

Sponsored by



Independently Conducted by
Ponemon Institute LLC

Presents

Database Security 2007: Threats and Priorities within IT Database Infrastructure

Published by Ponemon Institute, LLC
June 4, 2007



Application Security, Inc.
575 Eighth Avenue
Suite 1220
New York, NY 10018

Tel: 1-212-912-4100
Fax: 1-212-947-8788
info@appsecinc.com
www.appsecinc.com

2007 Survey on Database Security

By Dr. Larry Ponemon, June 4, 2007

Executive Summary

Technological advancements allow enterprises to be efficient and connected in ways that were not possible in the past. This increased connectivity provides many benefits, but has also left businesses increasingly vulnerable to threats from outsiders as well as entities within their organization. As a result of these challenges, enterprises wrestle with how to protect their intellectual property and prevent the remediation costs and damage to brand that can result from unintended exposure of customer and employee data.

Application Security, Inc. and the Ponemon Institute have conducted this inaugural study on database security to document how business and government organizations secure database resources and respond to targeted threats. This survey queried 649 respondents in corporate information technology (IT) departments within U.S. and EMEA based business or governmental organizations.

The survey focused on four key issues:

1. What does the IT environment look like within organizations? Do size and complexity play a part in determining priorities?
2. How critical is the need to deploy database security measures to protect sensitive or confidential information?
3. How important is database security relative to other information security measures or practices?
4. What are the priorities that drive database security initiatives within business and governmental entities?

Key findings of this survey include:

- Trusted insiders remain a significant, and largely unmonitored risk
- A majority of organizations do not have the technology or processes required to effectively manage against insider threat
- Due to perceived business value, many large organizations assign lower priority to the protection of customer and employee data versus intellectual property
- The vast majority of data exposed in the past two years has been confidential customer and employee information
- Over ninety-five percent of respondents would value solutions that enabled them to understand and prioritize database security needs within their organization.

The survey found that “trusted” insiders’ ability to compromise critical data is the most serious concern for respondent organizations. Despite this concern, fifty-seven percent of those surveyed do not believe that their organizations have taken adequate measures to protect against malicious insiders and fifty-five percent do not believe that they have taken adequate measures to protect against “data loss.”

The survey also found that despite being aware of these threats, inadequate protection of corporate databases is the norm rather than the exception. Forty percent of those surveyed do not have the mechanisms in place, or are unaware of whether databases are monitored for suspicious activity. This shortfall can be attributed to the massive scale of corporate data stores and the lack of IT resources. Eighty-eight percent of those surveyed manage greater than one hundred databases and a majority of respondents manage in excess of 500 databases. Although organizations experience continued and rapid data growth, fifty-four percent of the IT organizations surveyed plan no or only slight staff increases in the coming year.

Despite recent legislation and incentives relative to regulatory and standards based compliance, few organizations rate such activity as a priority for 2007. Forty percent of respondents stated that supporting changes in corporate governance (e.g., Sarbanes-Oxley, PCI, etc.) is not on the agenda. Fifteen percent consider such efforts a low priority.

Over seventy-eight percent of respondents believe that databases are either critical or important to their primary business. However, in a world of mounting priorities and demands, reality has forced organizations to prioritize what data gets protected first and most effectively. Among core security and IT professionals, operational efficiencies and system optimization are consistently higher priorities than efforts related to Sarbanes-Oxley, PCI, NIST 800-53 or other similar compliance initiatives.

The survey results rank data in terms of greatest risk to the core business in the following order:

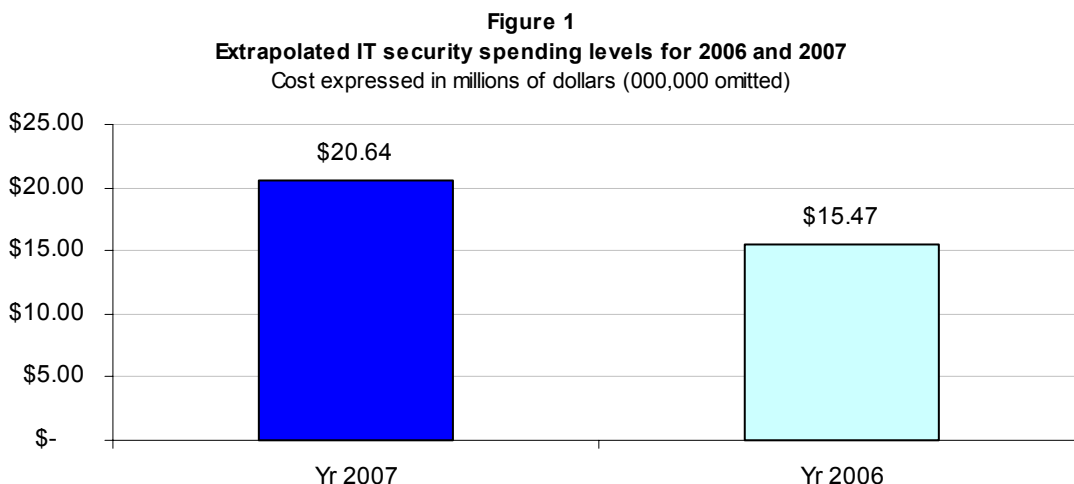
- Intellectual Property
- Business Confidential Information
- Customer and Consumer Data
- Employee Data

Detailed Findings

In today’s environment, IT infrastructure has grown increasingly complex. Multinational companies, distributed environments, and aggressive growth are creating increasingly complicated infrastructure. In order to support these requirements, budgets for information technology, including for security and database solutions, have grown significantly.

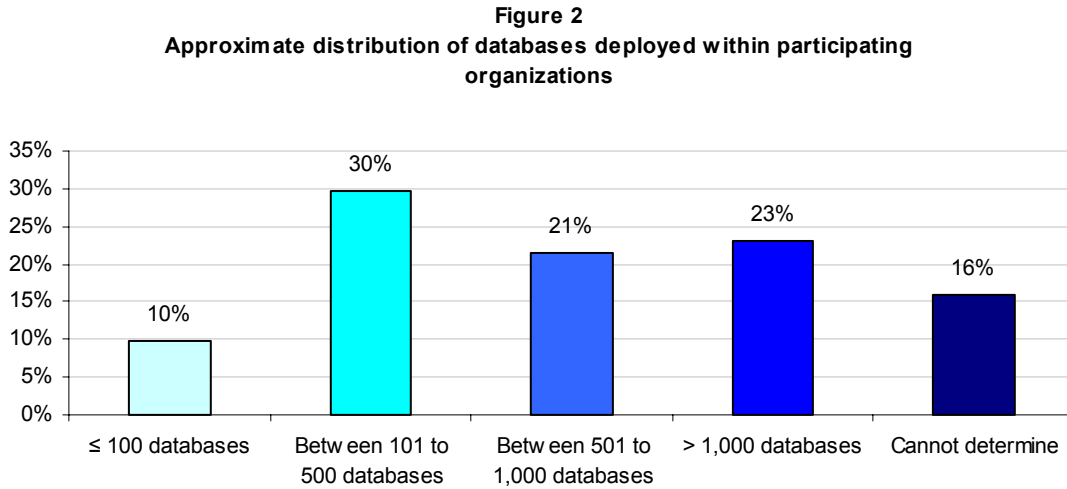
Over seventy-eight percent of the sample contains organizations which reported a corporate IT budget in excess of \$30 million. The extrapolated median value of corporate IT spending for the overall sample is \$94.7 million. From 2006 to 2007, large organizations increased spending for IT security from seventeen to twenty-three percent of the total IT budget. Small companies have likewise increased security spending from fourteen to eighteen percent of their total budget.

Figure 1: Security spending



The need for on-demand access and manipulation of data by both internal and external users is driving database proliferation. Though consolidation efforts continue, the majority of large enterprise organizations nonetheless have hundreds if not thousands of databases, often supporting multiple platforms.

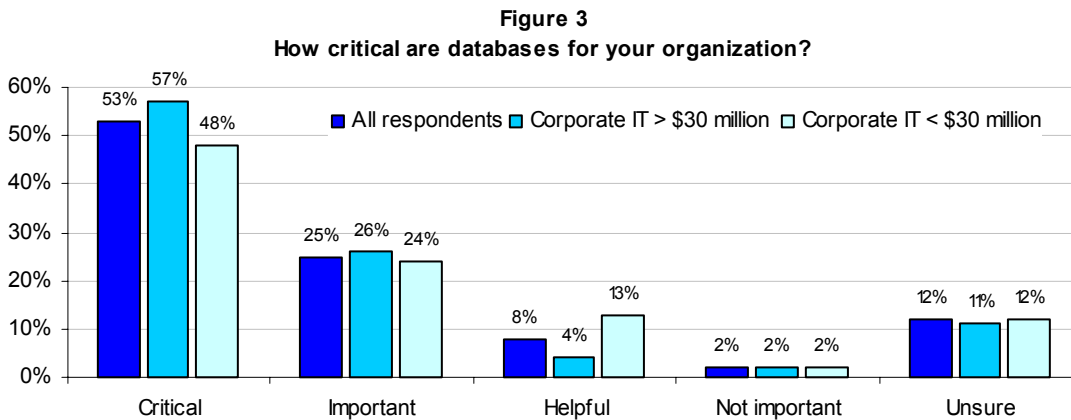
Figure 2: Database deployment



Ninety percent of surveyed organizations reported deployment of more than 100 databases within their organization. Twenty-three percent of organizations reported more than 1,000 databases.

Large and dispersed database installations present significant database security challenges to enterprise organizations. In response to this complexity, organizations are actively seeking database security solutions. Over ninety-five percent of survey respondents reported they would find value in solutions that helped them understand and prioritize database security needs within their infrastructure.

Figure 3: Database importance

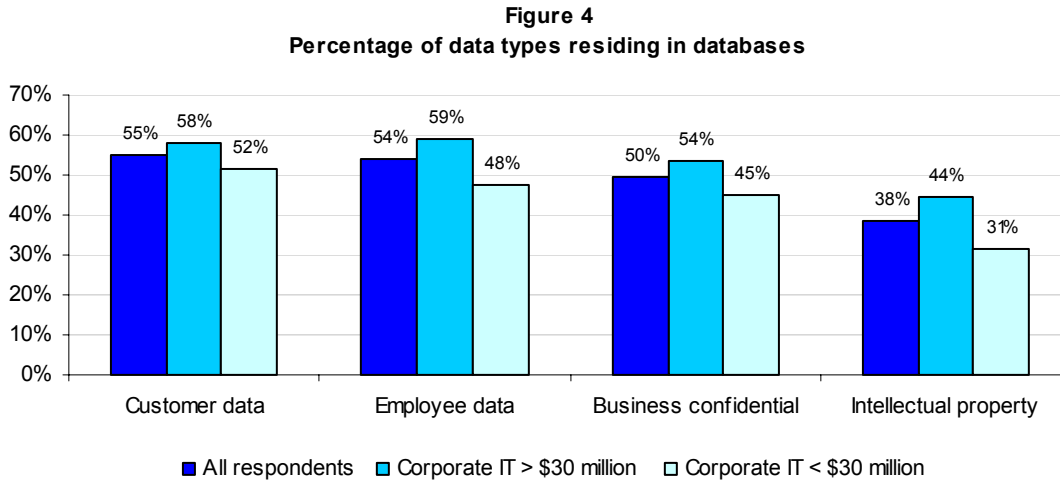


Organizations value their databases enormously. Fifty-three percent ranked database importance as critical, while another twenty-five percent responded with a rating of important. Perhaps more telling is the fact that less than two percent state that databases are not important to their business.

Organizational size had little impact on how organizations value their databases. Large organizations did, however rate the importance as slightly higher than small organizations.

The survey findings also indicate that a majority of organizations support multiple database platforms (SQL, Oracle, DB2, etc.) – twenty-nine percent of respondents stated that they have many different database platforms and thirty-eight percent indicated that their IT environment consists of a few different database platforms. Only twenty-four percent of respondents stated that their organization has standardized on a single database platform.

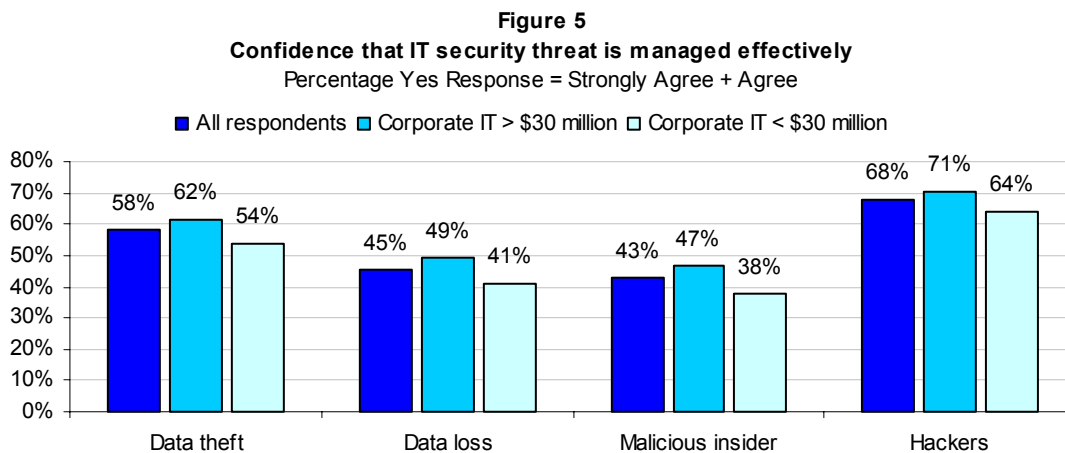
Figure 4: Types of data



Respondents indicated that several types of data reside on corporate databases. The most common data found consists of customer, employee, and business confidential data (fifty-five, fifty-four, and fifty percent respectively.) Intellectual property is less likely to be stored on corporate database and was only cited by thirty-eight percent of respondents. The results indicate that larger organizations are more likely to store multiple information types in corporate databases.

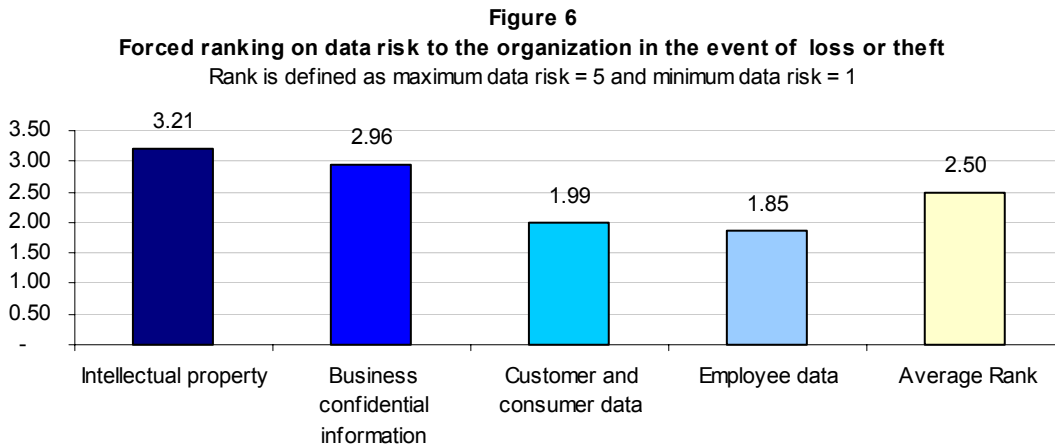
The results also indicate that database usage as a storage facility is inversely related to the risk priority of the same data. For example, the widest disparity is in the area of intellectual property, which was ranked as the highest data risk priority, but least likely to reside on databases.

Figure 5: Database security confidence



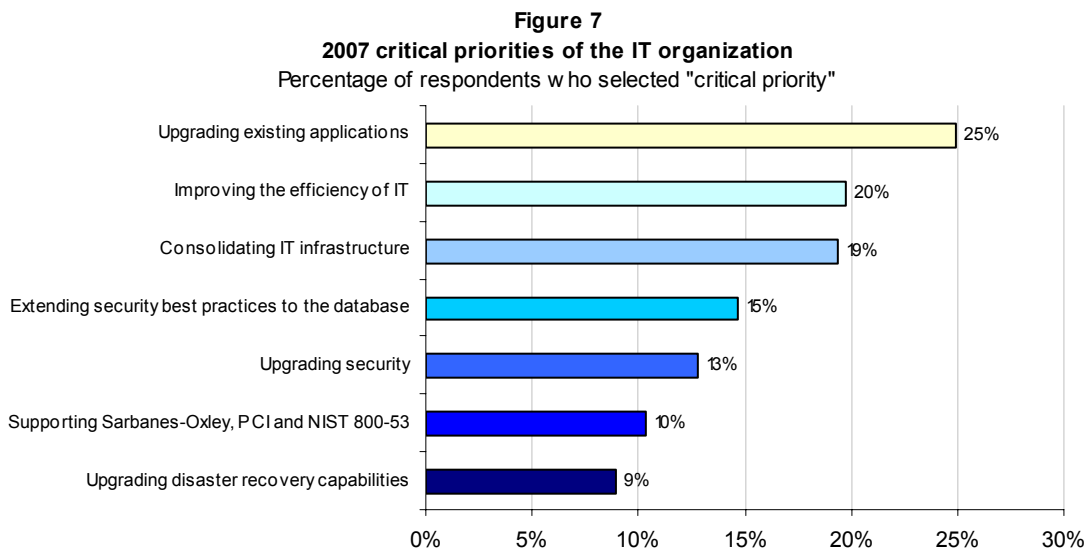
Respondents indicated varying levels of confidence in their organizations' ability to defend against data threats. They are most confident in their ability to negate hacker-related breaches. They have least confidence in their ability to defend against insider threats. Large-sized organizations are more confident than those in smaller-sized companies with respect to all four IT security threats.

Figure 6: Security priorities



Survey respondents ranked securing intellectual property as their highest priority while securing business confidential information was ranked second. Those surveyed assigned the lowest priority to securing employee and customer data.

Figure 7: Overall IT priorities



Respondents indicated that upgrading existing applications is the number one priority, followed by improving the efficiency of IT and consolidating IT infrastructure. Upgrading disaster recovery capabilities and supporting corporate governance initiatives such as Sarbanes-Oxley, PCI and NIST 800-53 score lowest on the critical priority list. In fact, forty percent of respondent organizations stated that supporting changes in corporate governance (e.g., Sarbanes-Oxley, PCI) was not on the agenda for 2007. These results indicate that despite several well publicized breaches in the past year, respondents do not currently make the protection of customer or employee information a high priority.

Conclusion

Our research findings suggest that information security practitioners understand the importance of databases and their role in advancing secure business operations. They also indicate a growing need to deploy database security solutions that address and minimize the risks of data loss, data theft, insider threats and hacker activity.

Despite this understanding, however, our results show that intellectual property and business confidential information in databases is not generally protected. Even in the face of frequent, expensive, and highly publicized breaches, respondents have not made protecting customer and employee information a high priority.

Our findings also suggest that smaller-sized organizations (with an annual IT budget less than \$30 million) spend a smaller percentage of their overall IT budget on security, including database security. This may explain why respondents from these companies are less confident in their ability to protect sensitive or confidential information.

Respondents to the survey have made corporate governance and regulatory compliance (including Sarbanes-Oxley and PCI) a low priority in 2007. The results indicate that compliance incentives and/or punishments have not yet reached a threshold sufficient to motivate IT behavior.

These observations are preliminary. We believe further research is needed regarding the use of database security and the controls necessary to secure data at rest. If you have questions or comments about this research report or you would like to obtain additional copies of the document (including permission to quote from or reuse this report), please contact us by letter, telephone or email.

About Application Security, Inc

Application Security, Inc. is the leading provider of database security solutions. The company's DbProtect suite, the industry's only complete database security solution combining database vulnerability assessment, database activity monitoring, database intrusion detection and auditing has helped over 800 enterprise organizations secure their databases from internal and external threats while also ensuring that those organization meet or exceed regulatory compliance requirements. Our security experts, combined with our strong support team, deliver up-to-date database protection that minimizes risk and allows organizations to confidently connect with customers, partners, and suppliers.

About Ponemon Institute, LLC

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the Council of American Survey Research Organizations (CASRO), we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions. For more information, please visit <http://www.ponemon.org>.

APPENDIX I

Polling Methods and Respondents

A random sampling frame of 11,140 adult-aged individuals who reside within the United States was used to recruit participants to this Web survey. Our randomly selected sampling frame was selected from three national mailing lists of information security professionals. In total, 750 respondents completed their survey results during an eight day research period. Of returned instruments, 101 survey forms were rejected because of reliability checks. A total of 649 surveys were used as our final sample. This sample represents a 5.8% net response rate. The margin of error on all adjective scale and Yes/No/Unsure responses is $\leq 3\%$.

Over 90% of respondents completed all survey items within 12 minutes. Respondents were given the following instruction before starting the survey.

Your participation is completely confidential. No personally identifiable or company identifiable information is requested. All responses will be compiled, analyzed, and distributed at an aggregate level.

The purpose of this study is to learn important information about your organization's IT security budget. If you have specific questions or issues regarding this survey, please contact Ponemon Institute, LLC at 800.887.3118. Or, send us an e-mail to research@ponemon.org.

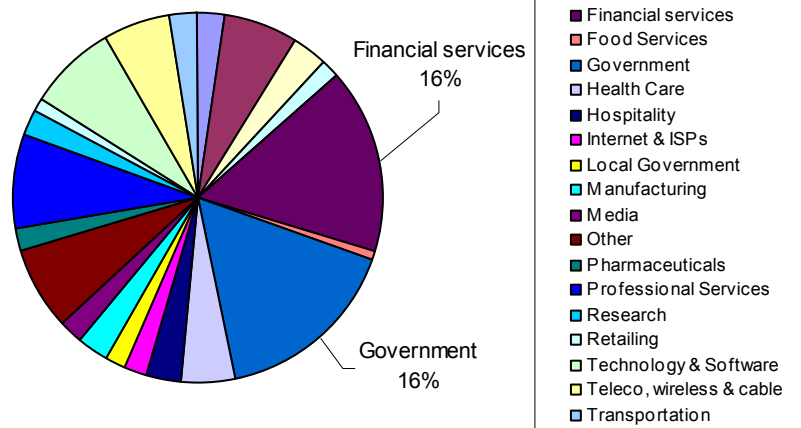
Following are demographics and organizational characteristics for 649 respondents. Table 1a reports the most frequently cited job titles of respondents (Top 5 list). Table 1b provides the self-reported organizational level of respondents. As can be seen, the majority of respondents are at the manager (28%) or director (21%) levels, respectively.

Table 1a: Job Titles (Top 5 Titles)	Freq.	Pct%
Manager, information systems	81	12%
Director, information security	73	11%
Director, network security	65	10%
Information systems auditor	47	7%
Chief information security officer	45	7%
All other titles	338	52%
Total	649	100%

Table 1b: Organizational levels	Freq.	Pct%
Senior Executive	41	6%
Vice President	37	6%
Director	175	27%
Manager	189	29%
Associate/Staff	130	20%
Other	77	12%
Total	649	100%

Pie Chart 1 reports the percentage distribution of respondents by major industry classification. As shown below, over 16% of respondents are employed in financial services or in federal, state or local government. Financial services include banks, insurance, credit cards, and brokerage.

Pie Chart 1: Distribution of Respondents by Industry Classification



On average, respondents have over seven years of experience in the information security field and over four years of experience in their current position. In total, 81% of respondents were males and 19% females. While results are skewed on the gender variable (more male than female respondents), this result is consistent with known demographics about the information security field in North America.

Over 62% of respondents state that their job function or position is located within the corporate CIO or CTO departments. About 15% state that they report to the organization's information security leader (CISO or CSO) and 6% state that they report to the company's chief risk officer.

Table 2a reports the global footprint of organizations that employ respondents. Table 2b provides the approximate headcounts of these companies. As can be seen, 64% of respondents are employed by larger-sized organizations (with more than 5,000 employees).

Corporate locations	Freq.	Pct%
United States	567	87%
Canada	11	2%
EMEA	47	7%
Latin America	3	0%
Asia-Pac	21	3%
Total	649	100%

Corporate headcount	Freq.	Pct%
Less than 500 people	34	5%
500 to 1,000 people	49	8%
1,001 to 5,000 people	148	23%
5,001 to 25,000 people	135	21%
25,001 to 75,000 people	163	25%
More than 75,000 people	120	18%
Total	649	100%

APPENDIX II

Detailed Results

The detailed findings are reported below. The survey question frequencies and percentage frequencies are reported in tabular format. The abbreviation “Pct%” denotes that the table percentages sum to the sample total. The column heading “Total%” means that the table percentages sum to the response sample total (which is greater than the sample total if a given question allows more than one response).

Table 3 shows that about 70% of the total sample of respondents have responsibility for all or part of their company’s IT budget. As noted above, we used the sub-sample of 453 individuals to extrapolate spending on databases, IT security and database security.

Table 3 Are you responsible for managing all or part of your organization’s IT budget in 2007?	Freq.	Pct%
Yes	453	70%
No	196	30%
Total	649	100%

Table 4 reports the budget range for corporate IT spending for the sub-sample. The extrapolated average value is approximately \$94.71 million for the group of 453 respondents with budget responsibilities in 2007.

Table 4 Approximately, what is the dollar range that best describes your organization’s IT budget for 2007?	Freq.	Pct%
Less than \$1 million	6	1%
Between \$1 to 2 million	7	2%
Between \$2 to \$5 million	8	2%
Between \$5 to \$10 million	10	2%
Between \$10 to \$15 million	8	2%
Between \$15 to \$20 million	20	4%
Between \$20 to \$30 million	43	9%
Between \$30 to \$40 million	38	8%
Between \$40 to \$50 million	34	8%
Between \$50 to \$100 million	128	28%
Between \$100 to \$200 million	110	24%
Over \$200 million	41	9%
Total	453	100%

Table 5 reports the budget range for corporate IT spending earmarked for databases. The extrapolated average value is approximately \$32.23 million for the group of 453 respondents with budget responsibilities in 2007.

Table 5 Approximately, what percentage of the 2007 corporate IT budget will go to infrastructure for databases?	Freq.	Pct%
Less than 5%	30	7%
Between 5% to 10%	52	11%
Between 10% to 20%	94	21%
Between 20% to 30%	64	14%
Between 30% to 40%	36	8%
Between 40% to 50%	76	17%
Between 50% to 60%	32	7%
Between 60% to 70%	8	2%
Between 70% to 80%	37	8%
Between 80% to 90%	15	3%
Between 90% to 100%	9	2%
Total	453	100%

Table 6 reports the budget range for corporate IT spending earmarked for security. The extrapolated average value is approximately \$20.64 million for the group of 453 respondents with budget responsibilities in 2007.

Table 6 Approximately, what percentage of the 2007 corporate IT budget will go to security (including database security)?	Freq.	Pct%
Less than 5%	78	17%
Between 5% to 10%	124	27%
Between 10% to 20%	66	15%
Between 20% to 30%	75	17%
Between 30% to 40%	31	7%
Between 40% to 50%	20	4%
Between 50% to 60%	34	8%
Between 60% to 70%	10	2%
Between 70% to 80%	10	2%
Between 80% to 90%	4	1%
Between 90% to 100%	1	0%
Total	453	100%

Table 7 reports the priority ranking of four different types of data from 1 = highest priority. It is clear that the highest priority data is intellectual property, and the lowest data priority concerns employee records.

Table 7 What kinds of data present the greatest risk to your organization if it is lost or stolen? Please rank from 1=highest risk to 4=lowest risk.	Forced Rank	Rank
Customer and consumer data	3.01	3
Intellectual property	1.79	1
Business confidential information	2.04	2
Employee data	3.15	4

Table 8 shows the percentage of company's sensitive information about customers, employees, confidential business information and intellectual property that might reside in corporate databases. It shows that customer and employee data are most likely to reside in corporate databases. Intellectual property is least likely to reside in a corporate database.

Table 8 Approximately, what percentage of your company's sensitive information about {insert data type} is stored in databases?	Customer data	Employee data	Business confidential data	Intellectual property
Less than 5%	5%	6%	7%	16%
Between 5% to 10%	9%	6%	6%	12%
Between 10% to 20%	4%	10%	13%	6%
Between 20% to 30%	7%	8%	12%	7%
Between 30% to 40%	8%	7%	4%	11%
Between 40% to 50%	7%	7%	7%	12%
Between 50% to 60%	12%	8%	9%	10%
Between 60% to 70%	11%	8%	7%	7%
Between 70% to 80%	8%	10%	14%	12%
Between 80% to 90%	11%	14%	5%	3%
Between 90% to 100%	18%	16%	15%	3%
Total	100%	100%	100%	100%
Extrapolated average	55%	54%	50%	38%

Table 9 reports the level of confidence that respondents have in combating four common IT security threats. Figure 2 shows that respondents are most confident about stopping hacker-related incidents, and are least confident about resolving malicious insider threats.

Table 9 I feel confident that sensitive or confidential information residing in our company's databases are protected against {threat}.	Data theft	Data loss	Malicious insider	Hackers
Strongly agree	24%	15%	11%	26%
Agree	34%	31%	31%	42%
Unsure	18%	23%	30%	15%
Disagree	16%	21%	17%	12%
Strongly disagree	8%	10%	10%	5%
Total	100%	100%	100%	100%

Table 10 reports the frequency of separate databases that reside within respondent companies. The extrapolated average is 485 databases for the sample. Figure 4 shows this average for larger-sized and smaller-sized organizations.

Table 10 Approximately, how many databases does your company have?	Freq.	Pct%
□ 2 databases	8	1%
Between 3 to 25 databases	4	1%
Between 26 to 50 databases	14	2%
Between 51 to 100 databases	38	6%
Between 101 to 500 databases	193	30%
Between 501 to 1,000 databases	139	21%
> 1,000 databases	149	23%
Unsure	104	16%
Total	649	100%

Table 11 reports how respondents define their organization's database environment. As shown, most companies are using more than one primary database solution within their organization.

Table 11 Please check the one option below that best describe your present database environment.	Freq.	Pct%
Our IT environment consists of many different types of database types and technologies.	188	29%
Our IT environment consists of a few different types of database types and technologies.	249	38%
Our IT environment consists of one primary database type and technology.	159	24%
I cannot determine	53	8%
Total	649	100%

Table 12 shows the databases most frequently used by respondents within their organizations. It also shows the databases most likely to be used to house the organization's most critical applications. Figure 6 reports findings for larger-sized and smaller-sized organizations. Findings show that the most popular databases are SQL, Oracle, Sybase and DB2.

Table 12 What types of databases currently exist within your organization? Please check all that apply.	Databases used	Total%	Databases that house most critical data	Total%
Oracle	277	21%	245	23%
DB2	257	20%	245	23%
SQL	283	22%	215	20%
Sybase	269	21%	173	16%
MySQL	116	9%	102	10%
Other	100	8%	87	8%
Total	1302		1067	

Table 13 reports the importance that respondents attribute to database technology. It clearly shows that over 78% of respondents believe that databases are either critical or important to their primary business. Figure 5 shown above provides a bar chart for these results.

Table 13 Which statement best describes the role of corporate database resources in your business?	Freq.	Pct%
Databases are critical to our business	345	53%
Databases serve an important role, but are not critical to our business	163	25%
Databases are helpful , but do not serve an important role in our business	54	8%
Databases are not important to our business	12	2%
Unsure	75	12%
Total	649	100%

Table 14 reports the percentage frequency of major corporate IT initiatives underway in 2007 for respondent companies. Figure 7 reports a bar chart for those initiatives considered a critical priority by respondents.

Table 14 Which of the following initiatives are likely to be one of your IT organization's major areas of focus during 2007? Please use the adjacent scale from "critical priority" to "not on our company's agenda."	Critical priority	High priority	Low priority	Not on our agenda	Total
Significantly upgrading your security environment	13%	53%	5%	29%	100%
Replacing or upgrading existing application systems	25%	46%	11%	18%	100%
Extending security best practices to the database	15%	31%	19%	36%	100%
Supporting changes in corporate governance (e.g., Sarbanes-Oxley, PCI)	10%	35%	15%	40%	100%
Consolidating IT infrastructure	19%	29%	11%	40%	100%
Significantly upgrading disaster recovery capabilities	9%	30%	33%	28%	100%
Improving the efficiency of IT by delivering more with less through automation	20%	31%	23%	26%	100%

Caveats

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most Web-based surveys.

- **Non-response bias:** The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.
- **Sampling-frame bias:** The accuracy of contact information and the degree to which the list is representative of individuals who are information security practitioners. Compensation was provided to ensure that respondents completed the survey task in a short holdout period. While compensation was held to a nominal amount, we acknowledge potential bias caused by compensating subjects to complete this research within a holdout period. Finally, because we used a Web-based collection method, it is possible that non-Web responses by mailed survey or telephone call would result in a different pattern of findings.
- **Self-reported results:** The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide a truthful response.