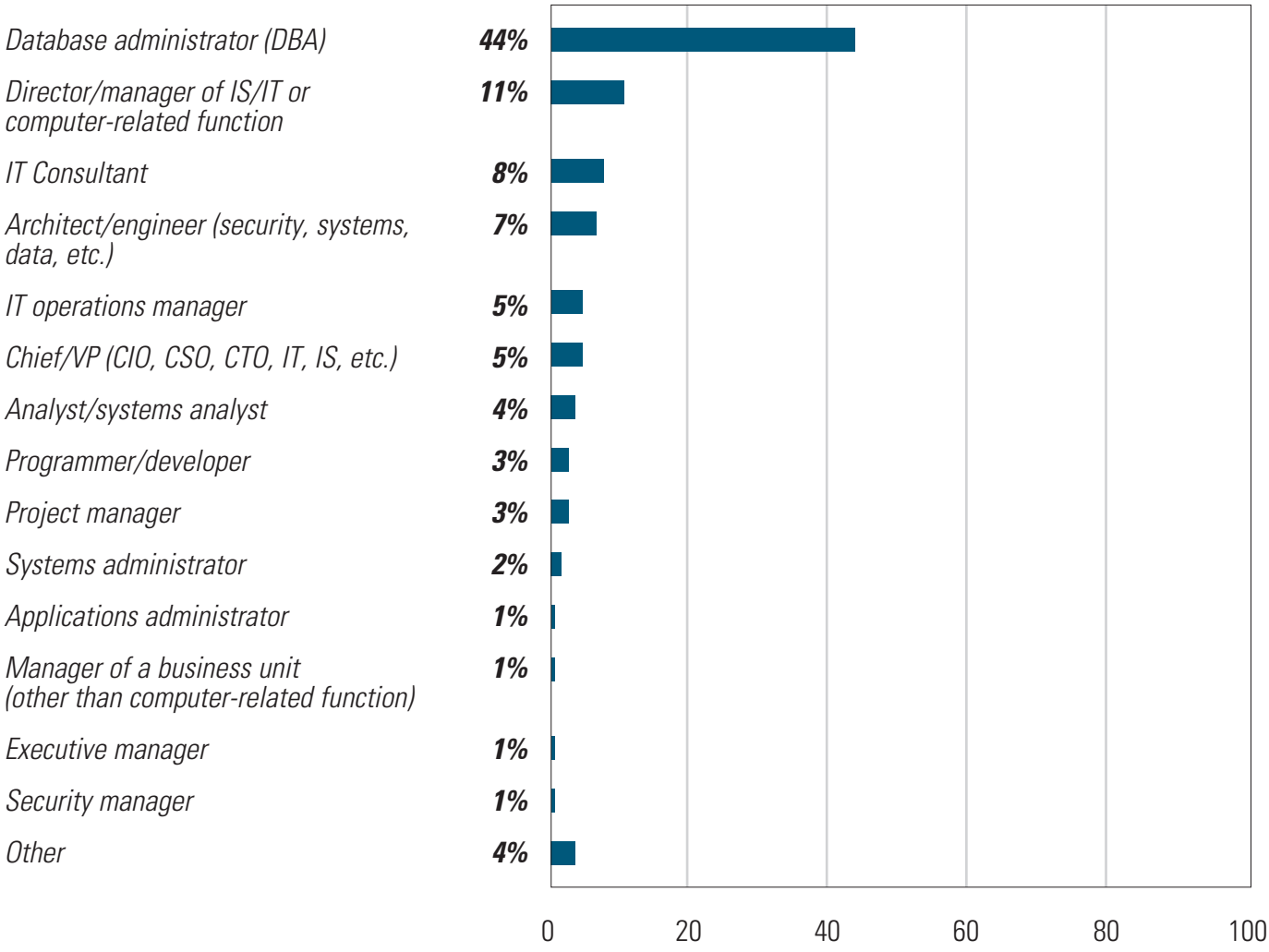


Figure 36: Respondents' Primary Industries