

DATA SECURITY AT AN INFLECTION POINT: 2011 SURVEY OF BEST PRACTICES AND CHALLENGES

By Joseph McKendrick, Research Analyst
Produced by Unisphere Research, a Division of Information Today, Inc.
December 2011

Sponsored by **APPLICATION
SECURITY, INC.**

Produced by  **UNISPHERE[®]**
RESEARCH
Delivering Certainty
Thomas J. Wilson, President

TABLE OF CONTENTS

<i>Executive Summary</i>	3
<i>Insecure Times</i>	4
<i>Breaches</i>	11
<i>Organizational Concerns</i>	15
<i>Compliance and Controls</i>	23
<i>Auditing and Monitoring</i>	27
<i>Solutions</i>	32
<i>Demographics</i>	36

EXECUTIVE SUMMARY

There's no question that data security has become a major concern for many enterprises, particularly since the internet opened up for business almost two decades ago. In recent times hackers have grown increasingly sophisticated, and able to target enterprises with an array of approaches, ranging from outright intrusions to the release of viruses and malicious code that either brings down networks, or sits stealthily, collecting sensitive data. While awareness of these external threats has heightened—even at the boardroom level—enterprises still engage in lax practices regarding the way data is moved around within the organization, and out to external business partners.

These are some of the findings from a new survey of 524 enterprise IT and data managers, conducted by Unisphere Research, a division of Information Today, Inc., and sponsored by Application Security, Inc. (AppSecInc). Emails were sent to subscribers of *Database Trends and Applications*, as well as AppSecInc customers, which directed them to the survey instrument posted on a website. The survey was conducted in October 2011.

Key findings from the study include the following:

- Risks to databases have only increased in recent years, an overwhelming majority of respondents agree. Hackers and other malicious third parties are becoming bolder and more technically proficient, making the jobs of data managers increasingly difficult. While many data managers have lost sleep over the years worrying about data security, recent high-profile hacker attacks have put organizations even more on guard. In addition, data security has gained more attention from management.
- Close to one-third know or suspect their organizations may have experienced a data breach, and even more expect a data breach over the coming year. However, few understand the costs of such breaches to their organizations.
- Organizational issues impede efforts to address database security. In most cases, security is overseen by both database and security teams. Adding to the challenge is the need to store data for long periods of time—a majority of respondents maintain data well beyond the required storage limits. One

out of four respondents now maintains data environments within private clouds, but a majority are concerned about security in these environments as well.

- Respondents are divided as to whether their organizations' existing data security controls provide an adequate level of protection against database breaches and attacks. Most companies have multiple copies of production data in their enterprises, and often don't have direct control of all copies.
- Database security audits are few and far between. When audits are conducted, issues typically uncovered include access control and configuration mistakes.
- Vendors' security patches are applied infrequently. Monitoring and configuration solutions are prevalent, but other security technologies such as encryption are only seen at a minority of companies.

Respondents are predominantly Microsoft SQL Server and Oracle shops, with about one-third also running MySQL. The largest segment of respondents, 24%, are database administrators, while 19% are IT executives and managers and 18% are developers and analysts. Respondents represent a range of organizations, from small firms with fewer than 100 employees (17%) to large organizations with more than 10,000 employees (30%). A wide range of industry groups is also represented, including IT service and software firms (19%), government agencies (16%), financial services (15%), and education (8%). (See Figures 41 to 44.)

As will be discussed throughout this report, data security not only relies on good technology, but also effective and committed management. The ability to “sell” data security best practices to management is often a challenge for IT and data executives and managers. “We face a lack of urgency in data security at all levels of management, including the CEO and CIO,” says one respondent. “Our database security has been ad hoc and delivered primarily through one individual. We face huge risk through unsecured web applications, unmonitored database activity, and poorly and undefined security mandates.”

On the following pages are the latest findings on how enterprises are responding—or not responding—to these challenges.

INSECURE TIMES

Risks to databases have only increased in recent years, an overwhelming majority of respondents agree. Hackers and other malicious third parties are becoming bolder and more technically proficient, making the jobs of data managers increasingly difficult. While many data managers have lost sleep over the years worrying about data security, recent high-profile hacker attacks have put many organizations even more on guard. In addition, data security has gained more attention from management.

An overwhelming majority of respondents agree that the overall risks to data security have increased over the last three years. In total, 81% believe the risk picture has risen “significantly” or “somewhat” over the past three years. (See Figure 1.) Those professionals involved in security or auditing roles tend to see the picture more darkly—82% say the risk is more significant, versus 74% of database managers. (See Figure 2.)

Many blame the increasing boldness and technical abilities of outside hackers, who, unfortunately, appear to be getting smarter. (See Figure 3.) Hackers have grown more sophisticated, developing malicious code capable of hiding within servers and PCs for extended periods of time. In addition, phishing attacks have increasingly grown more ambitious and targeted.

Among the minority of respondents who say the risk has actually lessened in recent times, the improved situation is attributed to having more internal rules/procedures to deter internal hackers/errors, as well as better tools from their vendors. (See Figure 4.)

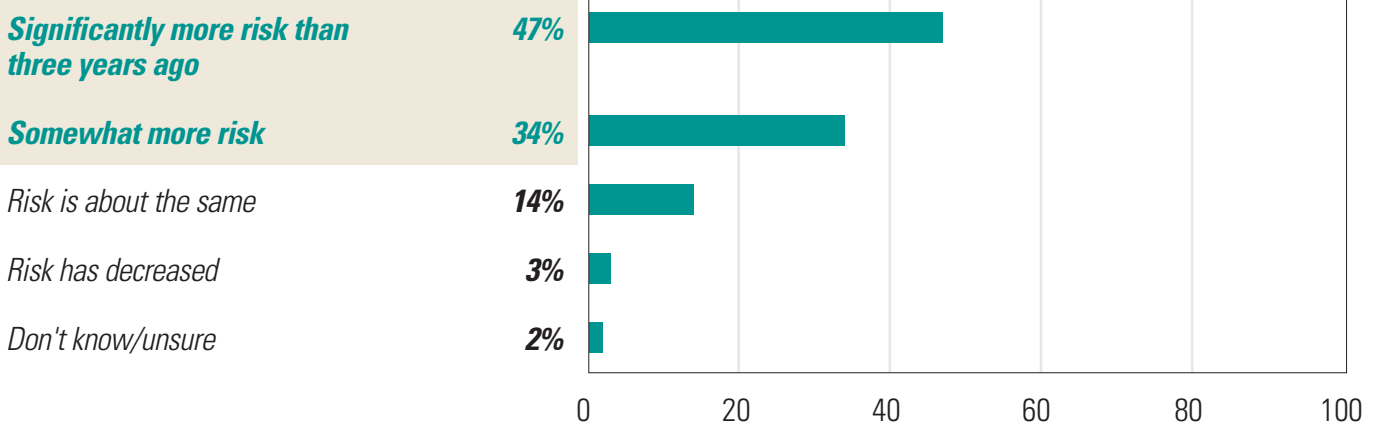
The recent barrage of security attacks by outside hackers—such as Anonymous and LulzSec—has caused more than half

the respondents’ organizations to step up their data security efforts. A majority, 51%, report that news of these high-profile attacks has resulted in ramping up data security “significantly” or “somewhat” in recent times. (See Figure 5.)

Where has this concern manifested itself? In the largest number of cases, organizations have stepped up the frequency of audits, and at least one-third report that these security issues have caught the attention of top management and board members. (See Figure 6.)

The ever-present threat of external hackers dominates this concern, cited by a majority (54%) of respondents. However, three out of five say internal errors continue to be their greatest threat. (See Figure 7.) The perception of threats also varies by the job role of the respondent. For example, DBAs in the survey are more concerned about human error and insider abuse than those directly involved with security and auditing (73% versus 52%). However, security and audit professionals are more likely to view the mishandling of storage media and abuse by privileged IT staff as vulnerabilities. (Thirty-nine percent of security pros see this as a risk, versus 29% of DBAs.) (See Figure 8.)

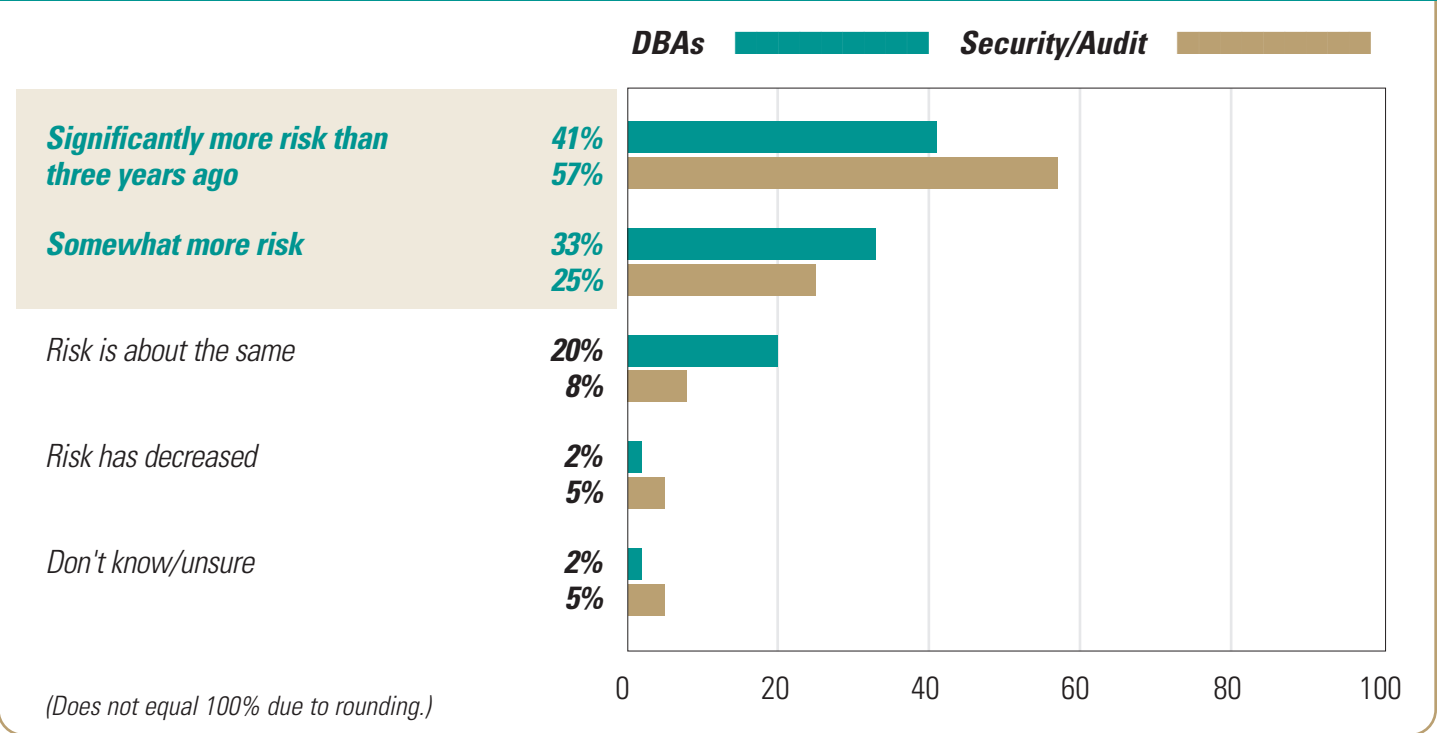
Figure 1: How Data Security Risks Have Changed Over Last Three Years



Data Security at an Inflection Point: 2011 Survey of Best Practices and Challenges was produced by Unisphere Research and sponsored by Application Security, Inc. 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, 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.

Figure 2: How Data Security Risks Have Changed—By Job Role

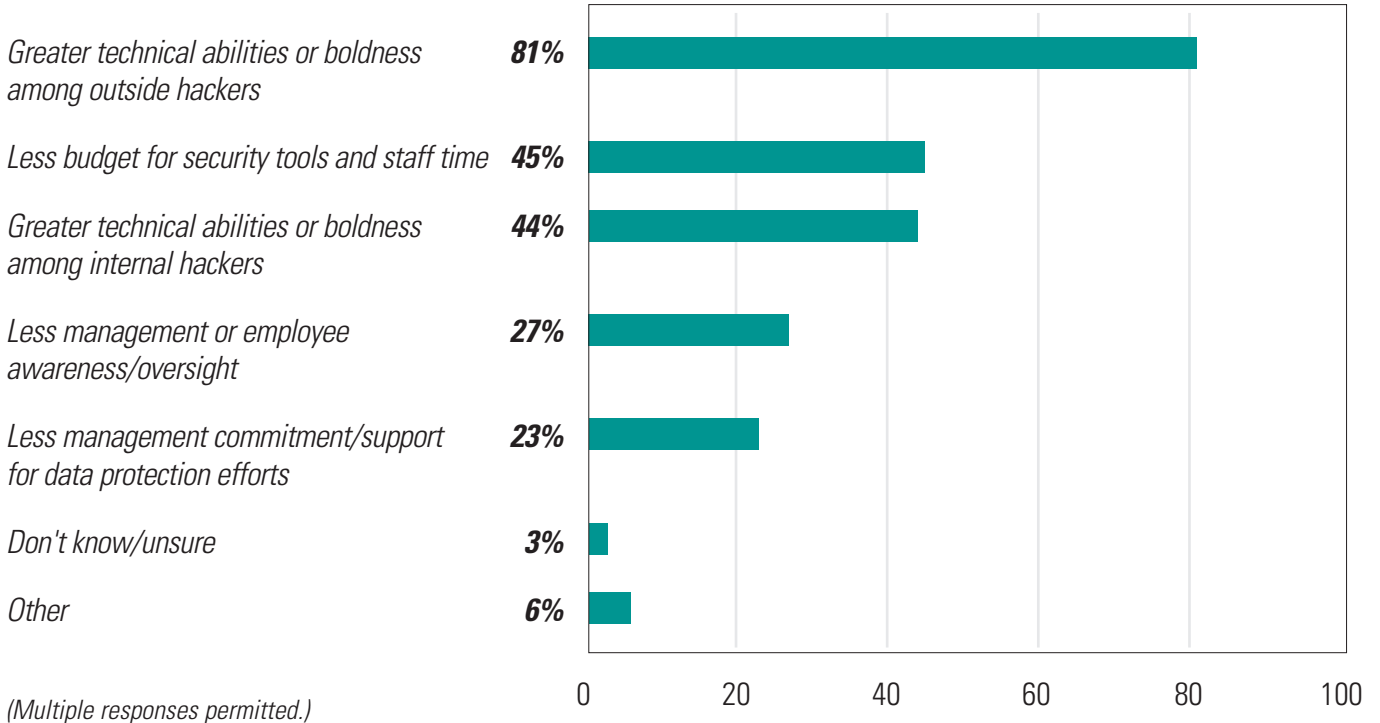


Data Security at an Inflection Point: 2011 Survey of Best Practices and Challenges was produced by Unisphere Research and sponsored by Application Security, Inc. Unisphere Research is the market research unit of Unisphere Media, a division of Information Today, Inc., publishers of Database Trends and Applications magazine and the 5 Minute Briefing newsletters. To review abstracts of our past reports, visit www.dbta.com/research. Unisphere Media, 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.

Figure 3: Factors Increasing Data Security Risks

(Among respondents that feel there is greater risk)

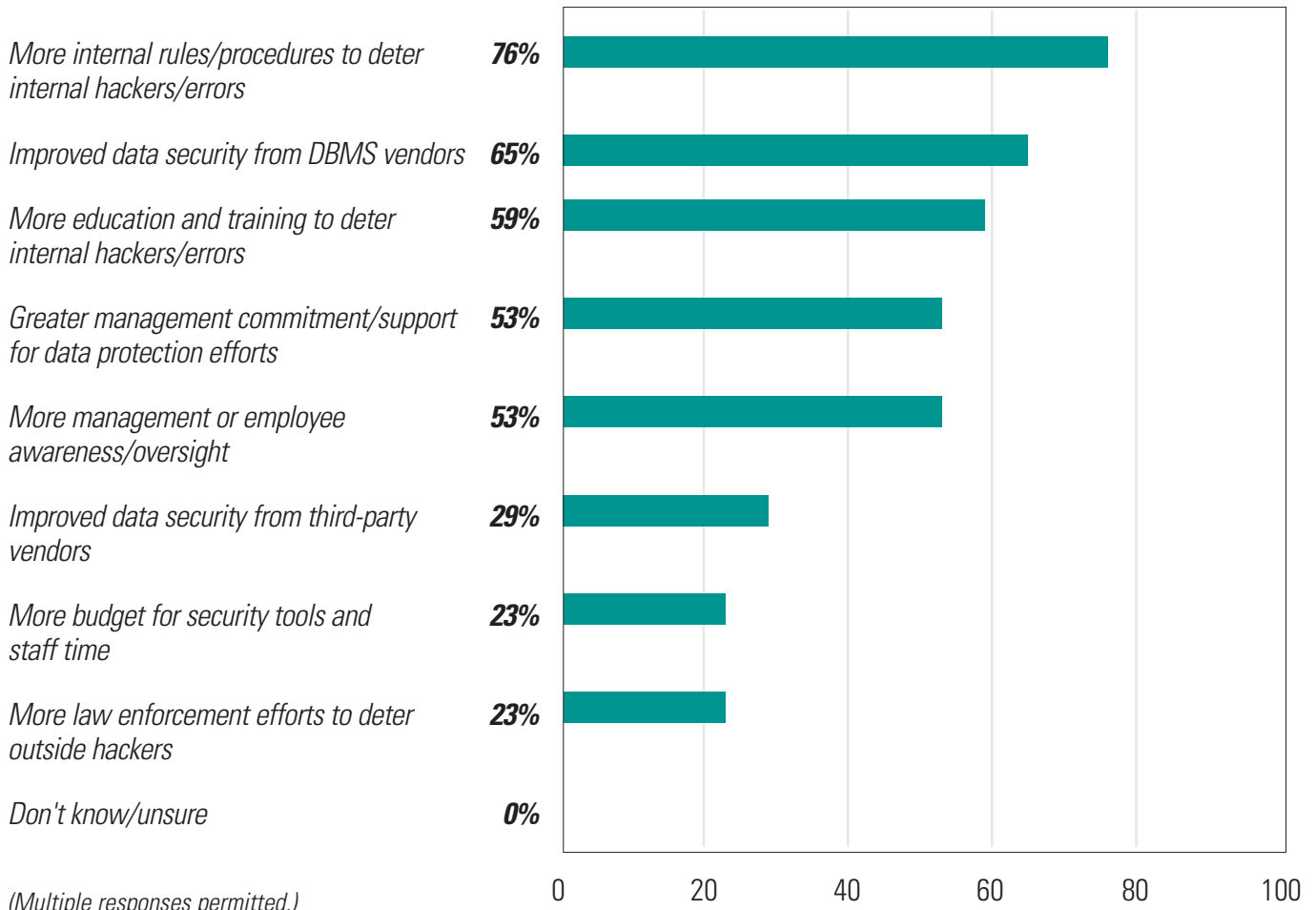


Data Security at an Inflection Point: 2011 Survey of Best Practices and Challenges was produced by Unisphere Research and sponsored by Application Security, Inc. Unisphere Research is the market research unit of Unisphere Media, a division of Information Today, Inc., publishers of Database Trends and Applications magazine and the 5 Minute Briefing newsletters. To review abstracts of our past reports, visit www.dbta.com/research. Unisphere Media, 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.

Figure 4: Factors Decreasing Data Security Risks

(Among respondents that feel there is lesser risk)



Data Security at an Inflection Point: 2011 Survey of Best Practices and Challenges was produced by Unisphere Research and sponsored by Application Security, Inc. 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, 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.

Figure 5: Have Recent High-Profile Attacks Resulted in Stepped-Up Data Security?

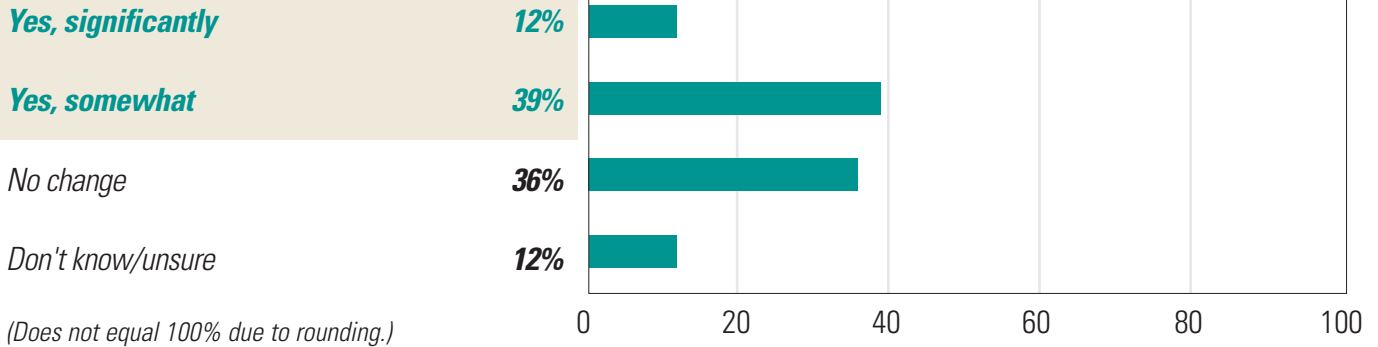
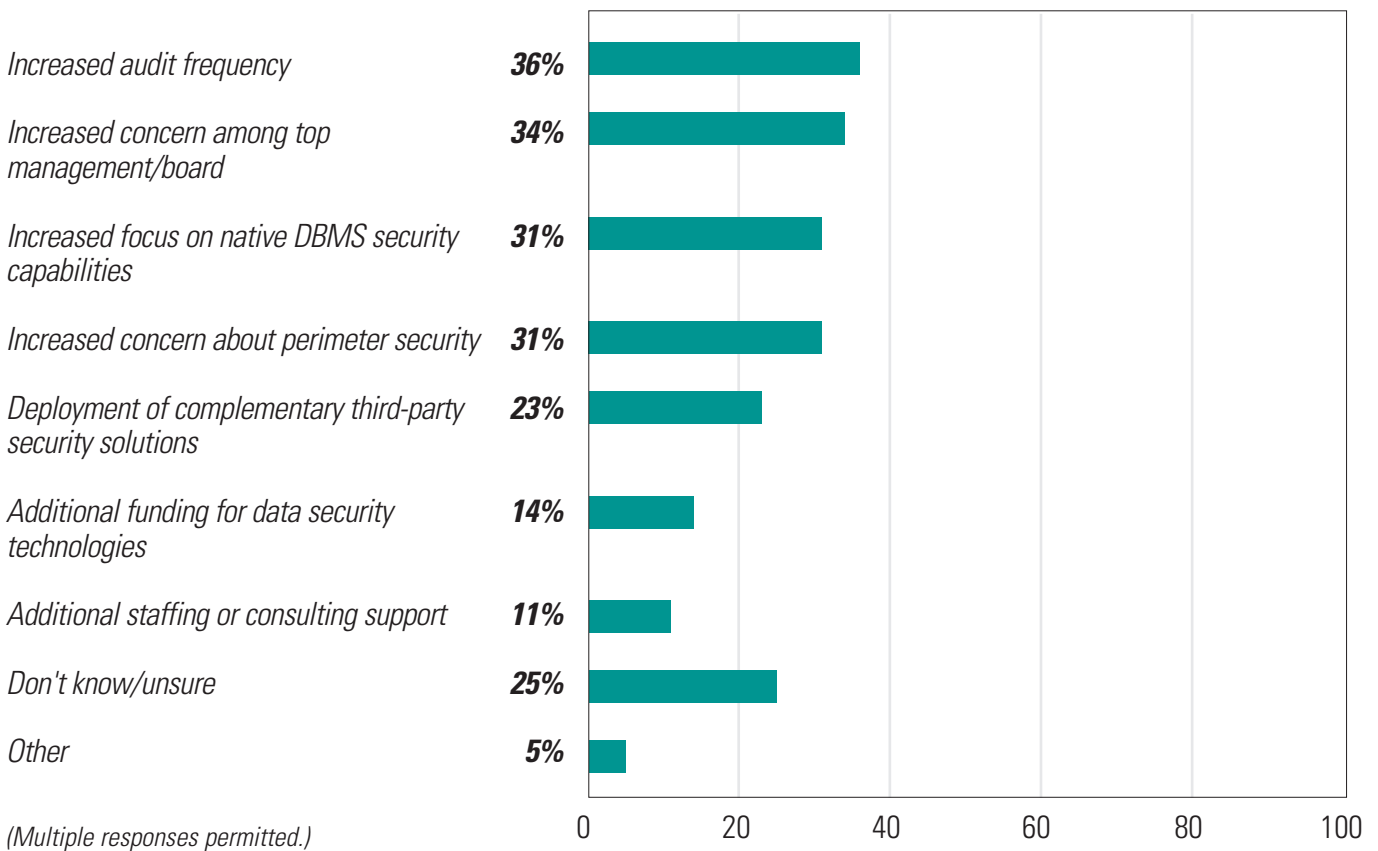


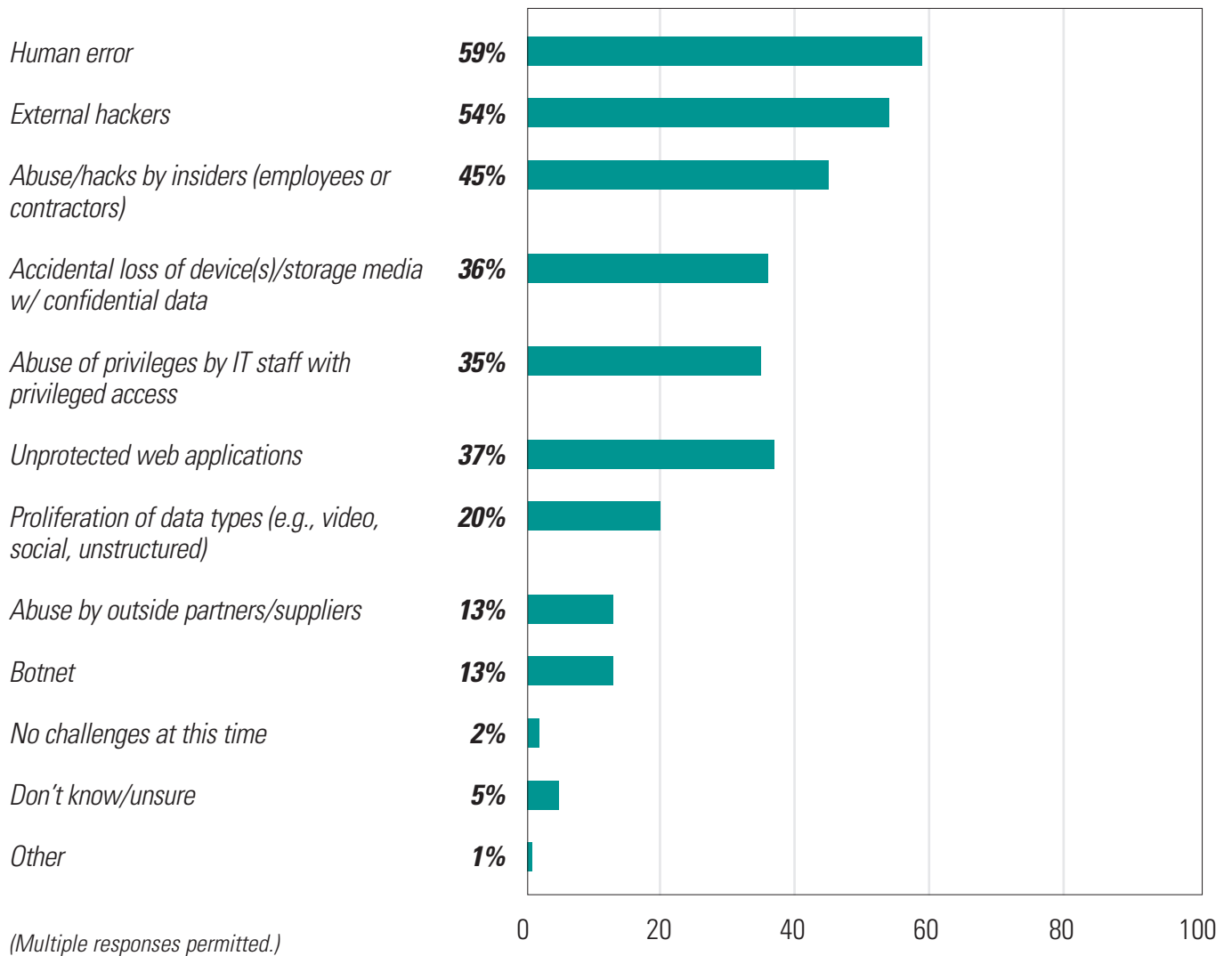
Figure 6: Additional Measures Taken As a Result of Stepped-Up Data Security



Data Security at an Inflection Point: 2011 Survey of Best Practices and Challenges was produced by Unisphere Research and sponsored by Application Security, Inc. 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, 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.

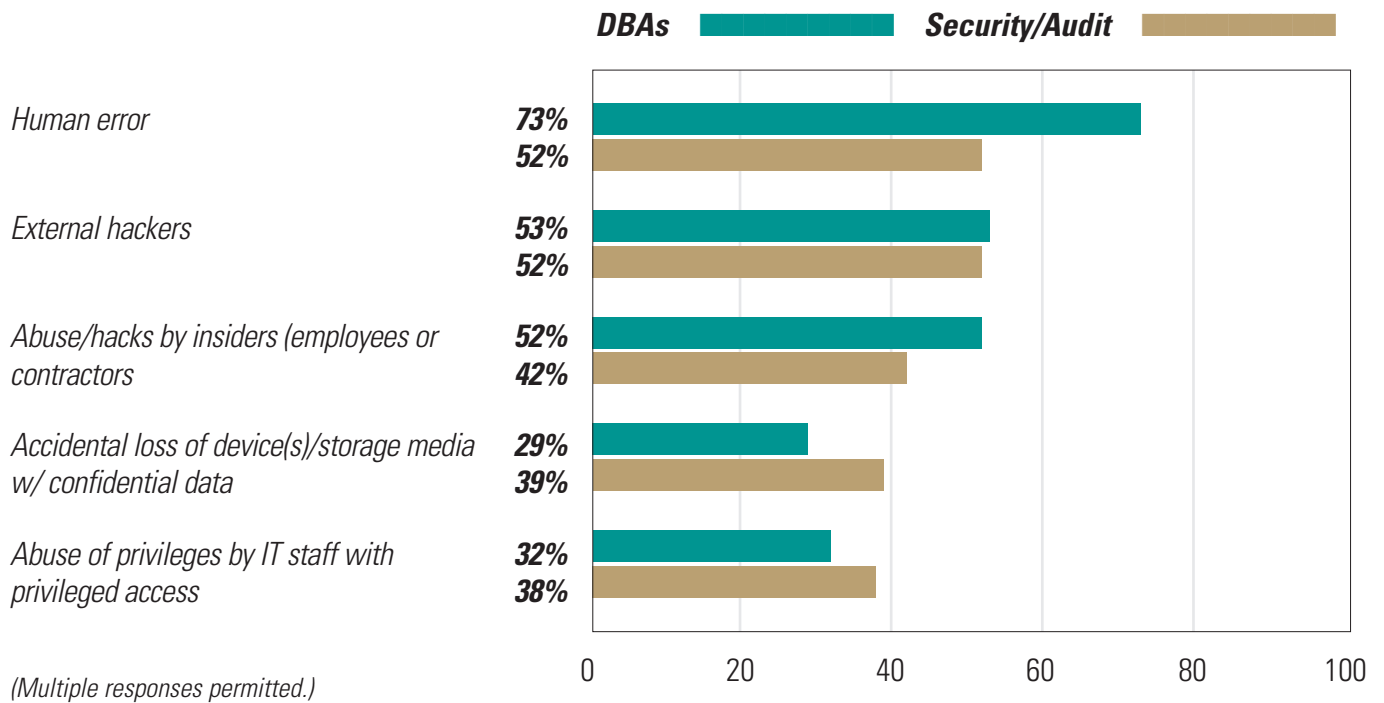
Figure 7: Greatest Challenges or Risks to Database Security



Data Security at an Inflection Point: 2011 Survey of Best Practices and Challenges was produced by Unisphere Research and sponsored by Application Security, Inc. 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, 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.

Figure 8: Top 5 Challenges or Risks to Database Security—By Job Role



Data Security at an Inflection Point: 2011 Survey of Best Practices and Challenges was produced by Unisphere Research and sponsored by Application Security, Inc. 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, 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.

BREACHES

Close to one-third know or suspect that their organizations have experienced a data breach, and even more expect a data breach over the coming year. However, few understand the costs of such breaches to their organizations.

About one-third of respondents report that their companies either definitely or may have suffered a confidential data breach over the past year. About 15% say they suffered a single or multiple breaches, while another 15% say it's likely they suffered a breach, but are uncertain of the details. (See Figure 9.) An even higher number, 39%, expect they will suffer some kind of breach over the coming year. (See Figure 10.)

In close to one out of four cases, 24%, these lapses were the result either of an insider attack, a combined insider and outside attack, or the result of abuse of privileges by privileged staff. In another 17% of cases, these security lapses were the result of human error, the survey finds. (See Figure 11.) The data-rich

application most likely to have been affected by the security incident was web applications, as cited by 17% of those suffering breaches. Another 16% reported there was a direct attack on their organizations' databases. (See Figure 12.)

The vast majority of respondents, 81%, that experienced data breaches report they are unaware of the costs to their businesses, suggesting that this is an inexact science. Among those that were aware of the costs, more than one out of 10 put the losses to their businesses at more than \$1 million. Another 21% say the cost was in the hundreds of thousands of dollars. The largest segment, 42%, say they did not see losses of more than \$10,000 for these incidents. (See Figure 13.)

Figure 9: Suffered Confidential Data Breach Within Last 12 Months?

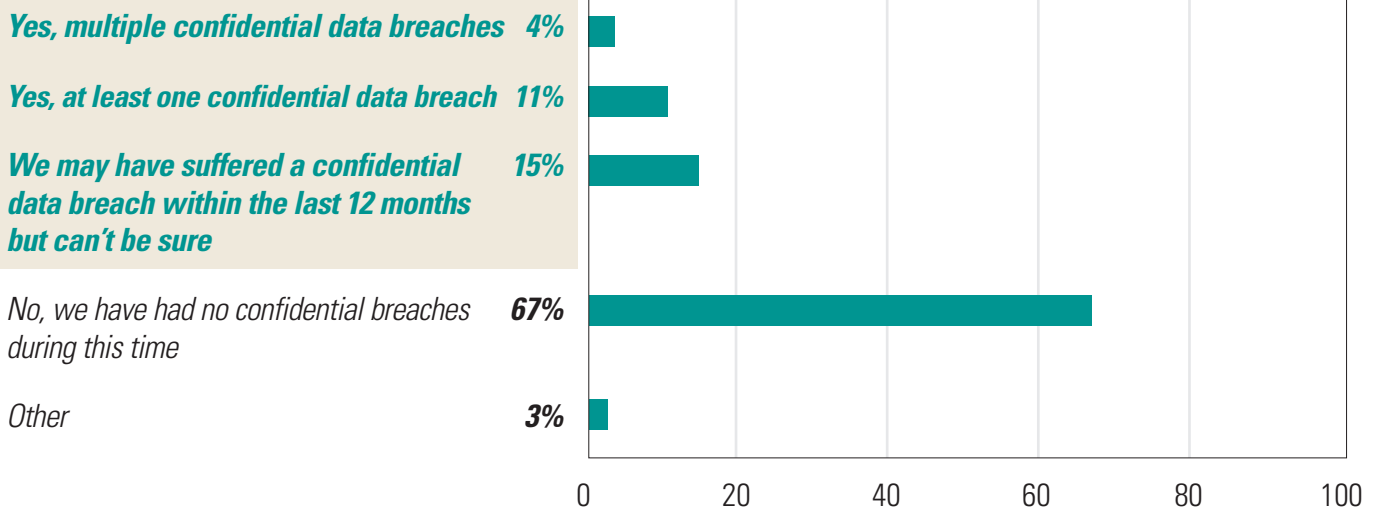


Figure 10: Likelihood of Data Breach Within Next 12 Months (Internal or External)

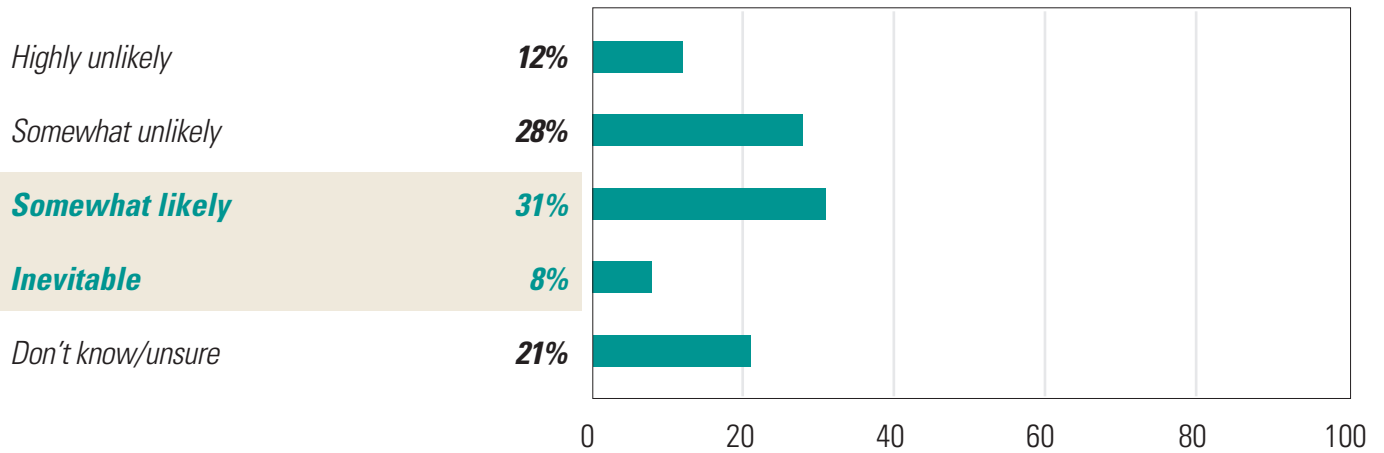


Figure 11: Root Causes of Confidential Data Breach(es)

(Among companies that have experienced data breaches over past year)

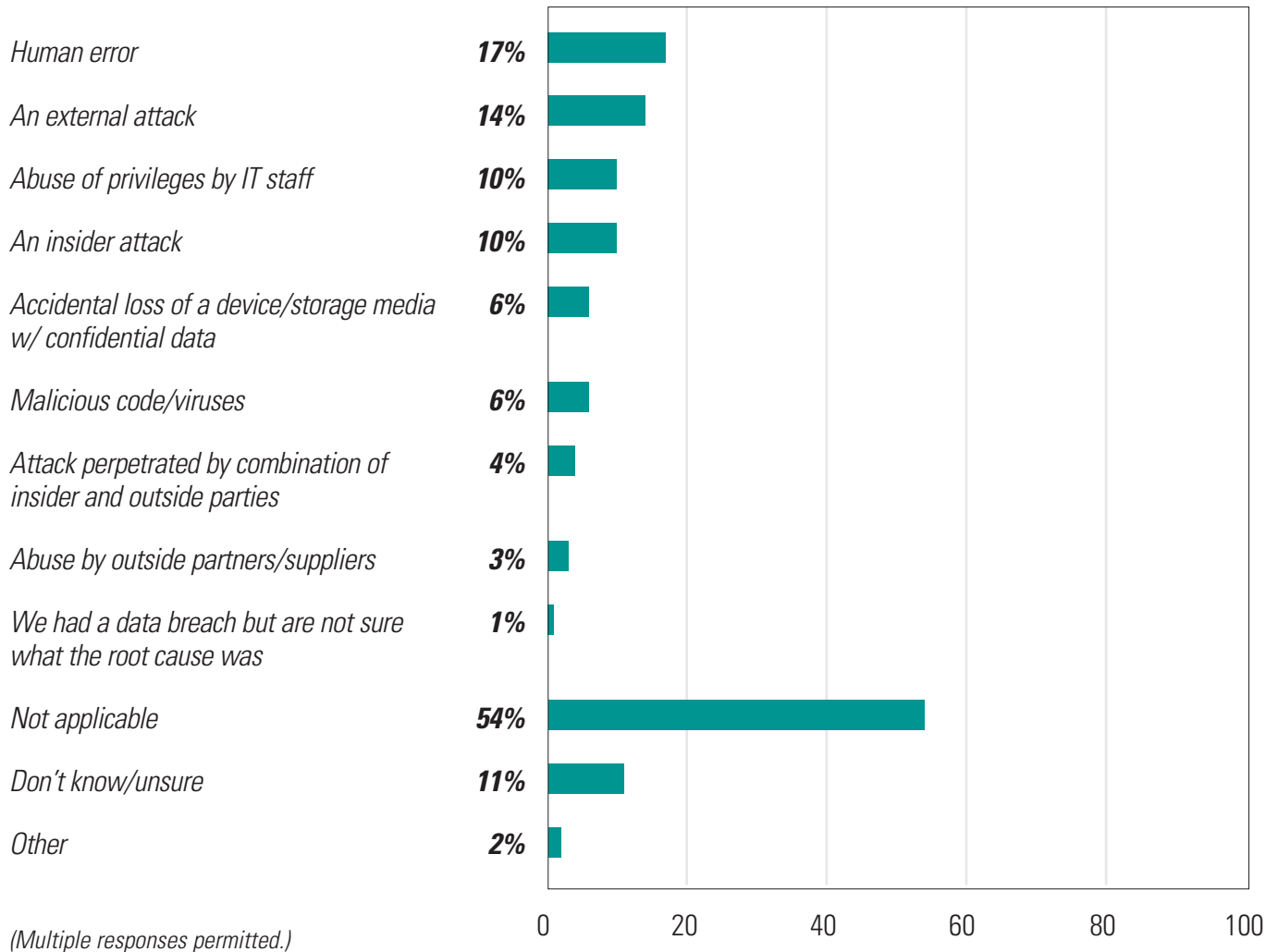


Figure 12: Data-Rich Components Compromised as a Result of Data Breach

(Among companies that have experienced data breaches over past year)

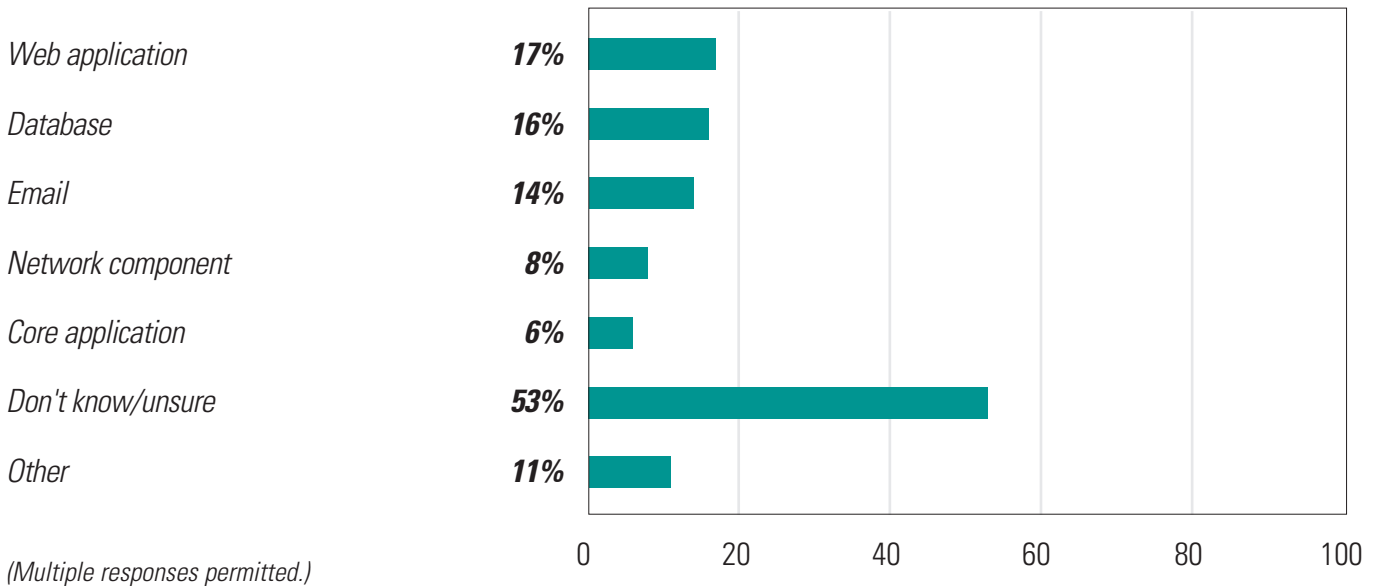
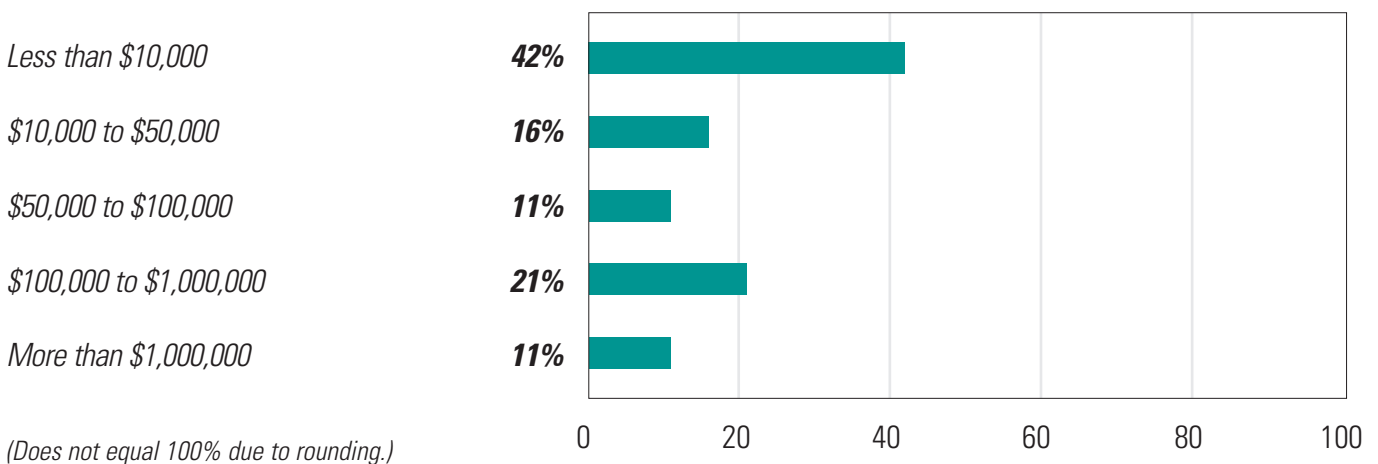


Figure 13: Total Costs of Data Breaches Over Past Year

(Among respondents knowledgeable about the cost of their data breaches over past year)



Data Security at an Inflection Point: 2011 Survey of Best Practices and Challenges was produced by Unisphere Research and sponsored by Application Security, Inc. 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, 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.

ORGANIZATIONAL CONCERNS

Organizational issues impede efforts to address database security. In most cases, security is overseen by both database and security teams. Adding to the challenge is the need to store data for long periods of time—a majority of respondents maintain data well beyond the required storage limits. One out of four respondents now maintains data environments within private clouds, but a majority are concerned about security in these environments as well.

What are the greatest impediments holding back efforts to address information security? A majority of respondents, 58%, say budget constraints are the most formidable issue. In addition, a sizable percentage of respondents say there isn't enough of an understanding of the threats that exist. (See Figure 14.) Perceptions of several of these issues vary by job role, the survey finds. While both DBAs and security/audit professionals agree that budget constraints are the number-one impediment to a robust data security initiative, database managers are more inclined to see a lack of management commitment as an issue as well. Database managers say management "just doesn't get it," a view not shared by security and audit professionals. (See Figure 15.)

Who is responsible for database security in respondents' organizations? Database managers and security managers appear to share this duty, among 59% and 58%, respectively, assuming this responsibility. (In many cases, respondents have both groups overseeing data security.) (See Figure 16.) Smaller firms tend to rely most on their general IT staff, while the largest organizations in the survey tend to have dedicated database and security teams equally sharing responsibility. (See Figure 17.)

However, having a robust security team present in the enterprise doesn't necessarily guarantee that data will be secure. As one respondent points out: "We have an organization to address security issues, yet it offers no clear interfaces, guidelines, or forum to assist application teams to implement the best security practices. The only option appears to be being audited and being threatened by upper management to not fail the audit, at the expense of one's job."

For the most part, information security spending has held steady over the past year, with seven-tenths reporting funding

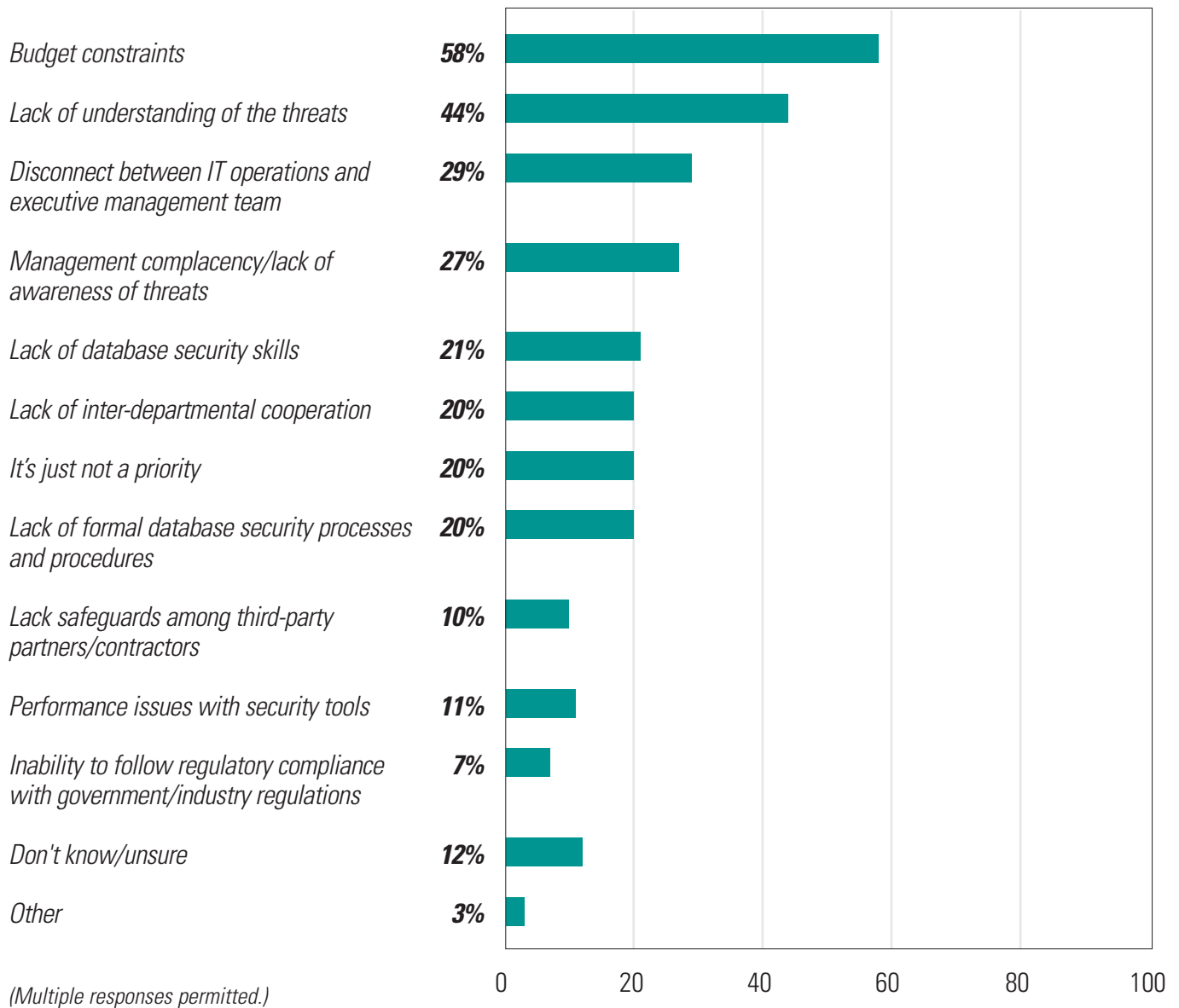
has either increased or remained the same. Thirty-nine percent increased their spending. (See Figure 18.) On average, database security represented about 10% of average IT security budgets. Still, as shown above, funding is inadequate in the eyes of most respondents. One respondent observes: "I think the biggest risks we have are from the lack of funding to the IT department. The knowledge is there but we have no cash to implement the necessary changes to secure our servers."

While cloud is still a nascent technology, close to one out of four respondents now report they support their database environments with private cloud platforms. Public cloud is slower to catch on in the database world, however, with only 7% deploying their database environments through public cloud offerings. (See Figure 19.) The largest companies in the survey were twice as likely to be implementing a private cloud environment than their smaller counterparts; public cloud adoption is stronger among small firms. (See Figure 20.)

There are perceived challenges with cloud computing, however. Close to two-thirds of respondents worry about data security within public cloud settings, and another 45% are concerned about data security in private cloud settings. Compliance and regulations could be another potential show-stopper for cloud, as indicated by 39% of respondents. (See Figure 21.) "Cloud computing is quickly becoming a concern to us as it depends on third-party vendors, and the security methods that are out of our control," says one respondent.

While private clouds are seen as a more secure way to take advantage of cloud protocols, data needs to be effectively managed against internal vulnerabilities, as explored in the next section.

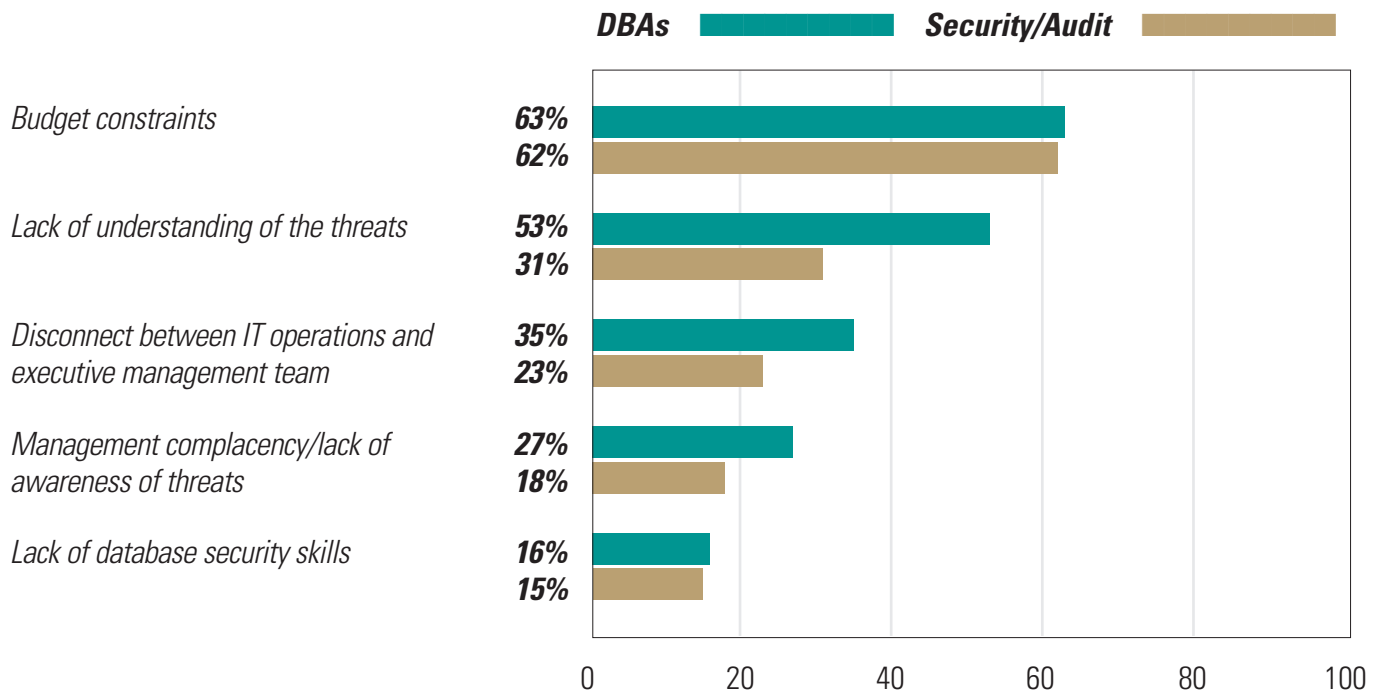
Figure 14: Greatest Impediments to Information Security



Data Security at an Inflection Point: 2011 Survey of Best Practices and Challenges was produced by Unisphere Research and sponsored by Application Security, Inc. 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, 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.

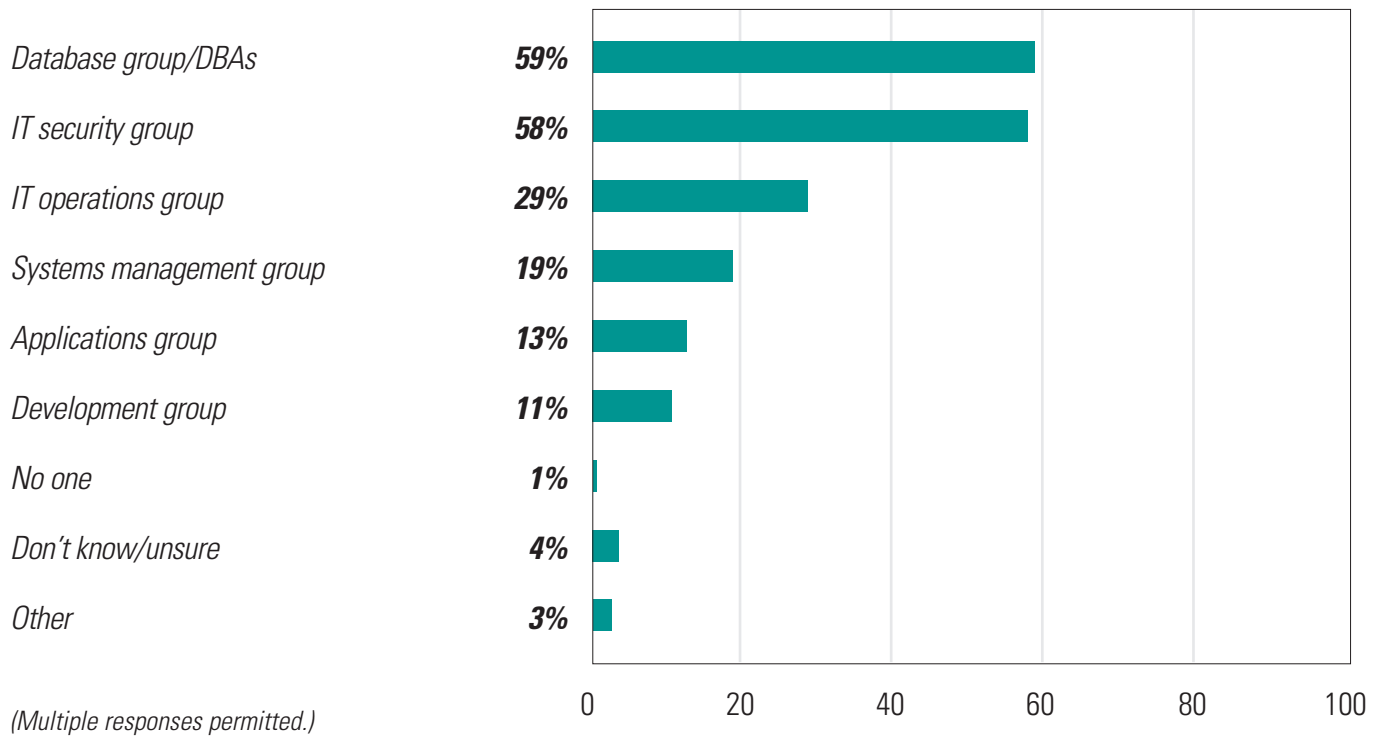
Figure 15: Top 5 Impediments to Information Security—By Job Role



Data Security at an Inflection Point: 2011 Survey of Best Practices and Challenges was produced by Unisphere Research and sponsored by Application Security, Inc. 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, 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.

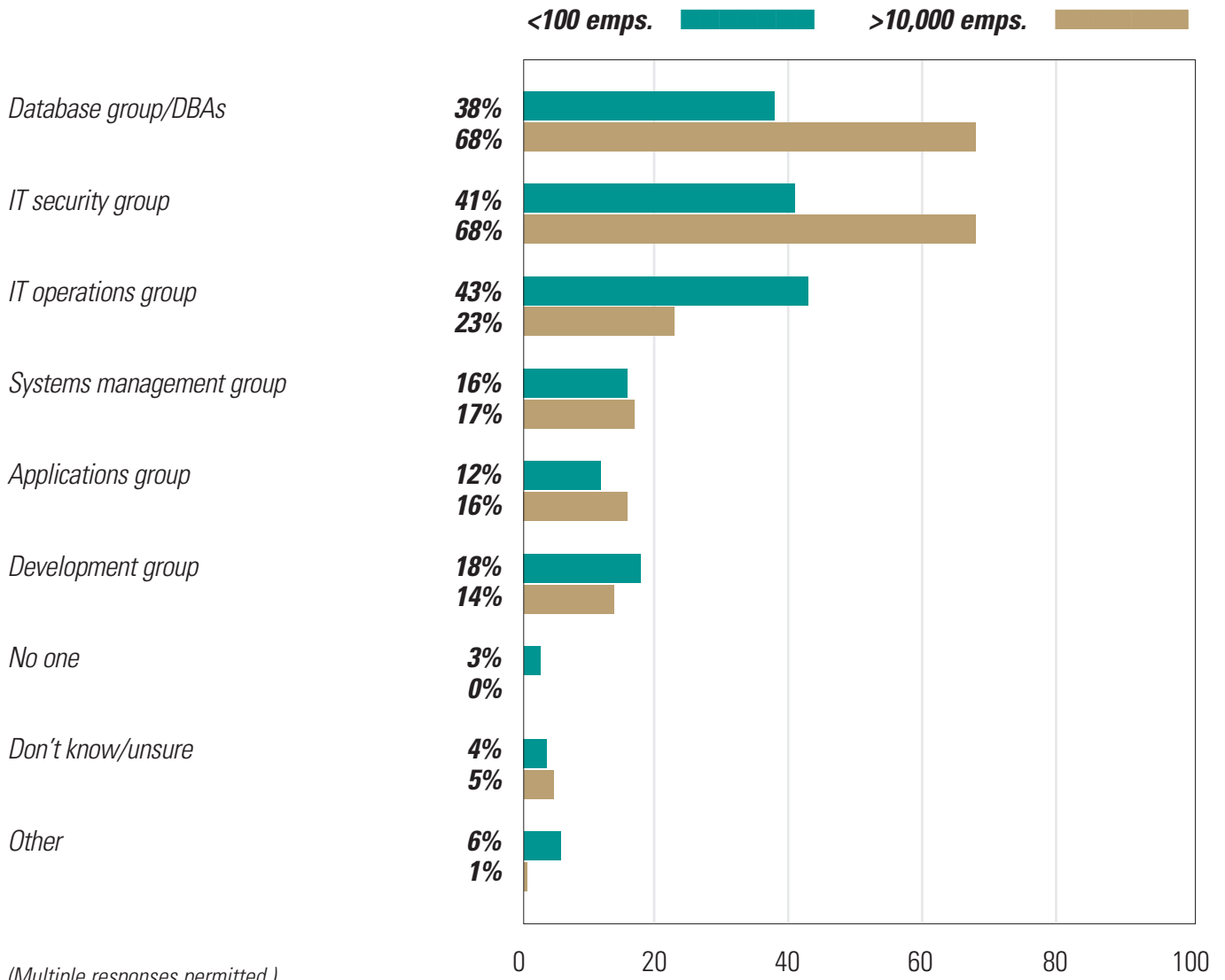
Figure 16: Who is Responsible for Enterprise Database Security?



Data Security at an Inflection Point: 2011 Survey of Best Practices and Challenges was produced by Unisphere Research and sponsored by Application Security, Inc. 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, 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.

Figure 17: Responsibility for Enterprise Database Security —By Company Size



(Multiple responses permitted.)

Figure 18: How Information Security Spending Changed Over Past Year

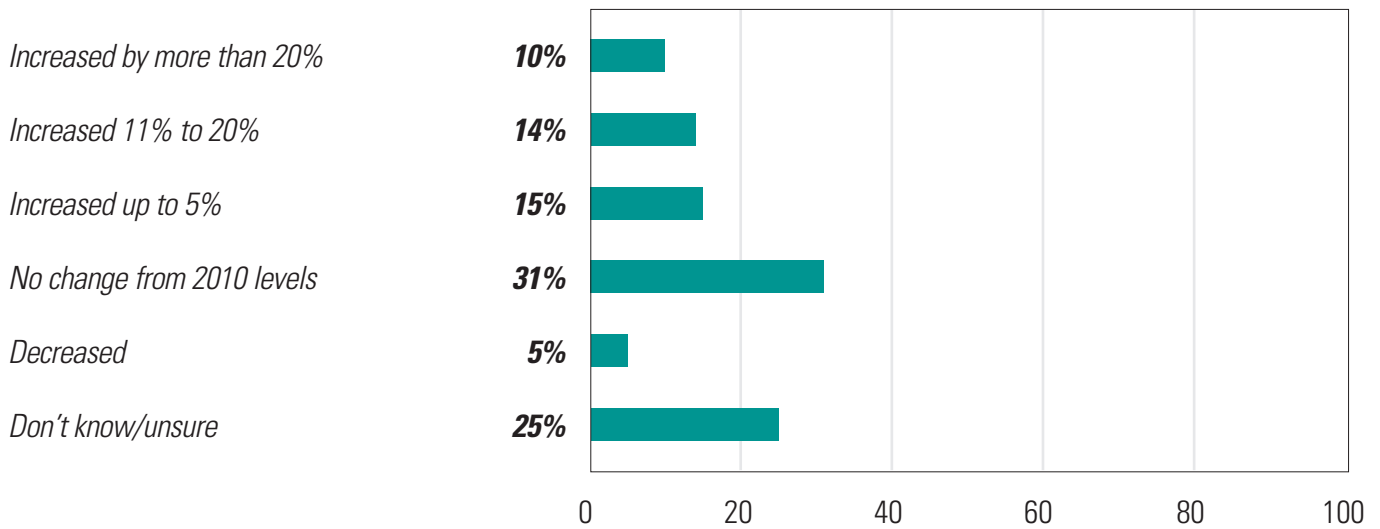


Figure 19: Currently Deploy Database Instances Via Cloud Technology

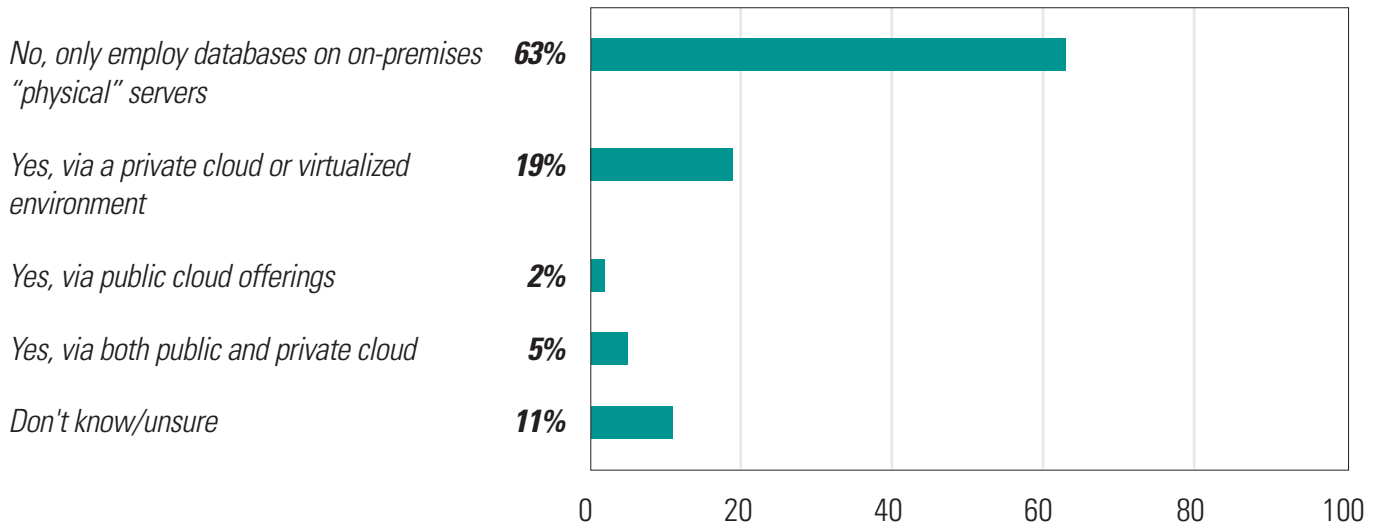


Figure 20: Databases in Clouds—By Company Size

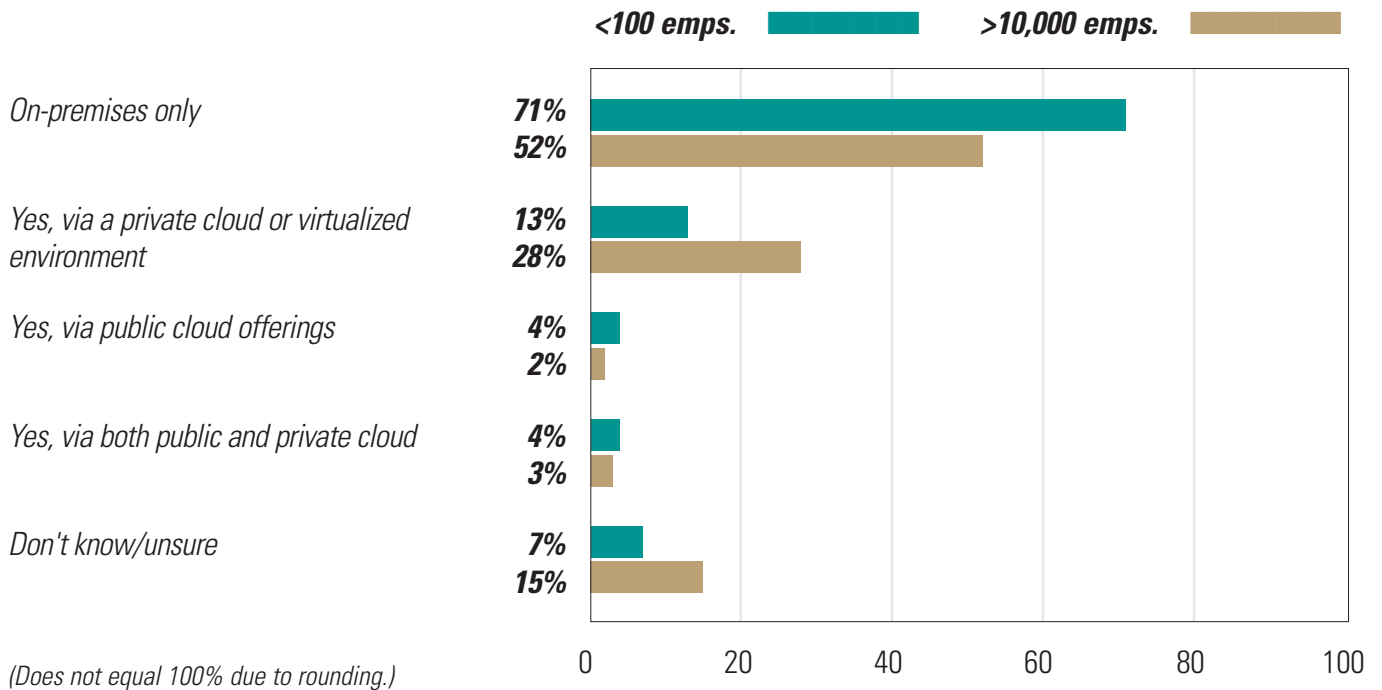
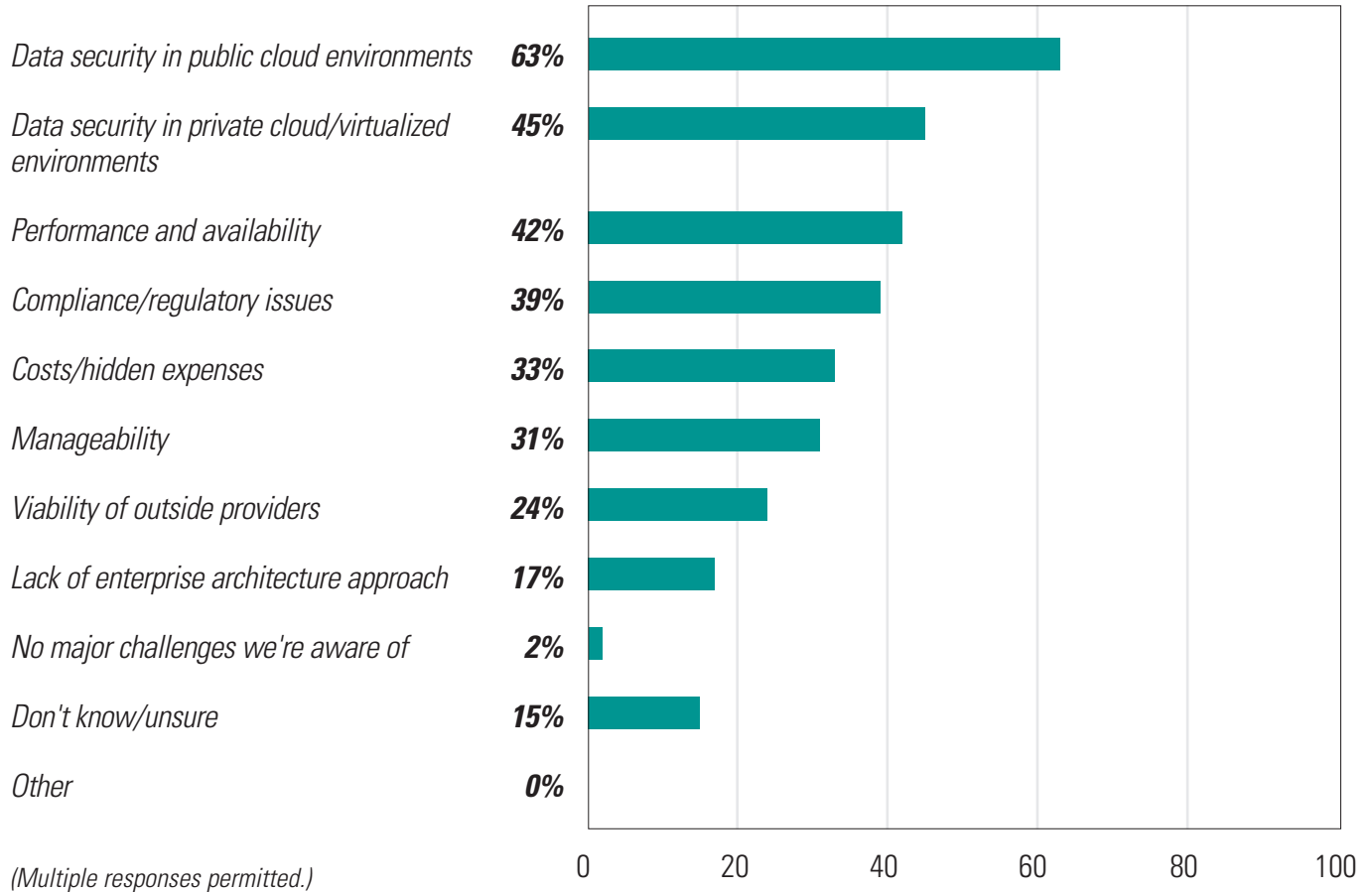


Figure 21: Greatest Challenges With Deploying Database Instances Via Cloud Environments



Data Security at an Inflection Point: 2011 Survey of Best Practices and Challenges was produced by Unisphere Research and sponsored by Application Security, Inc. 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, 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.

COMPLIANCE AND CONTROLS

Respondents are divided as to whether their organizations' existing data security controls provide an adequate level of protection against database breaches and attacks. Most companies have multiple copies of production data in their enterprises, and often don't have direct control of all copies.

While 53% report that all or most of their databases are adequately protected, another 33% say they lack such protection, and 10% don't know or are unsure about it. (See Figure 22.) A higher number, 62%, feel that their organizations' existing data security controls provide an adequate level of protection for confidential data as well. (See Figure 23.)

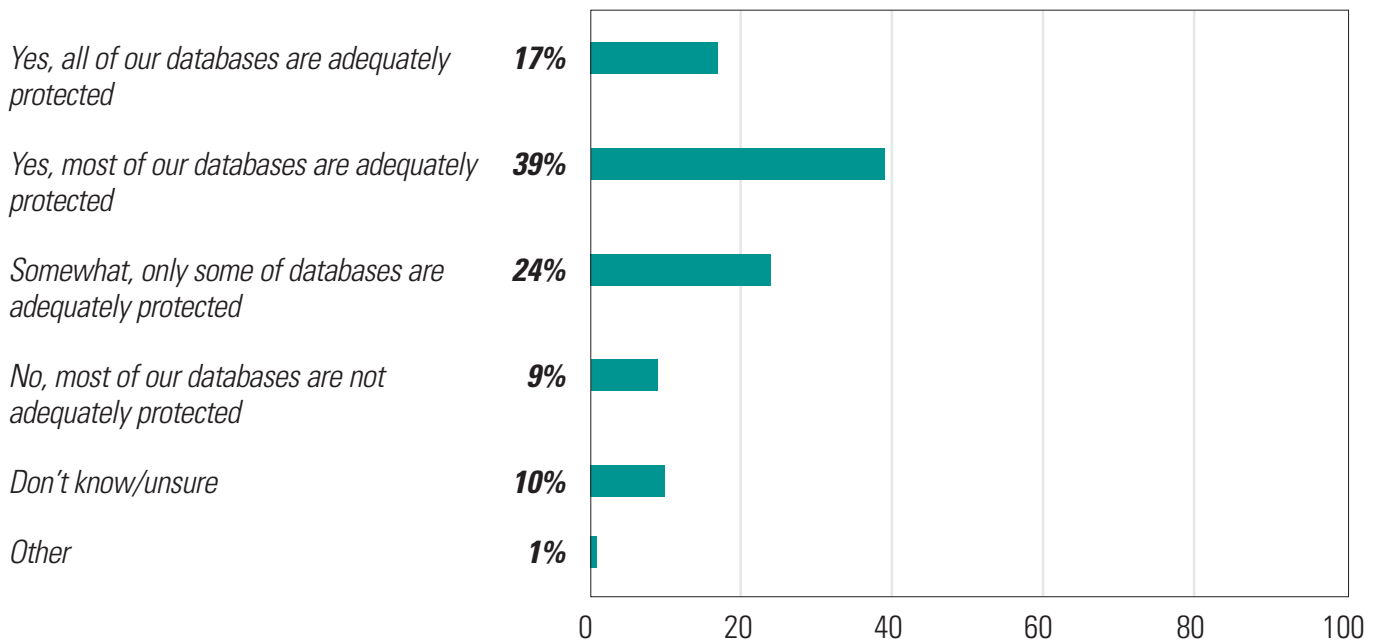
For most legal documents, the time required to store is about seven years. However, a majority of respondents, 54%, say they store data within their archived systems longer than that, due to policy or compliance mandates. Up to 12%, in fact, report they simply hold on to all data "forever." (See Figure 24.)

Close to one-third of respondents, 29%, say that a substantial portion of their enterprises' data (defined as more than one-quarter of their total data store) consists of personally identifiable information or confidential data (e.g., Social Security, credit card, and national identifier numbers). (See Figure 25.)

A challenge to data security is presented when confidential data leaves the main production environment and is sent to other parts of the enterprise for non-production purposes. Such environments may include development shops, backup sites, or application testing environments. Close to one-third of respondents, 31%, admit that "live" or production data is used within non-production environments. More than one-third report using simulated data for such non-production purposes. (See Figure 26.)

The proliferation of multiple copies of data is another security concern. In fact, a majority of respondents, 57%, report having at least two copies of their production data housed somewhere within their enterprises—which could include offsite backup and storage or partner sites. One out of five respondents has at least four or five copies throughout their enterprise. (See Figure 27.) Only 41%, however, could verify that these copies of data outside the production environment are within their direct control. (See Figure 28.)

Figure 22: Existing Data Security Controls Provide Adequate Database Protection?



Data Security at an Inflection Point: 2011 Survey of Best Practices and Challenges was produced by Unisphere Research and sponsored by Application Security, Inc. 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, 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.

Figure 23: Organizations' Existing Data Security Controls Provide Adequate Sensitive Data Protection?

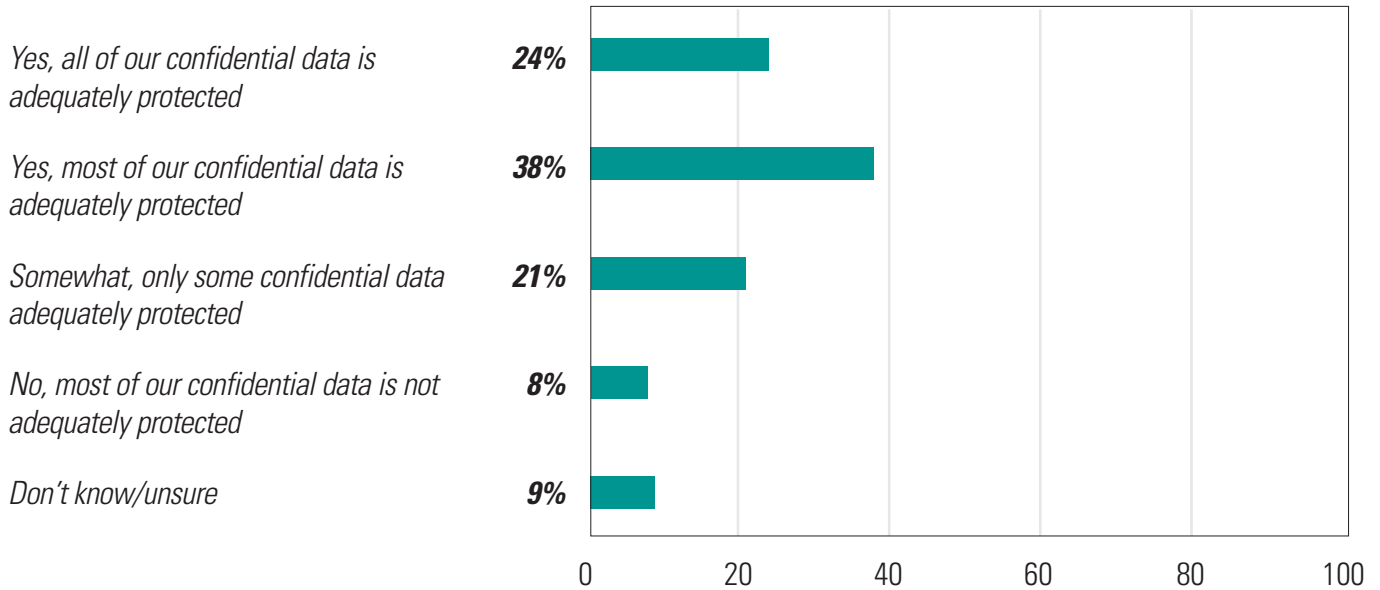
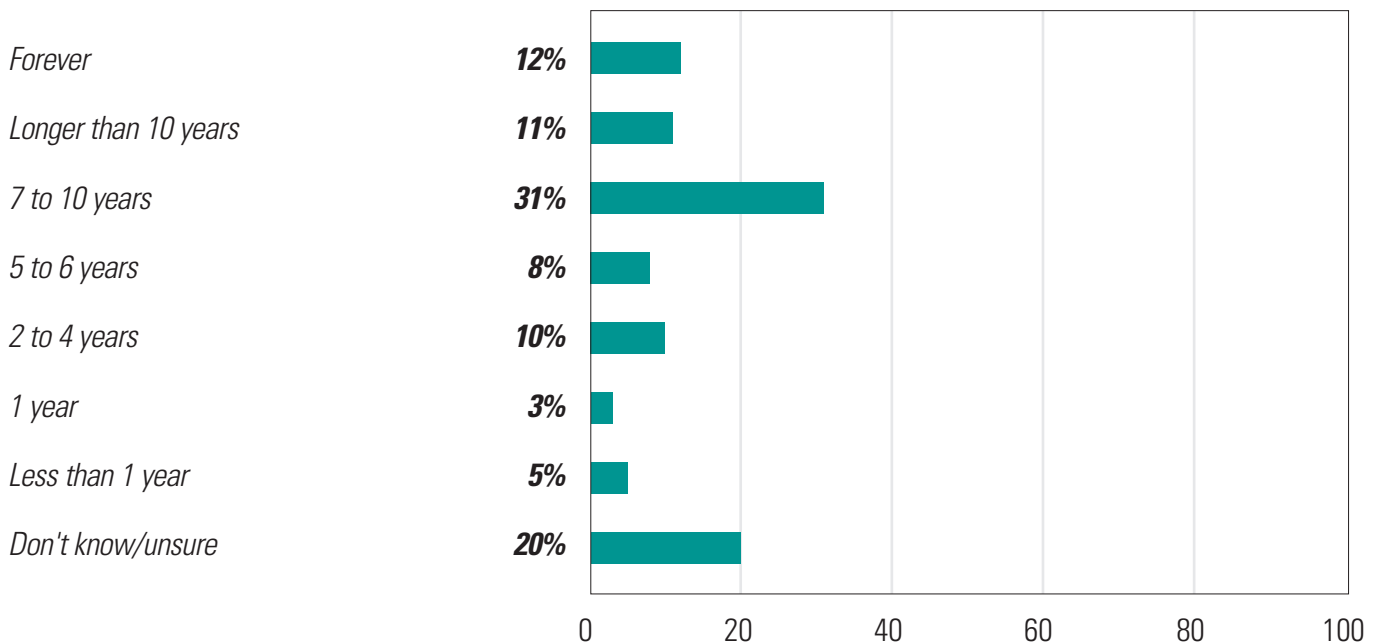


Figure 24: Length of Time Data Stored



Data Security at an Inflection Point: 2011 Survey of Best Practices and Challenges was produced by Unisphere Research and sponsored by Application Security, Inc. 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, 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.

Figure 25: Percentage of Enterprise Data that is Personally Identifiable Information

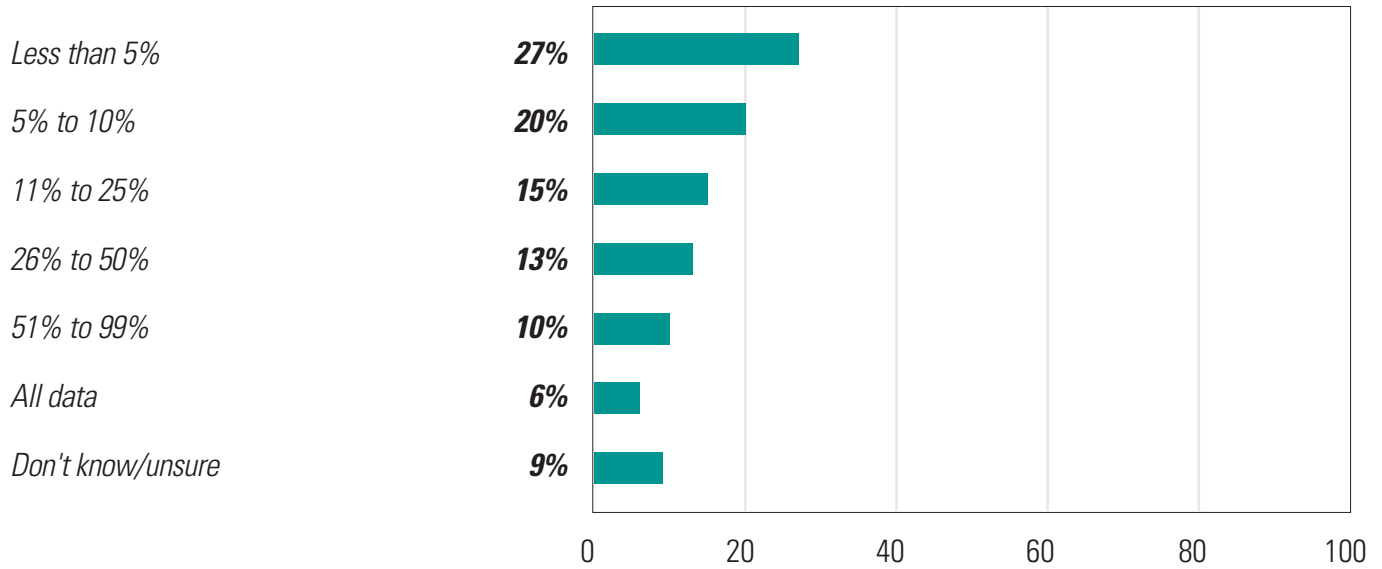


Figure 26: Data Used Within Non-Production Environments

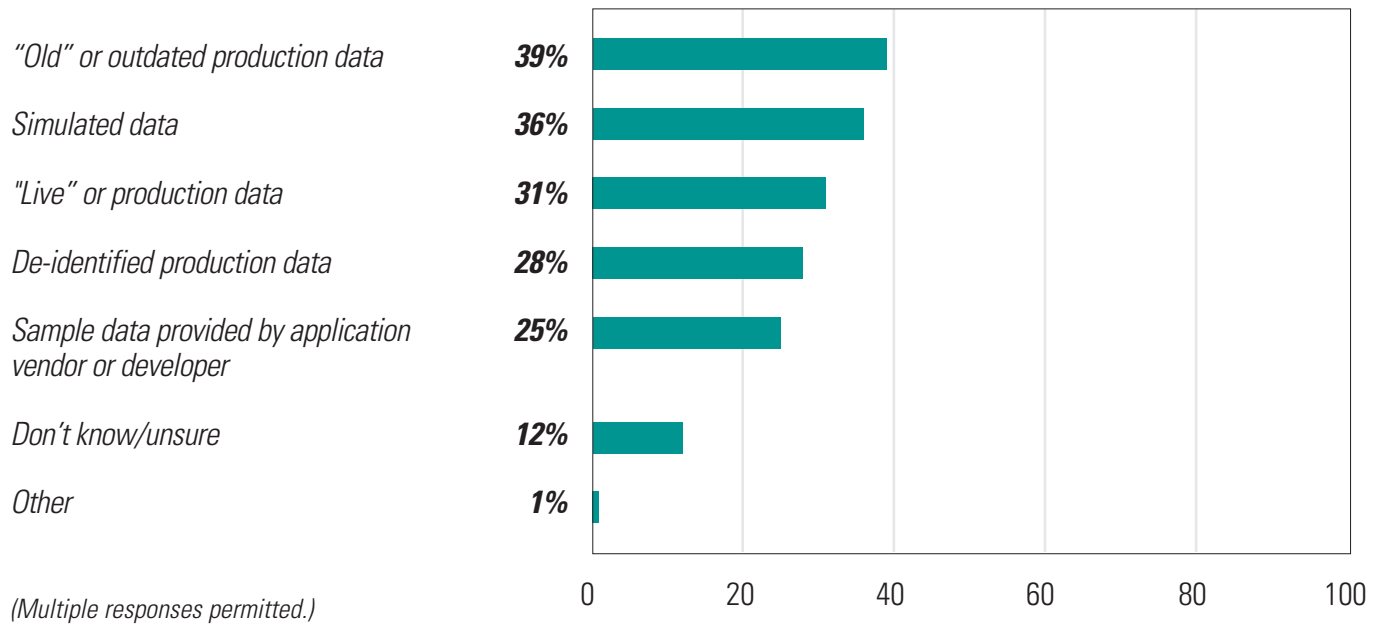


Figure 27: Number of Production Data Copies in Enterprises

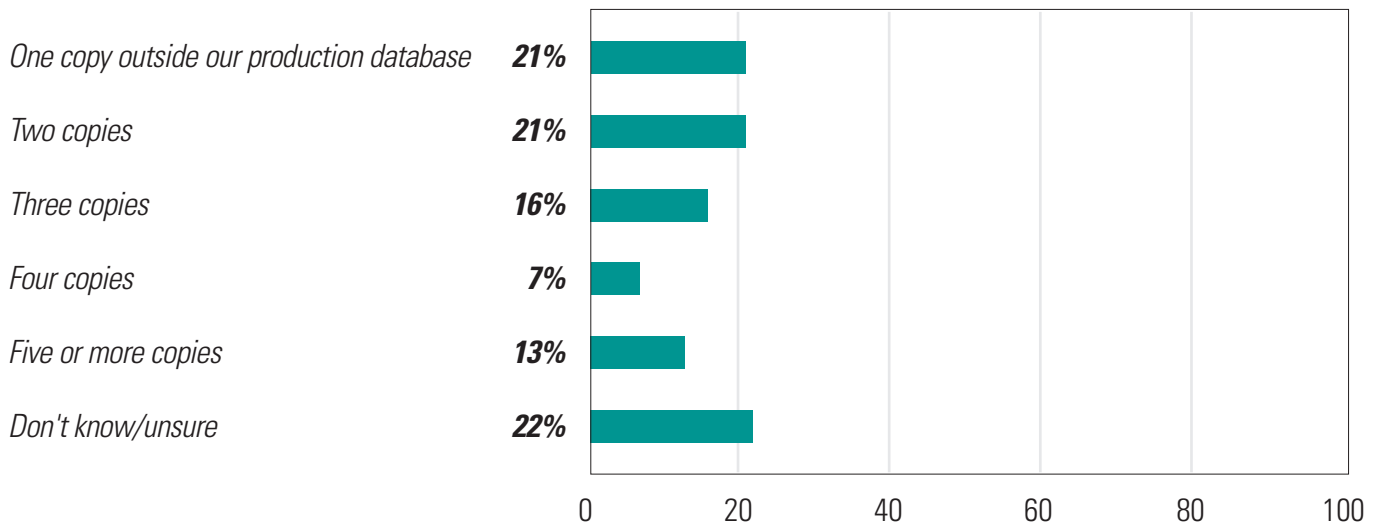
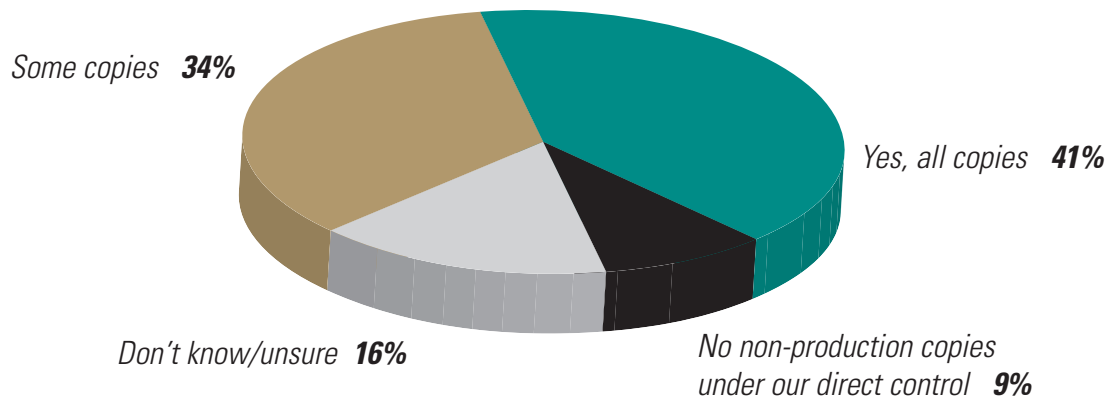


Figure 28: Direct Control of Non-Production Copies?



AUDITING AND MONITORING

Database security audits are few and far between. When conducted, issues typically uncovered include access control and configuration mistakes.

Many companies regard data security auditing and monitoring as critical best practices. However, auditing and monitoring often are only part of the data security story. These practices, when well managed, effectively spot security breaches or incidents after they have occurred. While the knowledge that they could possibly be caught may steer hackers or data thieves away from a particular data site, auditing and monitoring, for the most part, do not prevent data security breaches.

In the case of audits, if they are consulted infrequently, issues may only be spotted months after the breach occurred. As the survey finds, database security assessments or audits are not conducted with great frequency through the year. Close to half, 49%, say they conduct such audits no more than quarterly. Another 11% indicate they never conduct audits at all, while 18% simply don't know whether they audit or assess their data security standings. Only 18% are attentive, indicating they conduct such audits at least once a month. (See Figure 29.)

Among those respondents whose organizations have conducted audits, about 18% say the assessment delivered a moderate-to-significant number of findings. (See Figure 30.) In terms of issues identified, access control topped the list (34%) of security exposures, a reflection of the potential challenges that may be seen with insider abuse of data. Configuration issues also tend to be called out more frequently than other factors. (See Figure 31.)

“Configuration and access controls are the largest risks to databases,” agrees one respondent. “It is a team effort for everyone running and installing database systems to properly

secure the settings. Rogue systems are a common issue and are addressed immediately when identified. These rogue systems typically do not follow security baselines and are susceptible to compromise.”

Are respondents currently monitoring production databases for security issues such as unauthorized access to data or configuration changes? In most cases, they are, but respondents are divided as to the extent of automation. About 44% report running automated tools, versus 27% still conducting such monitoring on a manual basis. However, 13% indicate they do not conduct monitoring for data security issues, and 16% are not sure whether monitoring takes place. (See Figure 32.)

A majority of respondents who are monitoring the security of their production databases indicate that they are covering all privileged user activities. About half also look for failed logins, while two-fifths seek database definition changes, such as new tables that may have been added without prior authorization. (See Figure 33.)

Of course, monitoring and being aware of database breaches is only part of the challenge. It may take time until a breach is actually identified, and after that, corrected—depending on how closely activities are monitored, and how frequently audits and assessments are conducted. In the meantime, the breach stays open, and the data exposed behind it remains vulnerable. About 12%, in fact, estimate that it may take more than a week to remediate a breach while a third simply don't know how long it would take. (See Figure 34.)

Figure 29: Frequency of Database Security Assessments/Audits During Year

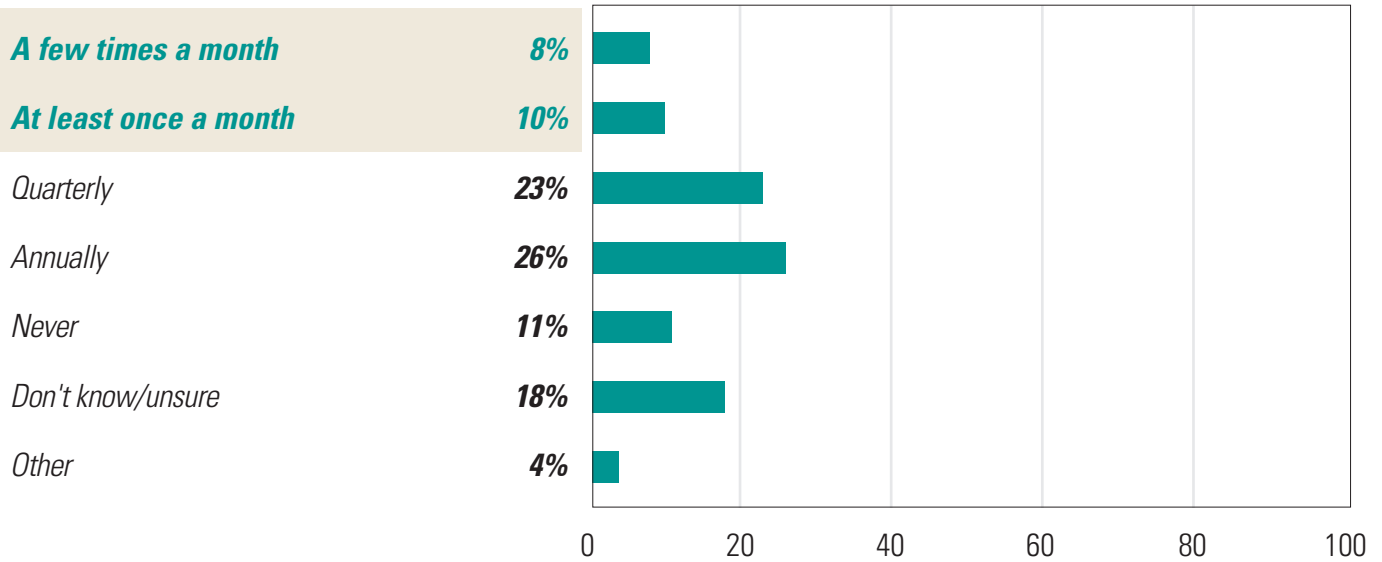
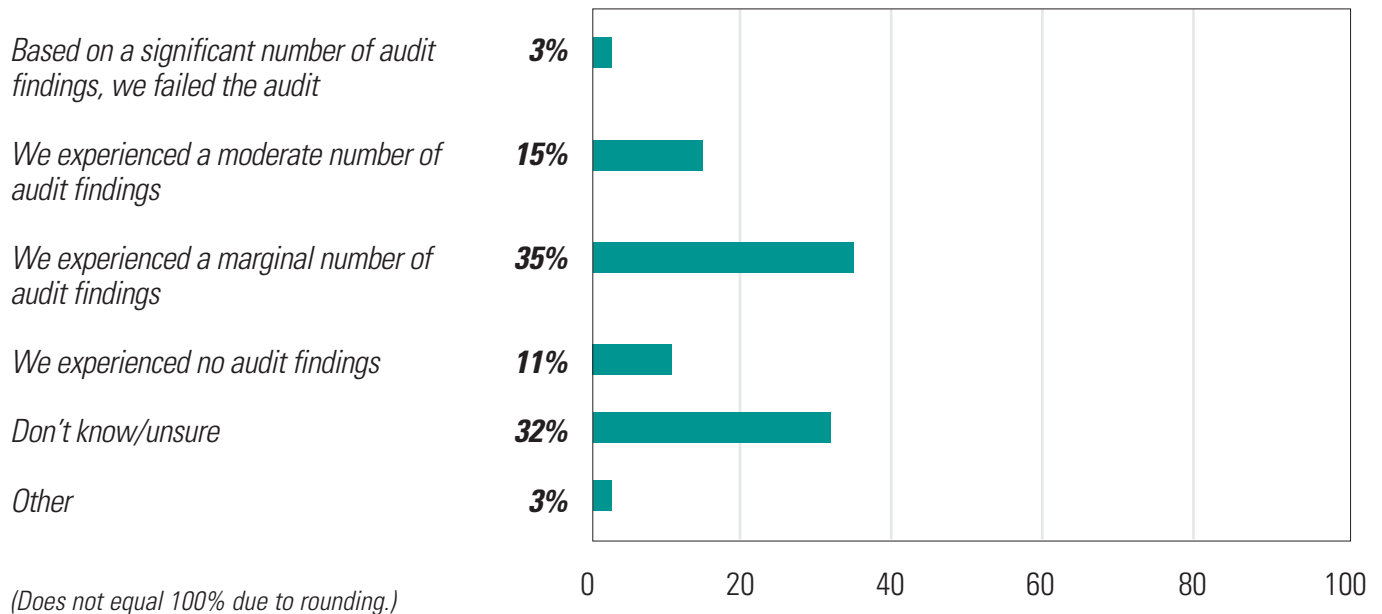


Figure 30: Database Security Audit Results

(Among companies regularly conducting audits)

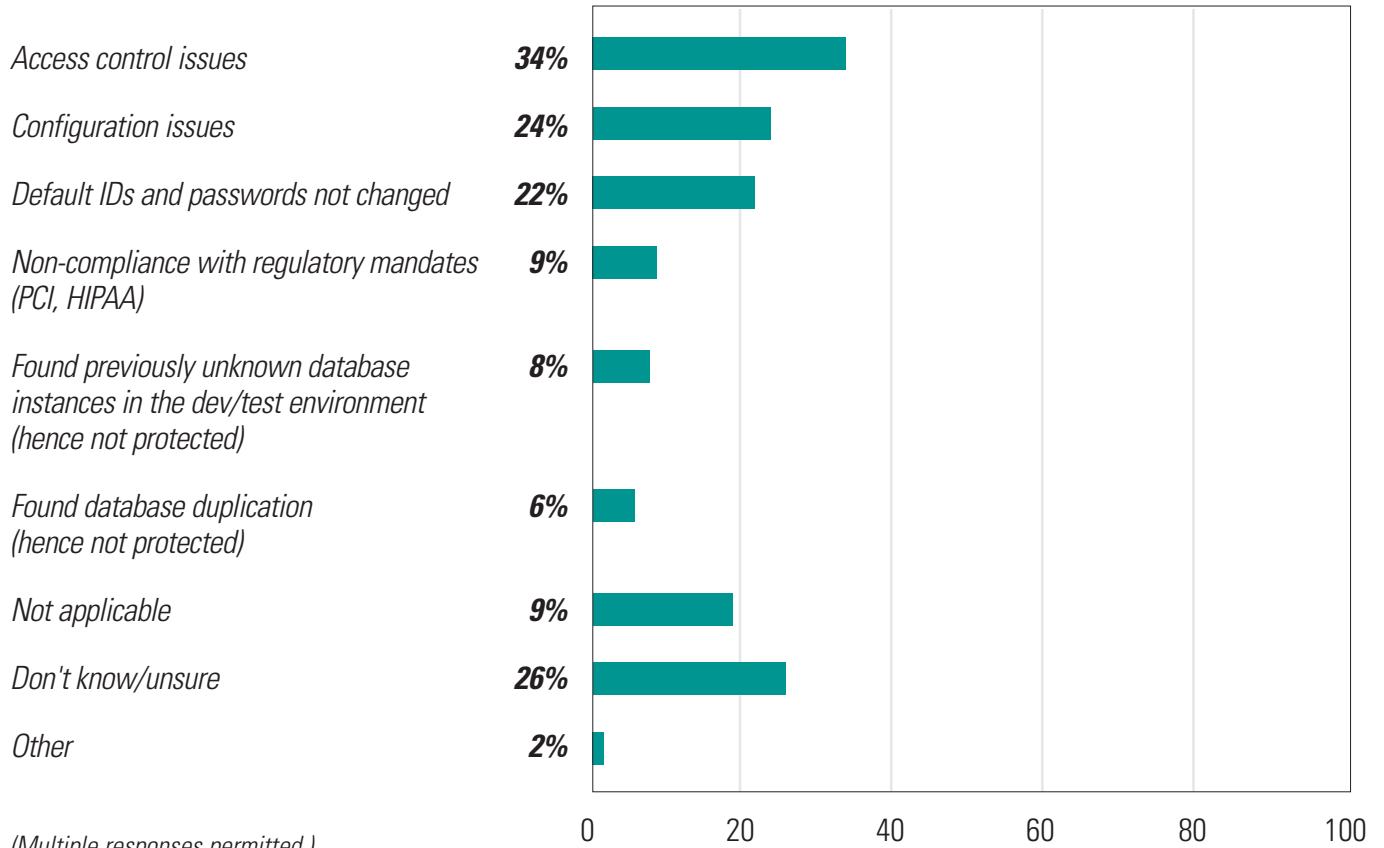


Data Security at an Inflection Point: 2011 Survey of Best Practices and Challenges was produced by Unisphere Research and sponsored by Application Security, Inc. Unisphere Research is the market research unit of Unisphere Media, a division of Information Today, Inc., publishers of Database Trends and Applications magazine and the 5 Minute Briefing newsletters. To review abstracts of our past reports, visit www.dbta.com/research. Unisphere Media, 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.

Figure 31: Areas of Non-Compliance Found in Database Security Audit Results

(Among companies regularly conducting audits)



Data Security at an Inflection Point: 2011 Survey of Best Practices and Challenges was produced by Unisphere Research and sponsored by Application Security, Inc. 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, 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.

Figure 32: Currently Monitoring Production Databases for Security Issues?

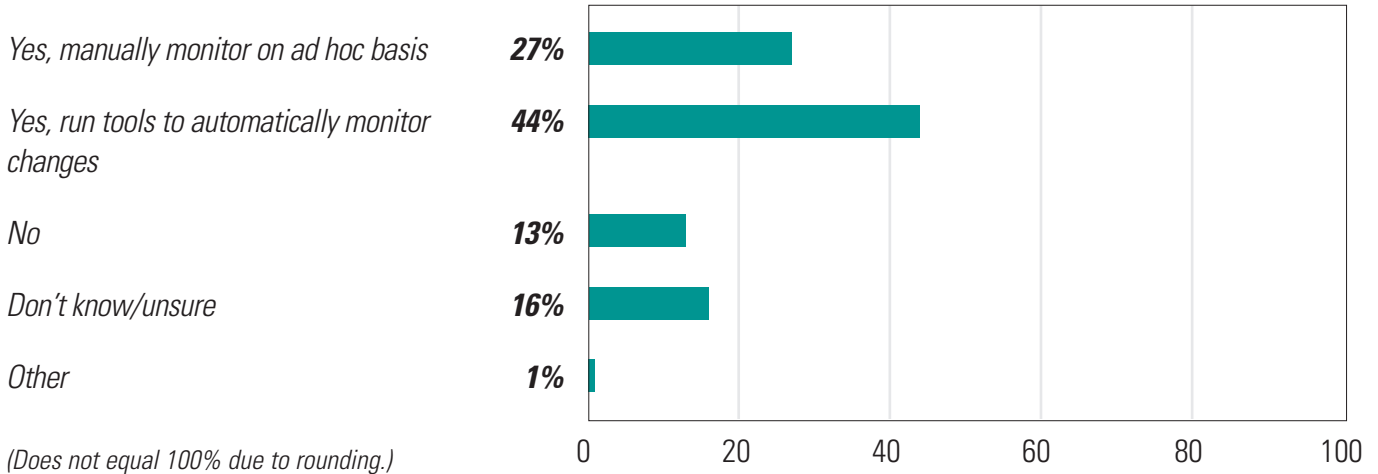
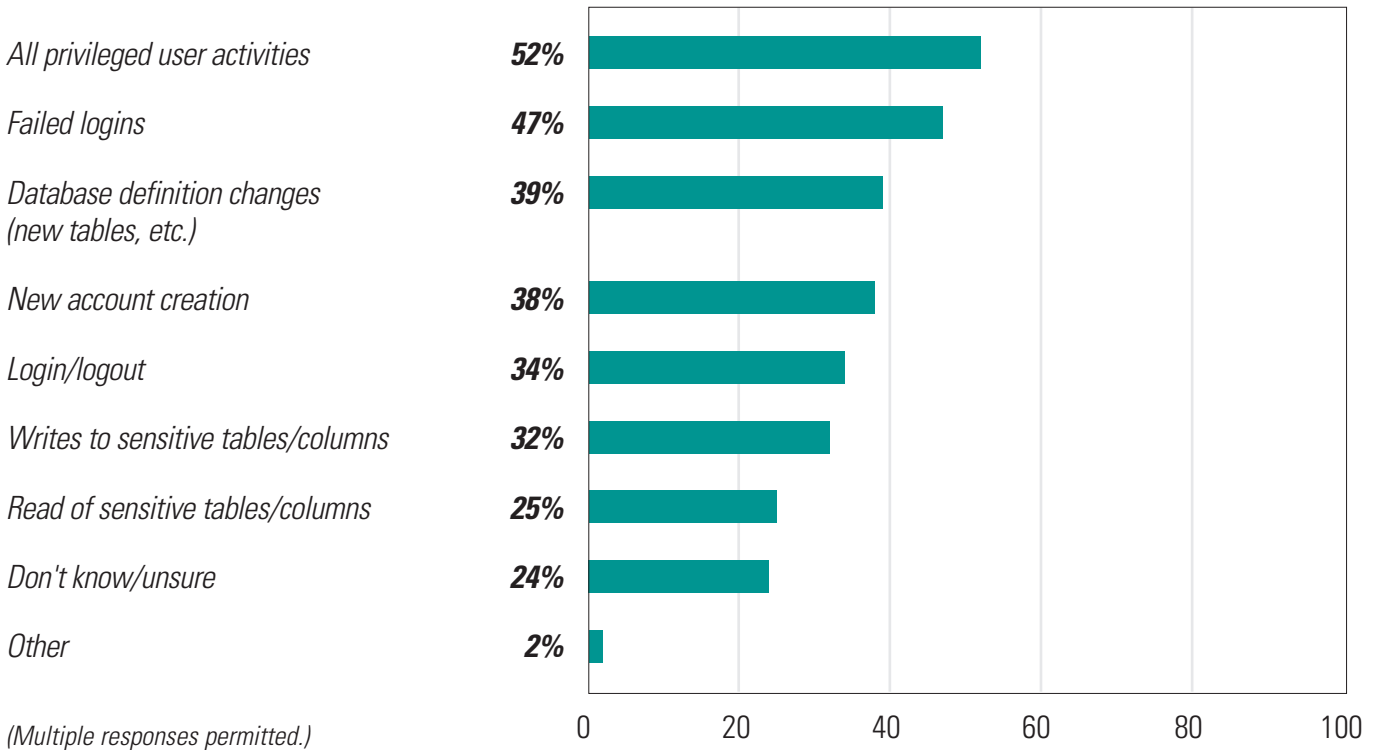


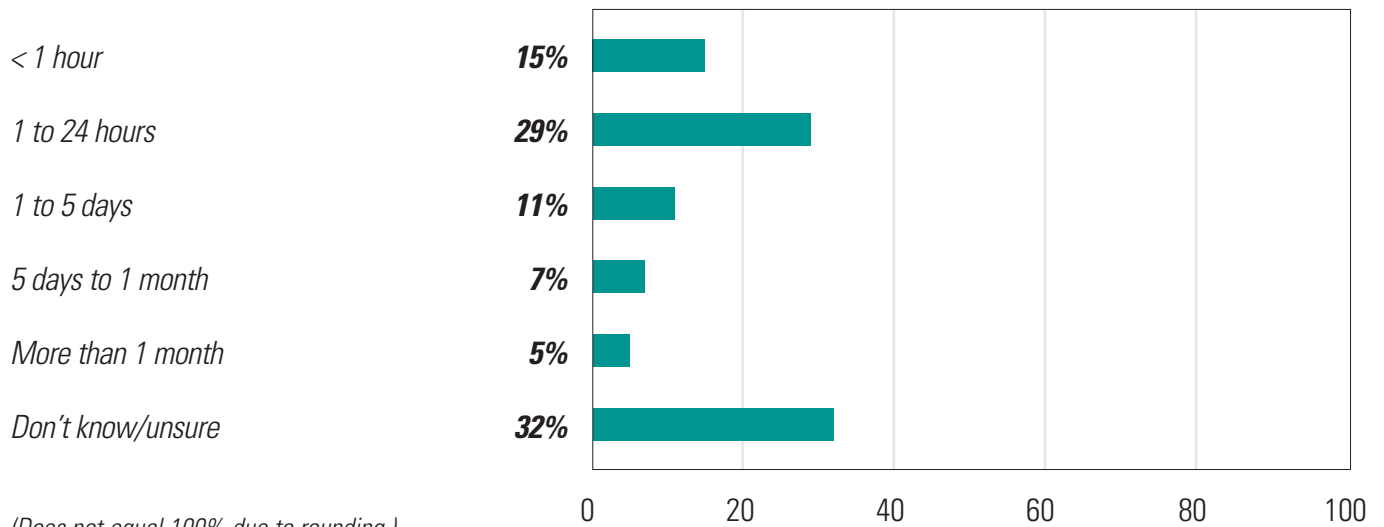
Figure 33: Database Activities Monitored

(Among companies monitoring production databases for security issues)



Data Security at an Inflection Point: 2011 Survey of Best Practices and Challenges was produced by Unisphere Research and sponsored by Application Security, Inc. 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, 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.

Figure 34: Length of Time to Detect and Correct Security Issues

SOLUTIONS

Vendors' security patches are applied infrequently. Monitoring and configuration solutions are prevalent, but other security technologies such as encryption are only seen at a minority of companies.

This survey finds that while concern is high, there is a severe lack of attention being paid or resources being committed to enterprise data security. There are a number of relatively straightforward technical approaches that can be taken to alleviate many security holes both inside as well as outside enterprises, but many organizations appear to lack the will to put these solutions in place.

While vendors advise that enterprises apply their database security patches as soon as possible, most respondents take a more deliberate approach. More than one-fourth, 27%, report that they don't apply patches more frequently than quarterly. (Figure 35.) In addition, it takes time for these patches to proliferate across enterprise environments. Fewer than one-third apply these updates across their entire portfolios. (See Figure 36.)

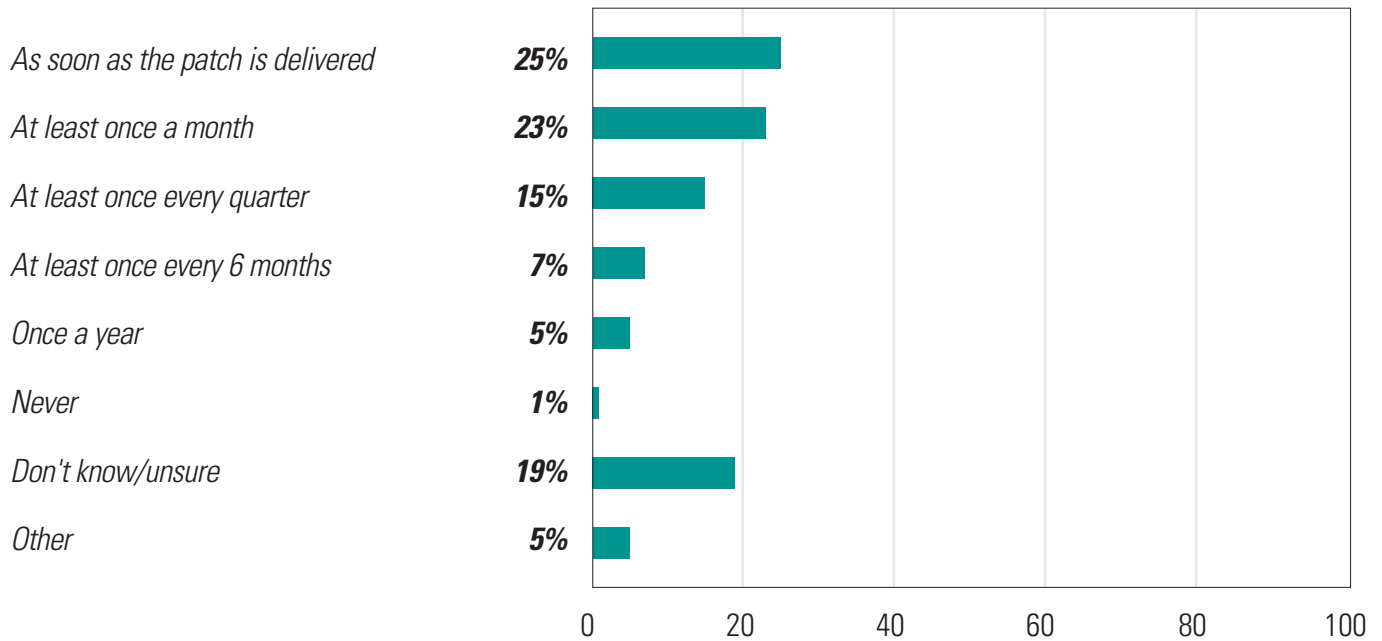
Database activity monitoring solutions are the database security technologies most likely to be deployed at organizations, as cited by 43% of respondents. Another 41% report employing database configuration and patch management. However, only a minority of respondents report implementing database

vulnerability assessment solutions (26%) or encryption solutions (25%). (See Figure 37.)

For the most part, respondents are generally satisfied with the security offerings of their primary DBMS vendors. Only one out of 10 gave these vendors poor ratings. (See Figure 38.) In two out of three cases, respondents report they employ these offerings within their environments. (See Figure 39.) In terms of security, the open source and commodity offerings get the lowest marks. The largest number of respondents, 24%, indicate that MySQL has the barest security features of the major data products used. (See Figure 40.)

However, as discussed earlier in this report, tools won't keep an enterprise secure if there isn't enough management support behind data security initiatives. As one respondent put it: "We continually find the same vulnerabilities existing each time a scan is performed. We can have all the security tools in the world but until the mindset changes and people are held accountable for their lack of addressing security, we will continue this trend and no tool is going to fix that."

Figure 35: Frequency of Applying Vendor Security Update Patches



Data Security at an Inflection Point: 2011 Survey of Best Practices and Challenges was produced by Unisphere Research and sponsored by Application Security, Inc. 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, 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.

Figure 36: Are Security Updates Installed Across Entire Database Portfolio?

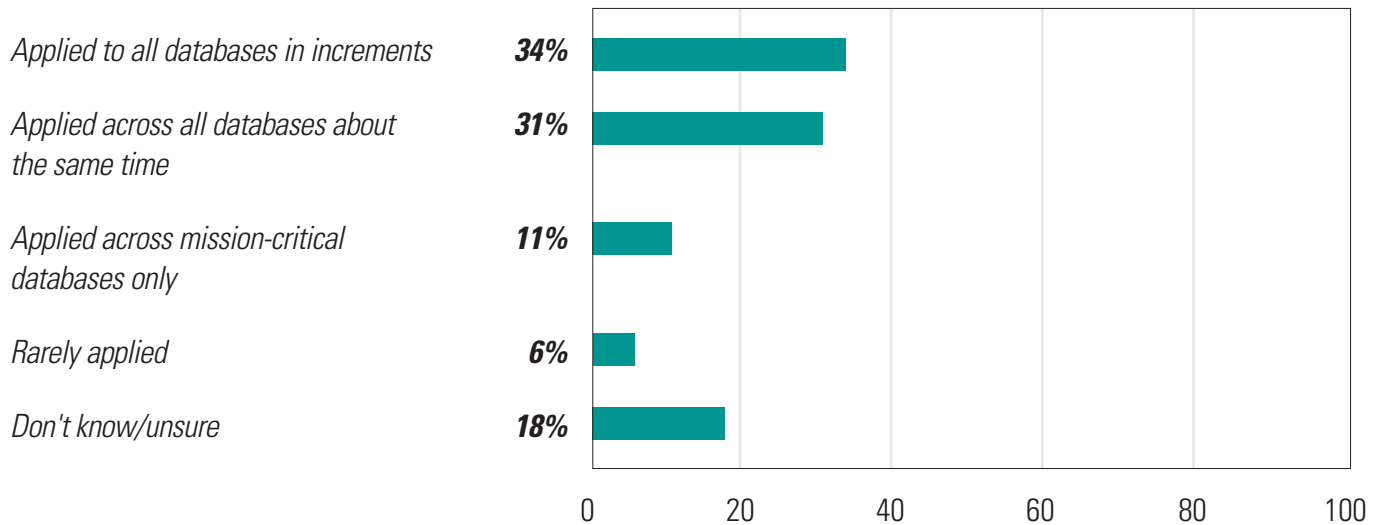
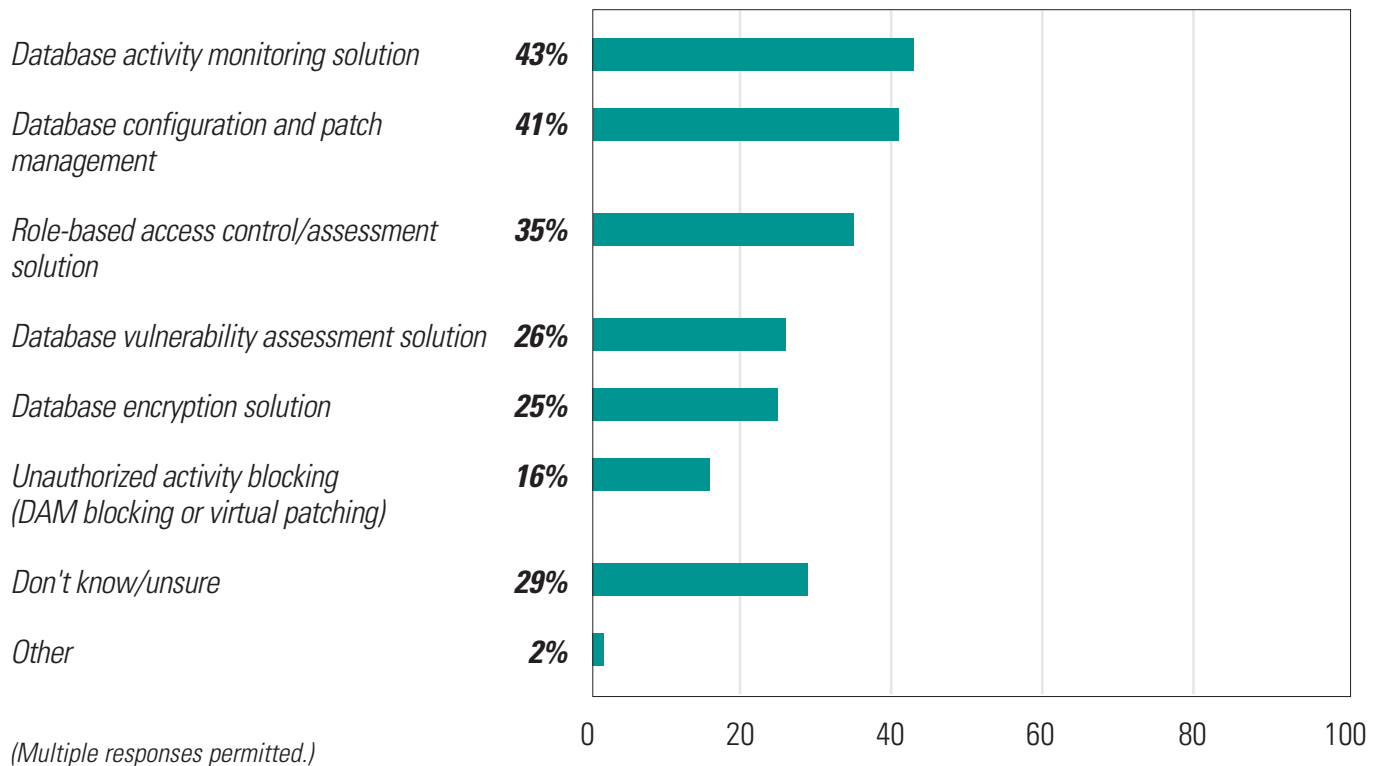


Figure 37: Database Security Technologies Currently Deployed



Data Security at an Inflection Point: 2011 Survey of Best Practices and Challenges was produced by Unisphere Research and sponsored by Application Security, Inc. 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, 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.

Figure 38: Rating the Native Security Offerings of Primary DBMS Vendors

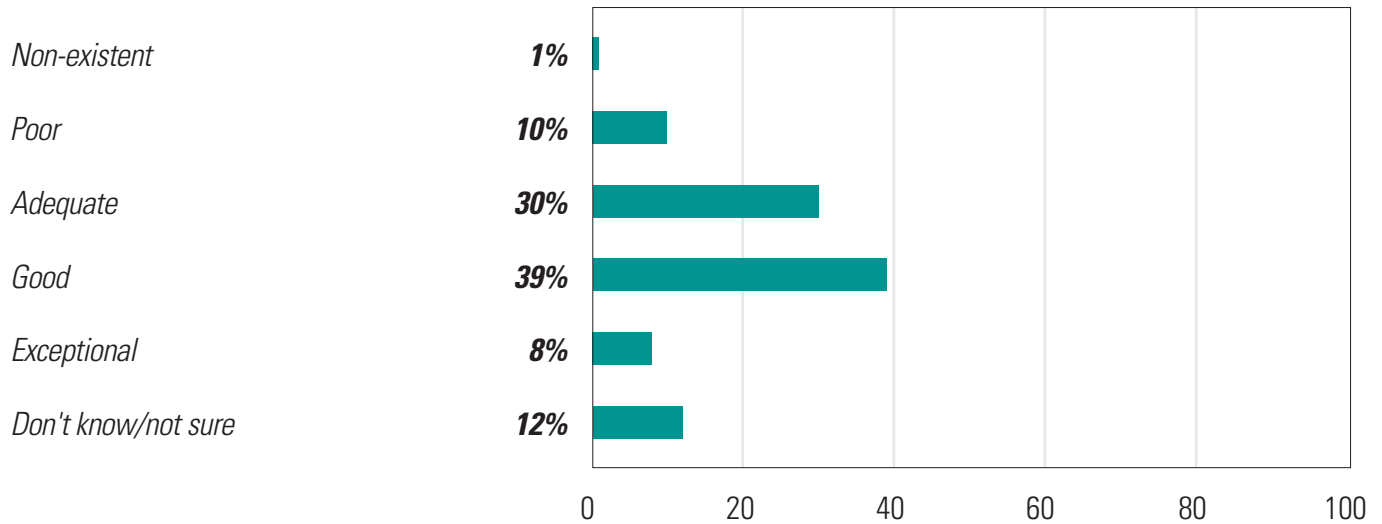


Figure 39: Employ Native Security Offerings of Primary DBMS Vendor?

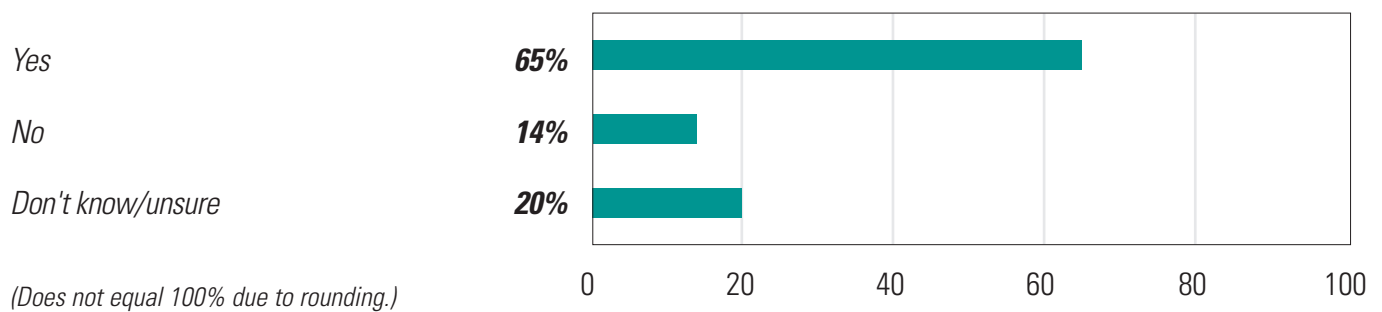
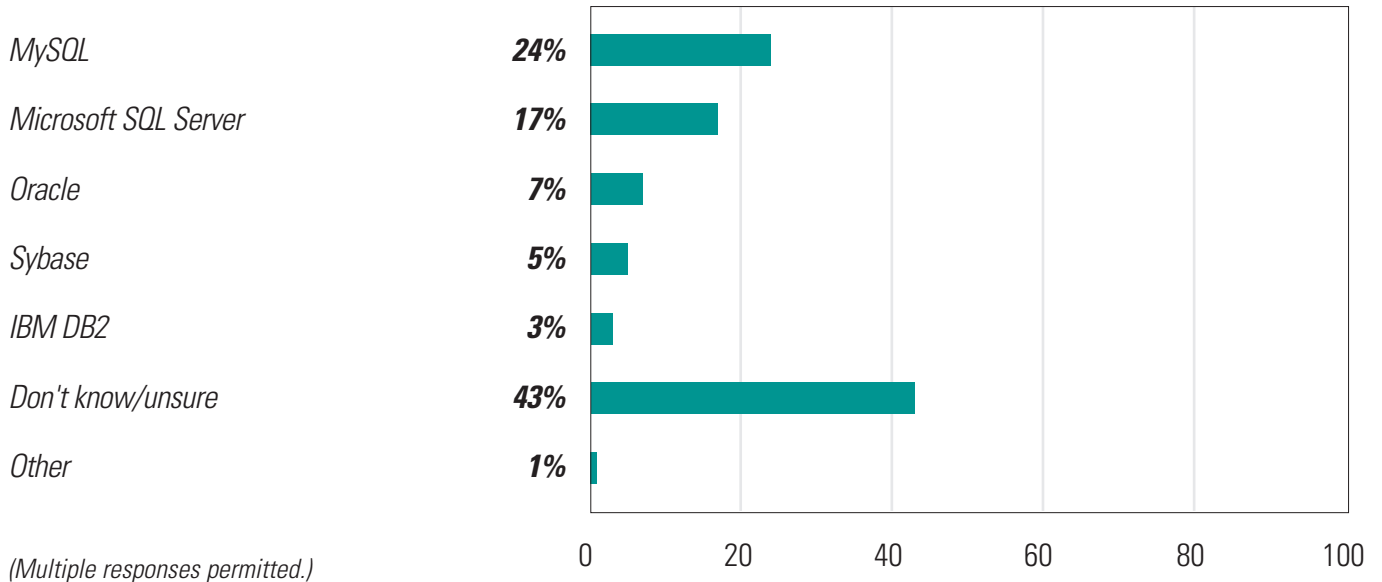


Figure 40: Which Major DBMS Platform is Least Secure



DEMOGRAPHICS

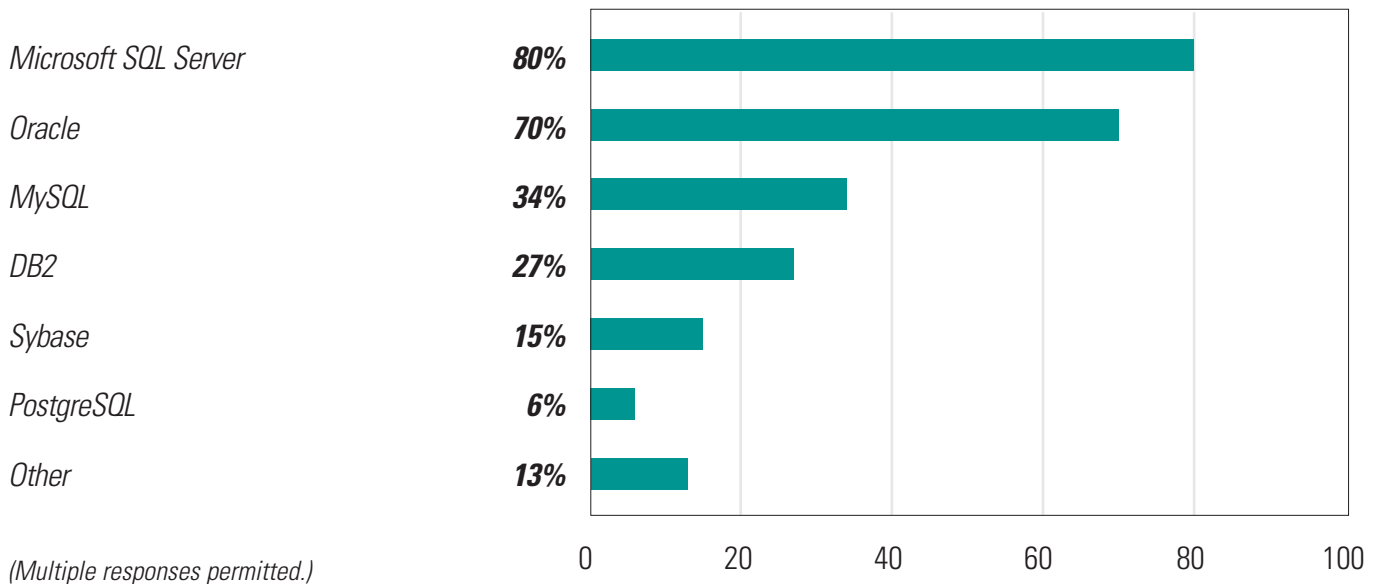
Figure 41: DBMS Platforms Deployed

Figure 42: Respondents' Primary Job Titles

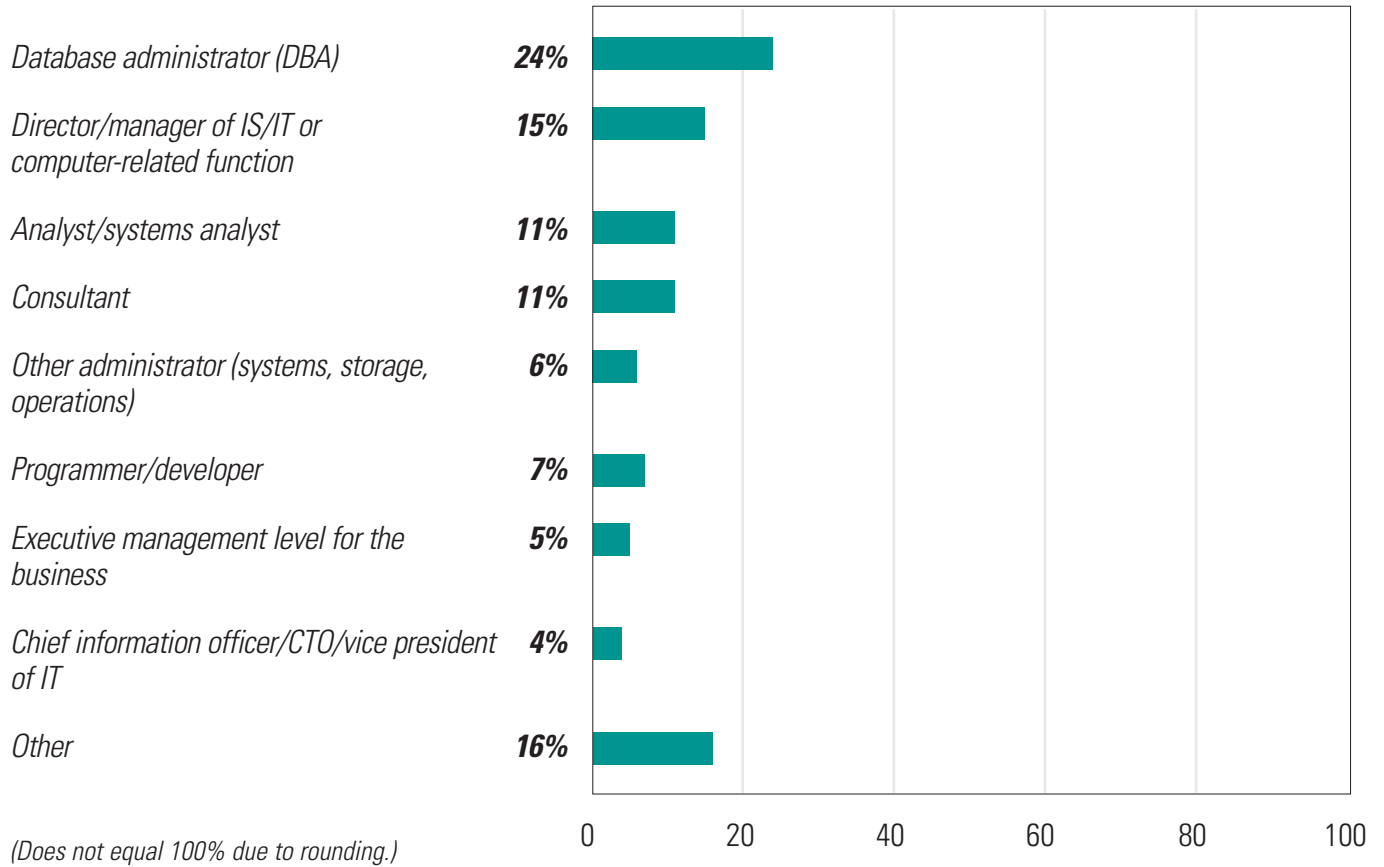


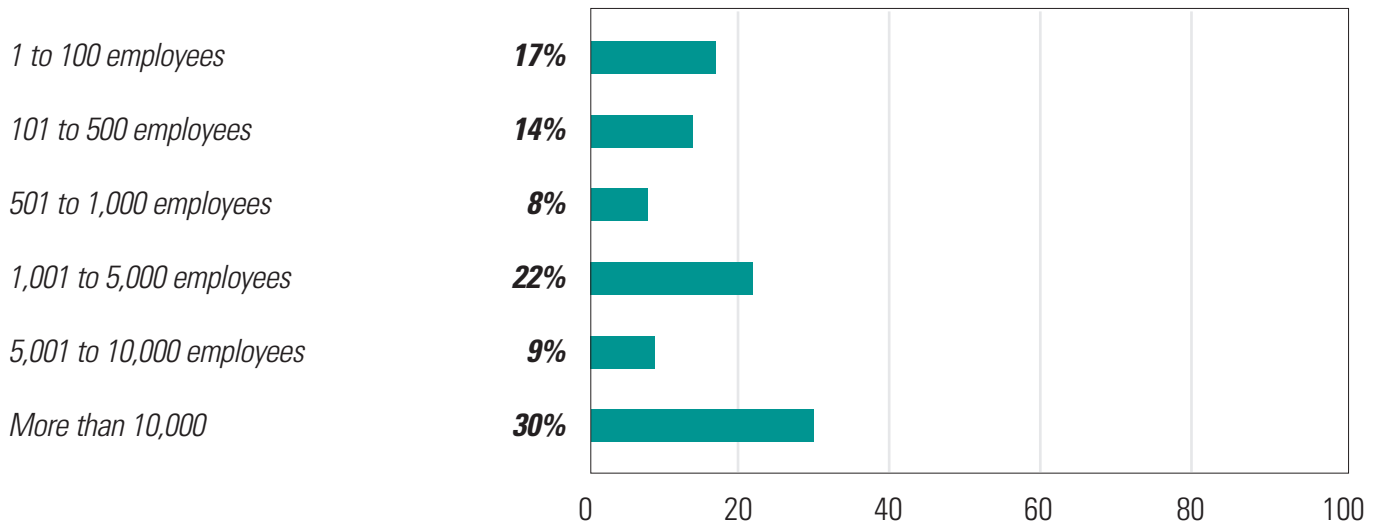
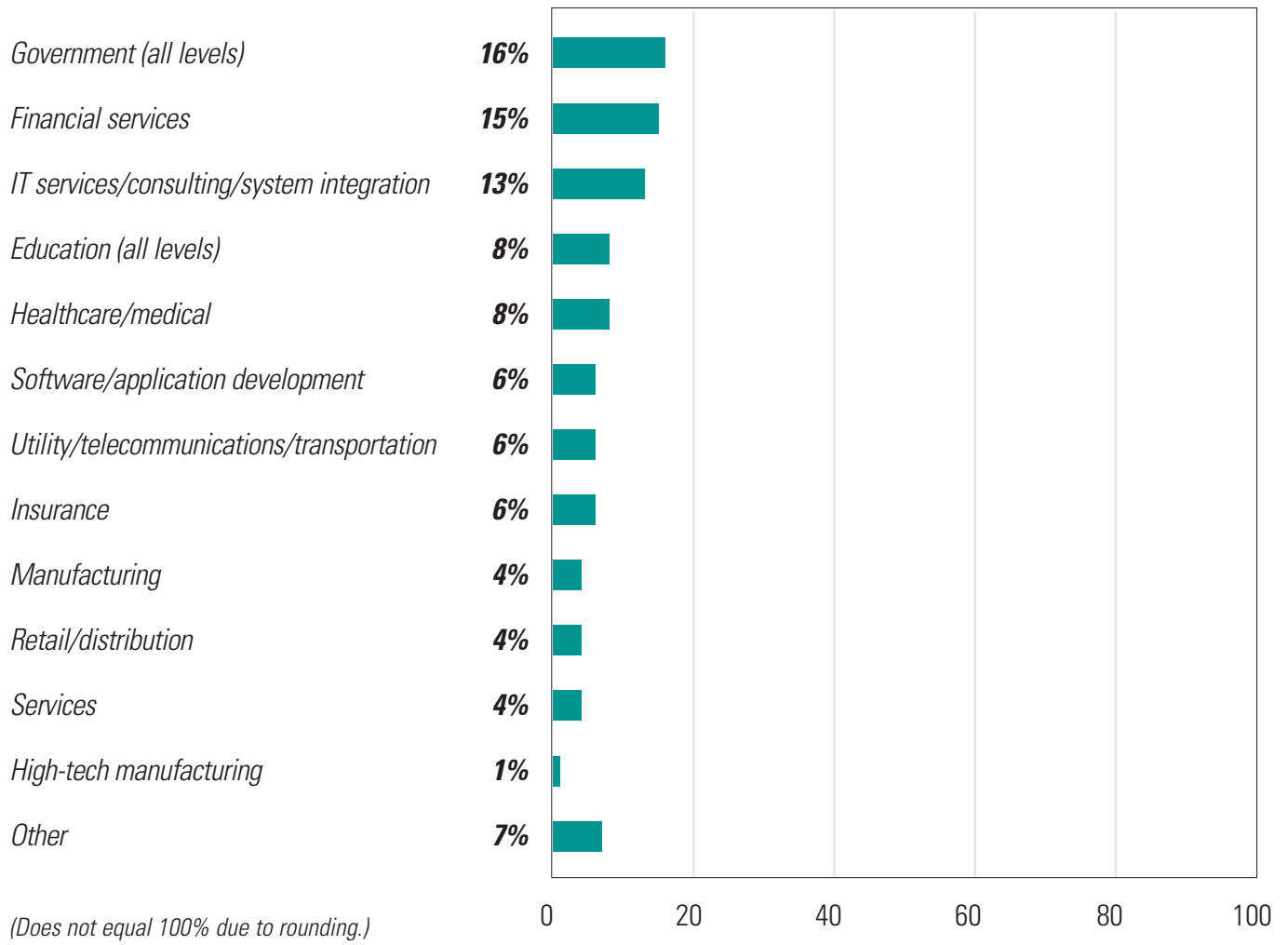
Figure 43: Respondents' Company Sizes—By Number of Employees

Figure 44: Respondents' Primary Industries



Data Security at an Inflection Point: 2011 Survey of Best Practices and Challenges was produced by Unisphere Research and sponsored by Application Security, Inc. 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, 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.