Market Research Study

Database Security and Compliance Risks

By Jon Oltsik

December, 2009

An ESG Market Research Study Sponsored by Application Security, Inc.

Contents

Executive Summary

Summary of Report Conclusions

In October 2009, the Enterprise Strategy Group (ESG) conducted a comprehensive web-based survey on behalf of Application Security, Inc. The survey included 175 North American security professionals from enterprise-class organizations (defined as those with 1,000 or more employees) focused on their database security and regulatory compliance policies, experiences, and strategies. Respondents came from over 20 industries in the public and private sectors. To a great extent, this research project built upon data and analysis from a similar effort conducted in 2008.

Based upon this research, ESG concludes that there are a large number of independent risks to confidential data[1] stored in databases and that many large organizations remain extremely vulnerable to compliance audit failures and data breaches. Similar to 2008, users recognize weaknesses in their security processes, controls, and technologies, but continue to lack the adequate funding, senior management oversight, organizational support, and security skills needed to address these issues.

ESG believes that this data indicates a clear and present danger as corporate database security weaknesses leave hundreds of millions of users vulnerable to a breach of their personal data or, worse yet, identity theft. In 2008 alone, 706 publicly-disclosed data breaches exposed over 85 million personal records.[2]

The impact of security weaknesses like those described in this report on society at large have not escaped the attention of governments around the world—many are now demanding action. For example, in May 2009, U.S. President Barack Obama released a long-awaited *Cyberspace Policy Review* report which detailed significant security weaknesses to government agencies and privately-held critical infrastructure like power plants, communications networks, and health care organizations. Upon the release of the report, President Obama declared that he would henceforth treat the nation's entire digital infrastructure as a critical asset. The president stated, "Protecting this infrastructure will be a national security priority. We will ensure that these networks are secure, trustworthy, and resilient. We will deter, prevent, detect, and defend against attacks and recover quickly from any disruptions or damage."

Like the *Cyberspace Policy Review,* this ESG report should be viewed as yet another metric describing the fragile state of data security. Hopefully, this report will have a similar effect. ESG recommends that business, IT, and security managers review this data, initiate broad-based database security and compliance reviews, and lead their organizations to address these critical database security gaps soon.

[1] For the purposes of this survey, confidential data is defined as information that can be categorized as:

- Intellectual property
- Information that is protected by government regulations
- Non-public private information (NPPI)
- Information that is protected by industry regulations
- Information classified as company confidential or private

[2] Source: datalossdb.org

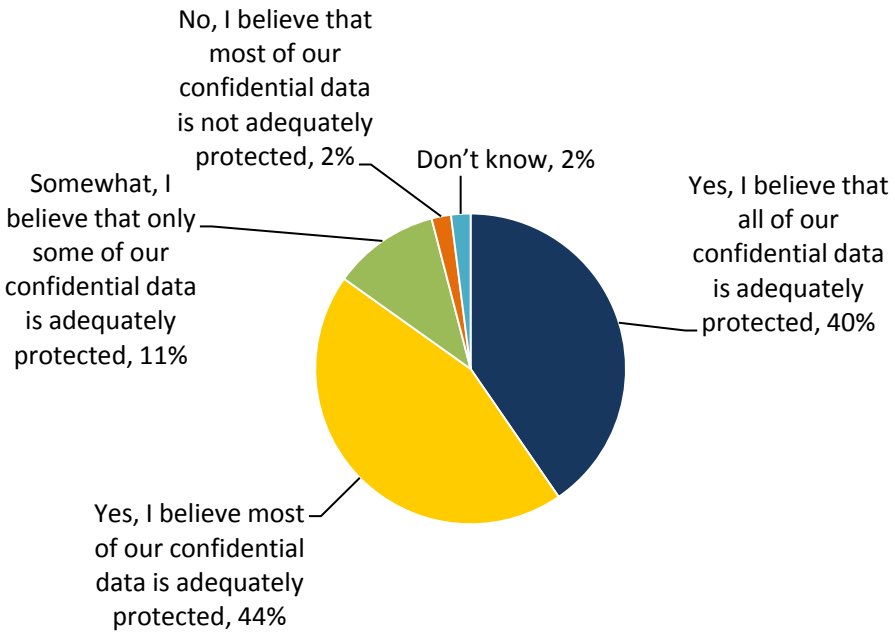
Report Conclusions

Based upon the data derived from this survey, ESG believes that:

- **Confidential data remains unprotected.** Only 40% of security professionals indicated that existing controls can adequately protect all of their organization's confidential data while the remainder of respondents reported numerous data security gaps. Alarmingly, 13% of large organizations believe that some or most of their organization's confidential data continues to be unprotected for the most part (see Figure 1). On a more focused level, ESG's data revealed similar weaknesses related directly to database security: Less than half of all organizations believe that their existing database security controls provide adequate protection for all of the databases (containing confidential data) distributed across the enterprise.

Figure 1. Confidential Data Remains Unprotected

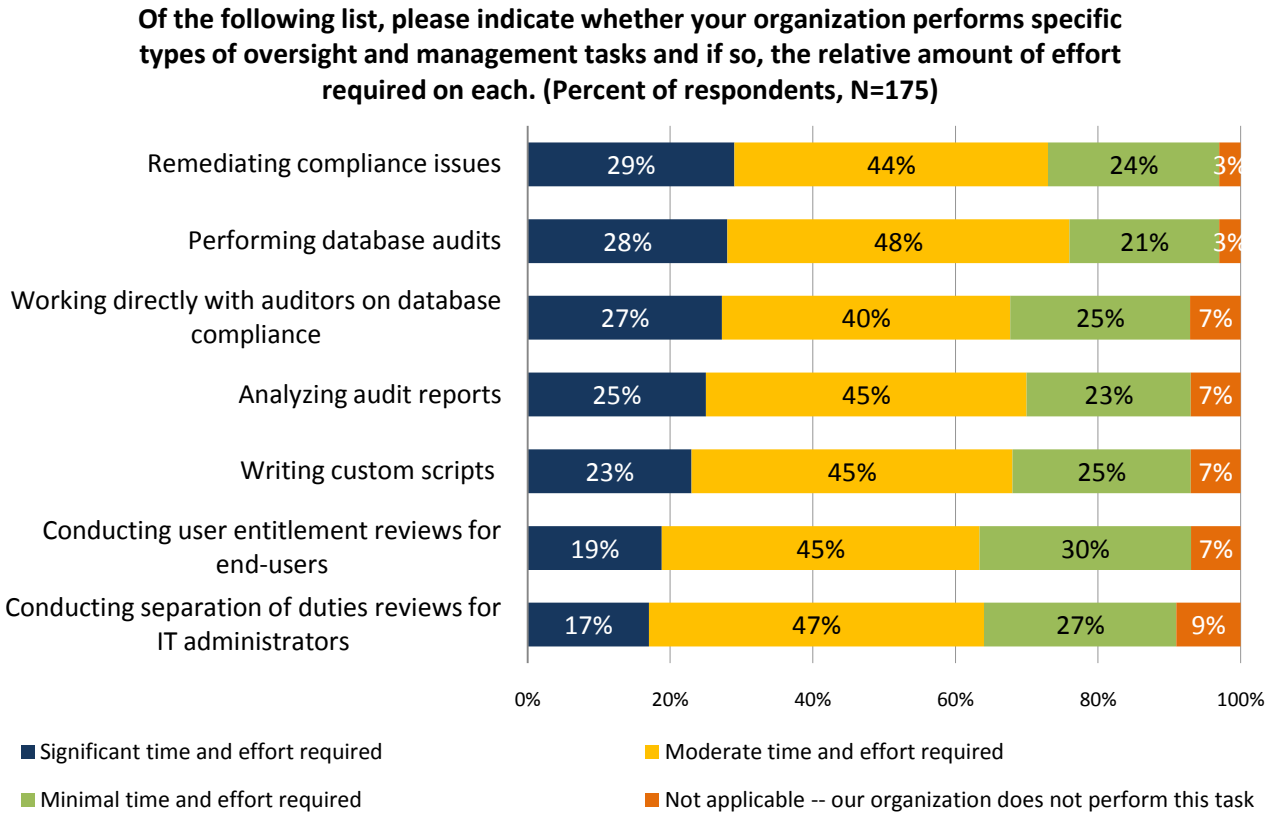
Given today's security and regulatory compliance requirements, do you feel that your organization's existing data security controls provide an adequate level of protection for confidential data? (Percent of respondents, N=175)



Source: Enterprise Strategy Group, 2009.

- **Regulatory compliance is a major security driver, but large organizations still depend upon manual, time consuming database security processes.** Nearly one-third of users claim that regulatory compliance will continue to have the biggest impact on overall security requirements, strategies, and purchasing plans over the next 12 to 24 months. Given this compliance focus, it is quite surprising that more than 25% of large organizations spend a "significant amount of time and effort" and more than 40% spend "a moderate amount of time and effort" on manual processes like remediating compliance issues, performing database audits, and working with auditors on database compliance (see Figure 2). This indicates that many organizations are investing their security and compliance dollars in the wrong places, on things like general purpose security tools and "check box" compliance processes and solutions. This strategy, which cannot formalize processes, automate security operations, or address real risks, is bound to fail over time.

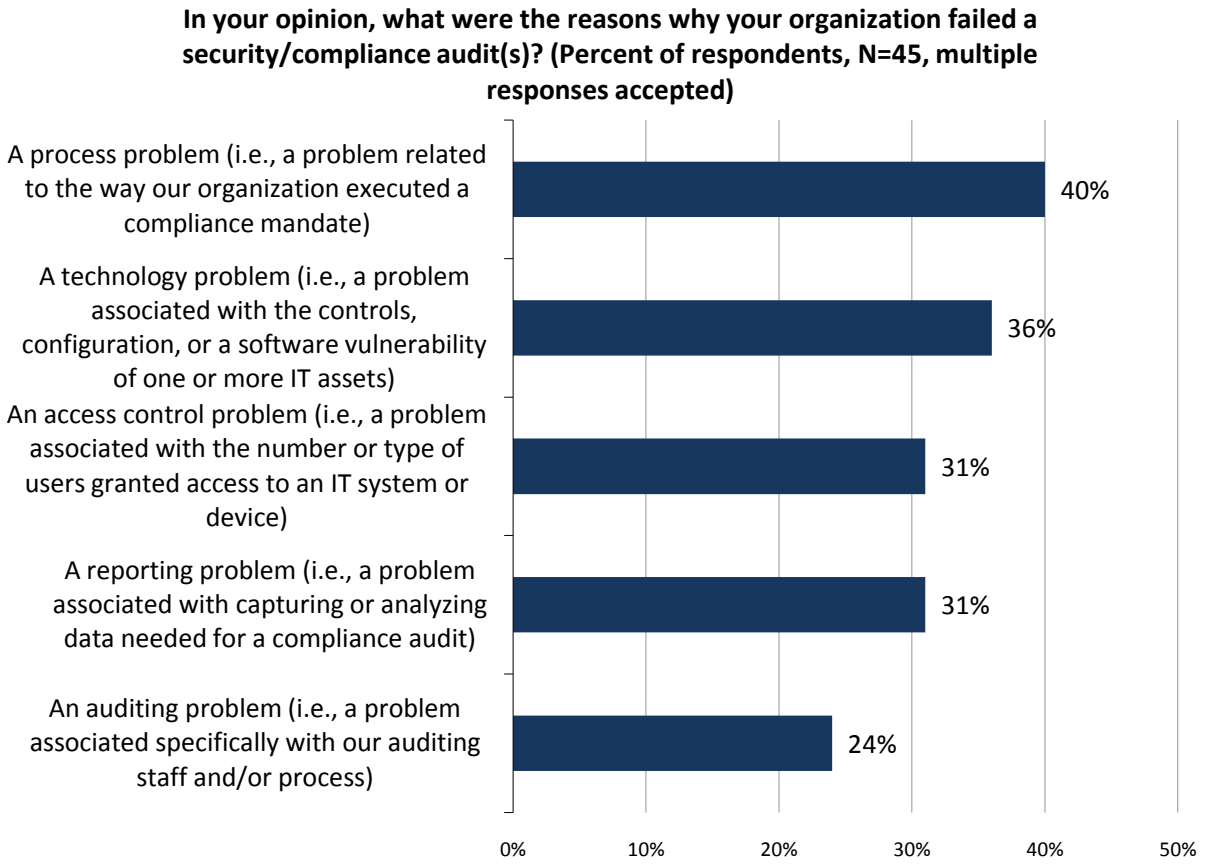
Figure 2. Organizations Rely on Manual Processes for Regulatory Compliance



Source: Enterprise Strategy Group, 2009.

- **Large organizations have trouble passing compliance audits.** In spite of the fact that a majority of large organizations claim that compliance has the greatest impact on data security, only 37% of security professionals believe that their organizations can meet regulatory compliance requirements with respect to ensuring the security of confidential or sensitive information at all times. As a result, nearly 30% of organizations admit that they failed a security/compliance audit regarding data privacy or security within the past three years. Why? A myriad of problems: Large organizations said that compliance audit failures were the result of process problems, technology problems, access control problems, and reporting problems (see Figure 3). Given the number of time-consuming manual processes described above, this is not a surprise.

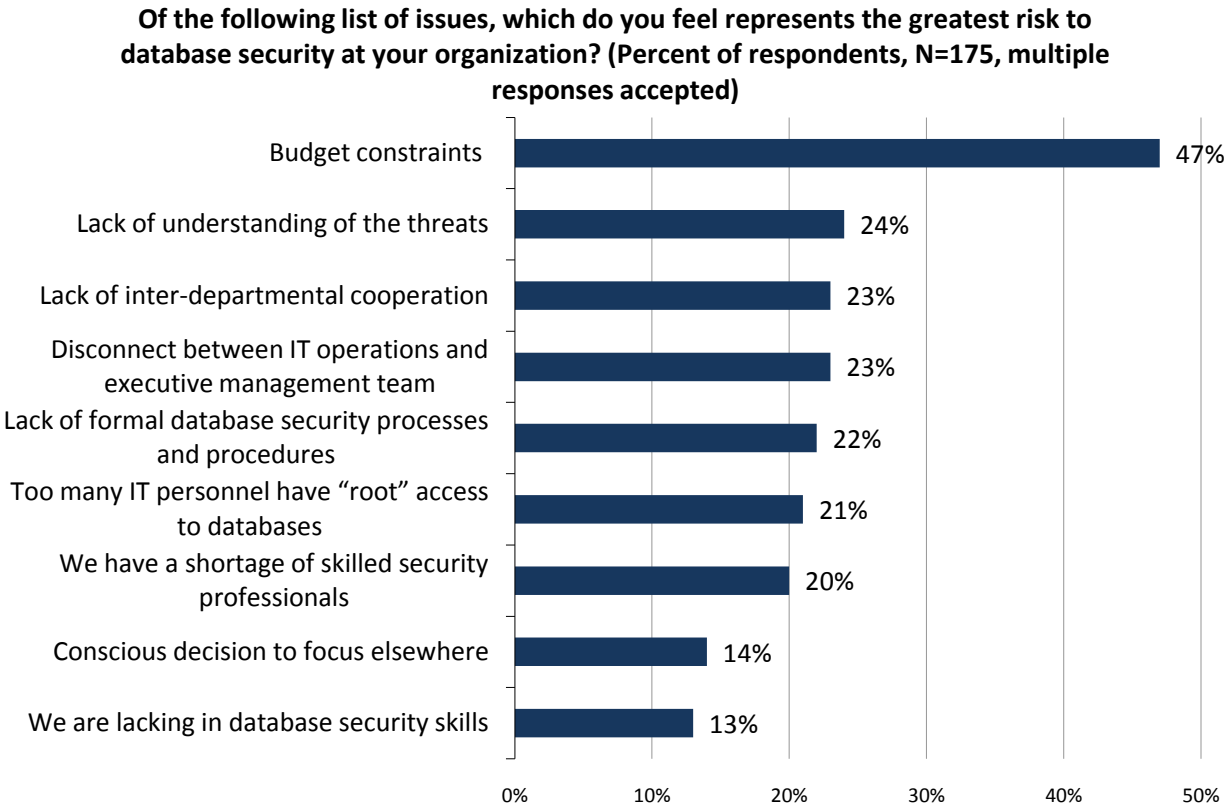
Figure 3. Large Organizations Identify Problems Leading to Compliance Audit Failures



Source: Enterprise Strategy Group, 2009.

- **Existing database controls for regulatory compliance requirements are mismatched.** Here's another reason why large organizations are failing their compliance audits: Less than one-fourth of large organizations believe that their database controls are extremely well defined and documented. In other words, a lot of confidential data is protected with database controls that are managed and monitored on an informal, ad-hoc basis. Clearly, this is a far cry from IT "best practices" and must change soon if large organizations expect to automate processes, pass compliance audits, and manage risk effectively.
- **Data breaches continue.** In 2009, 22% of large organizations surveyed had suffered at least one confidential data breach within the last 12 months, as compared to 56% of organizations that reported a confidential data breach incident in 2008. Does this indicate a measurable improvement? No. In spite of this improvement, ESG believes that the more broad-based publicly-disclosed breach data (i.e., from datalossdb.org) described previously suggests that year-over-year variance in ESG's data represents "the luck of the draw" rather than any real security progress. The root causes of data breaches also seem to be going through a metamorphosis. While 2008 respondents indicated that insider attacks were the primary cause of data breaches, 2009 respondents identified other root causes such as human error (53%) and external attacks (34%). In other words, data breaches may now be a function of poor database security skills, process weaknesses, and the rapidly growing threat of cybercrime. Given these multiple threat vectors, it is safe to assume that database security will grow worse—not better—in the next few years.
- **Budgetary limitations and organizational confusion continue to hinder database security and compliance efforts.** When asked to identify the biggest risks to database security, nearly half of all users pointed to budget constraints. Other issues around security knowledge, skills, poor cooperation, and disconnects between IT and the business were also called out (see Figure 4).

Figure 4. Risks To Database Security



Source: Enterprise Strategy Group, 2009.

Research Analysis

As in 2008, ESG's 2009 report on database security and compliance demonstrates that confidential data stored in relational databases remains at risk. To summarize, ESG believes that the data indicates:

1. **A false sense of security.** While large organizations tend to believe that most of their data is protected, they also suffer from continuing data breaches, face new threats, rely on manual processes, and don't have the controls in place to keep up. In contrast to many user illusions, ESG can only conclude that database security has become a weak link in the overall data security chain.
2. **Regulatory compliance remains a monumental effort.** To meet regulatory compliance mandates, large organizations are forced to rely on manual tasks and time consuming processes. This is a growing problem as enterprises increase data capacity, add new databases, and share data with external constituents. The result? Many organizations are failing compliance audits. This is especially concerning since compliance audits are often "checkbox" exercises that are only marginally effective at addressing real risks. ESG believes that this data should be a wake-up call. Large organizations must move from inefficient compliance exercises to automated risk management ASAP.
3. **Database security spending is not keeping up.** While CIOs continue to spend on security, specific database security safeguards remain underserved. This may be a result of the communications gap between IT and business executives previously described in Figure 4 or the misguided belief that database vendors provide all the integrated security needed. Regardless of the reason, ESG's data indicates that database security suffers from a lack of investment. Clearly, large organizations are spending on the wrong things in the wrong places. Dedicated tools that can help address real risks, automate processes, and streamline compliance efforts are sorely needed.

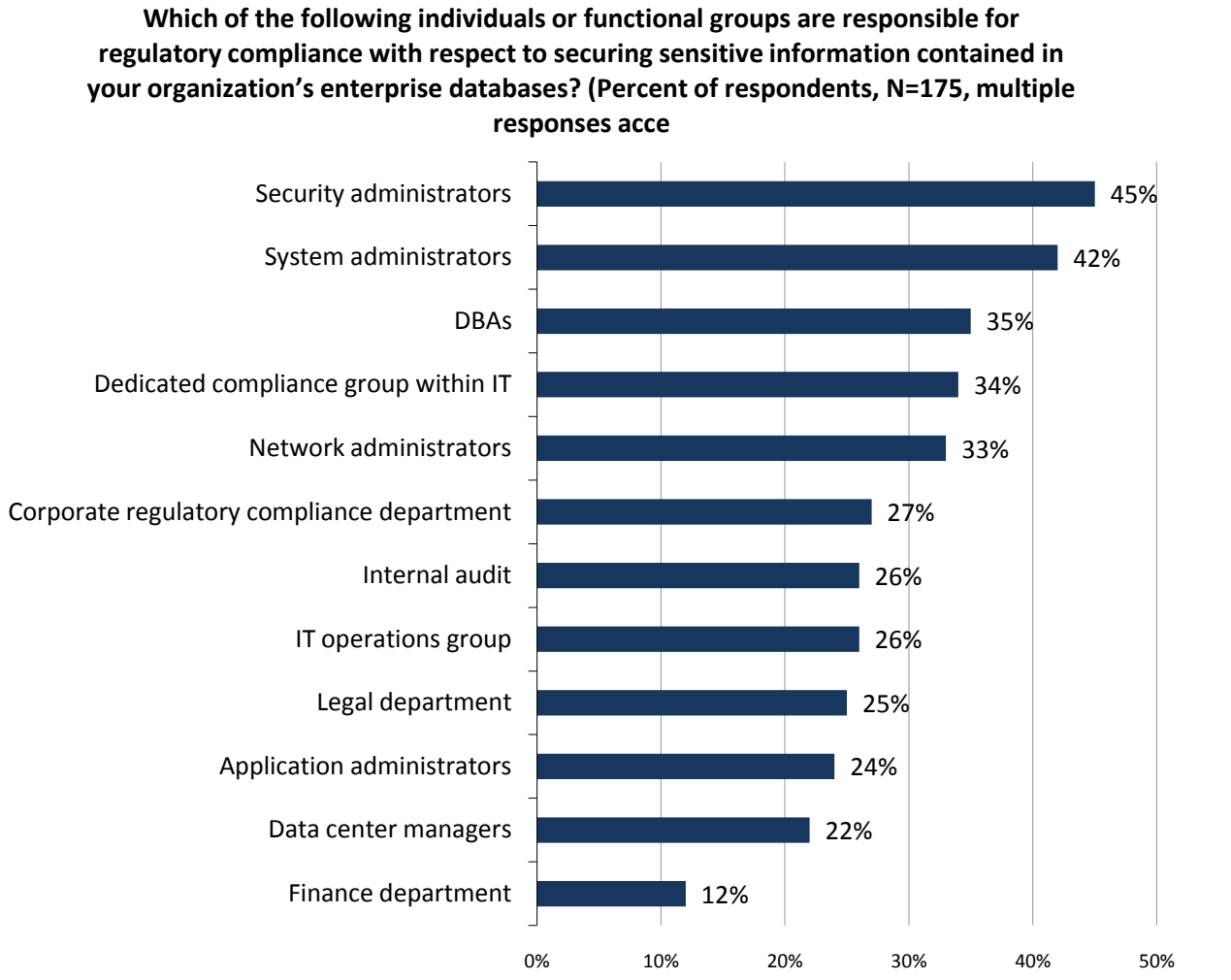
Recommendations

While ESG's data uncovers some unacceptably high database security risks, it also hints at a few priorities that could help address vulnerabilities, automate processes, and improve controls. ESG strongly suggests that CIOs and CISOs:

- **Educate business and financial executives.** The data presented herein should be used as third-party validation illustrating pervasive data security problem to business executives. When presenting this case to business executives, IT managers should highlight the following points:
  - Data breaches continue, therefore data security must remain a high priority.
  - Threats are changing and growing, therefore new countermeasures and security skills are always needed.
  - Database security shortcomings can pose regulatory compliance issues for the entire organization; security is a business and not just a technology issue.
  - Organizational problems can impede database security; therefore security leadership must come from the executive office suite.
- **Re-examine security spending priorities**. While most firms invest in security tools like firewalls, IDS/IPS, and PC security suites, they remain behind with regard to database specific security tools. ESG's data identifies several problems around database security controls, manual/time-consuming processes, and access control issues that may be related to this discrepancy. Database-specific tools can help scan for these problems, automate processes, monitor controls, and streamline audits. Given the risks uncovered in this report, CISOs may want to prioritize database security investments over other more pedestrian needs sooner rather than later.
- **Conduct a cost/benefit analysis**. Since incremental security budget dollars may be unlikely at this time, ESG recommends that CISOs use the data presented here as a basis of a cost/benefit analysis. For example, what are the costs of the time consuming processes described in Figure 3? Savings in these operations alone could cost justify an investment in a more automated technology-based approach.
- **Determine database security ownership.** Like 2008, the 2009 ESG data indicates that when it comes to database security, there are simply too many cooks in the kitchen (see Figure 5). This may explain loose

controls, process problems, and the lack of database security safeguards. ESG believes that database security oversight must become more centralized in the hands of a subset of security and database professionals with a greater understanding of threats, vulnerabilities, and risks. CIOs should assess current database security problems and then re-structure IT organizational responsibilities and accountability around security, systems administration, and database administration. Again, centralized database security tools can help ease this transition by automating processes and providing role-based management capabilities.

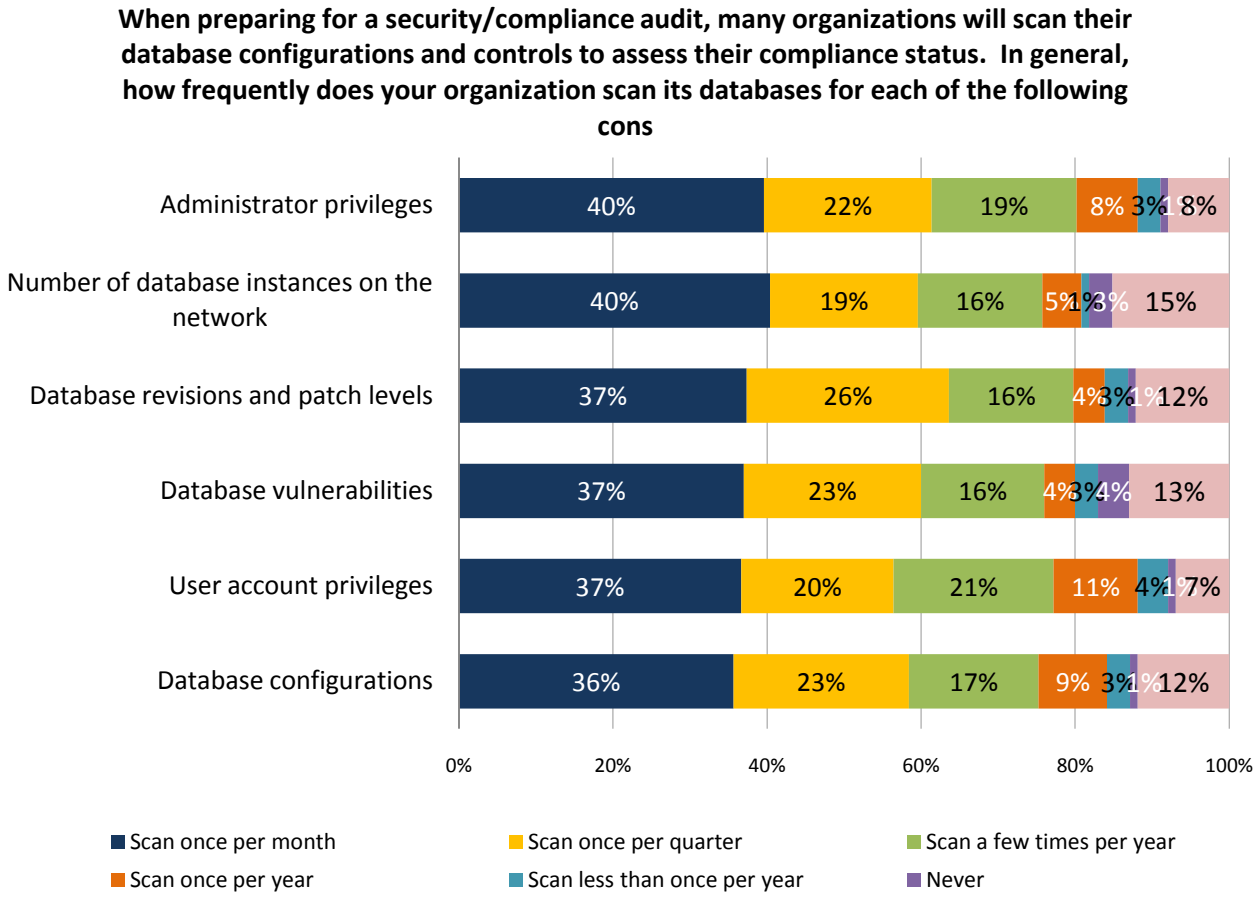
Figure 5. Too Many IT Groups are Involved in Database Security



Source: Enterprise Strategy Group, 2009.

- **Define best practices.** The data indicates a lot of variability regarding what needs to be done and how often. For example, while about 40% of organizations regularly scan their databases for things like administrator privileges, database instances, and configuration status on a monthly basis, the remaining 60% do so once per quarter or even less frequently (see Figure 6). It is safe to assume that the 40% minority have defined database security policies, procedures, and best practices that mandate these monthly database audits while others maintain informal or ad-hoc approaches. It is imperative that security, compliance, application, and database professionals reach a consensus on best practices and then religiously adhere to formal processes and schedules. Automated tools will go a long way to help achieve this goal.

Figure 6. Approximately 40% of Large Organizations Have Defined Database Security Best Practices



Source: Enterprise Strategy Group, 2009.

- **Use regulatory compliance efforts to measure success.** Create a baseline for the time and effort it takes to prepare enterprise databases for regular compliance audits. Make sure to include problems like remediating compliance issues, participating in audits, and working with the auditors outlined above. Once comfortable with these time and cost estimates, challenge the security and compliance team to figure out how to improve upon these metrics. This may also help target and cost justify database security operations investments.

Research Methodology

To gather data for this report, ESG conducted a comprehensive online survey of IT and information security professionals from private- and public- sector organizations in North America during October 2009. To qualify for this survey, respondents were required to be responsible for and/or familiar with the policies, procedures, and technologies their organization used to protect confidential information. Furthermore, qualifying respondents also had to be responsible for overseeing, implementing, and/or managing security or compliance policies, procedures, and technologies related to data stored in enterprise databases.

All respondents were provided with an incentive to complete the survey in the form of cash awards and/or cash equivalents.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on a number of criteria) for data integrity, ESG was left with a total sample of 175 IT and information security professionals.

Please see the *Respondent Demographics* section of this report for more information on these respondents.

Note: Totals in figures throughout this report may not add up to 100% due to rounding.

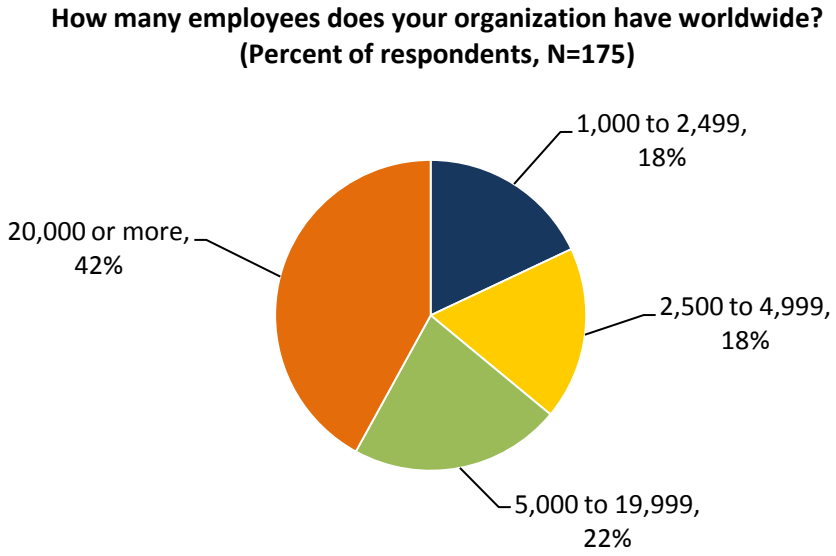
Respondent Demographics

The quantitative information presented in this report is based on 175 qualified survey respondents. The figures below detail the demographics of the respondent base.

Respondents by Number of Employees

The number of employees in respondents' organizations is shown in Figure 7.

Figure 7. Survey Respondents by Number of Employees

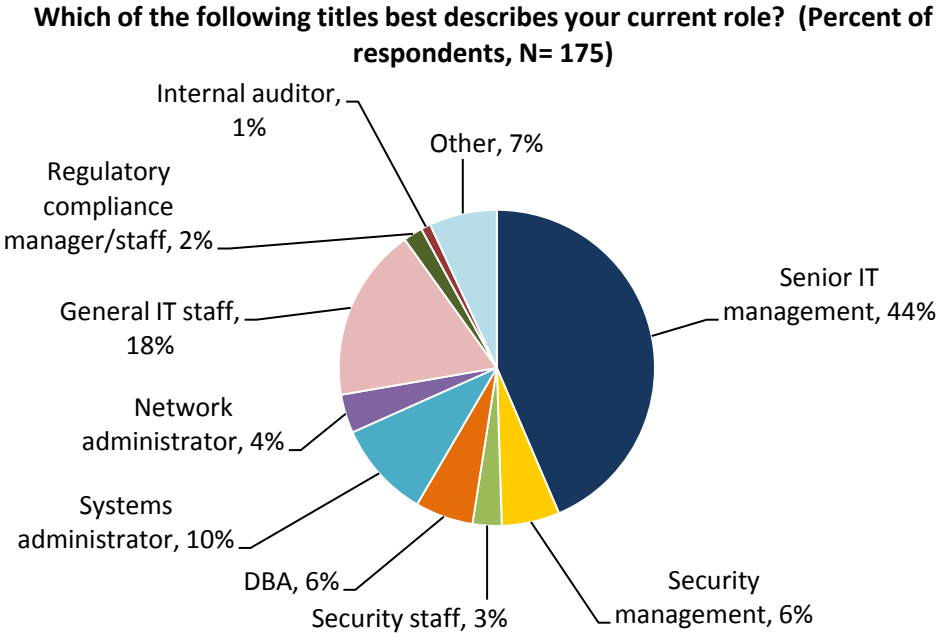


Source: Enterprise Strategy Group, 2009.

Respondents by Role

ESG asked respondents to choose one of nine titles (or "other") that best described their current role (see Figure 8).

Figure 8. Survey Respondents by Role



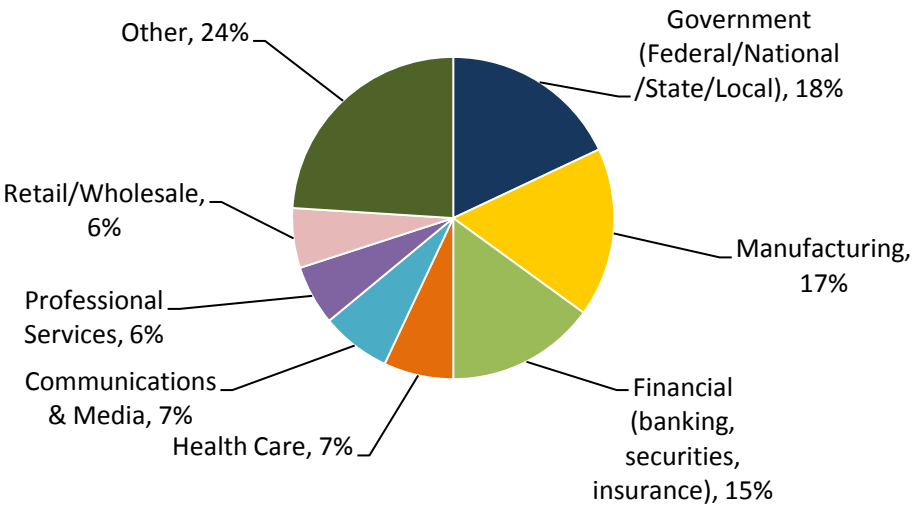
Source: Enterprise Strategy Group, 2009.

Respondents by Industry

Respondents' primary industries are shown in Figure 9.

Figure 9. Survey Respondents by Industry

What is your organization's primary industry? (Percent of respondents, N= 175)



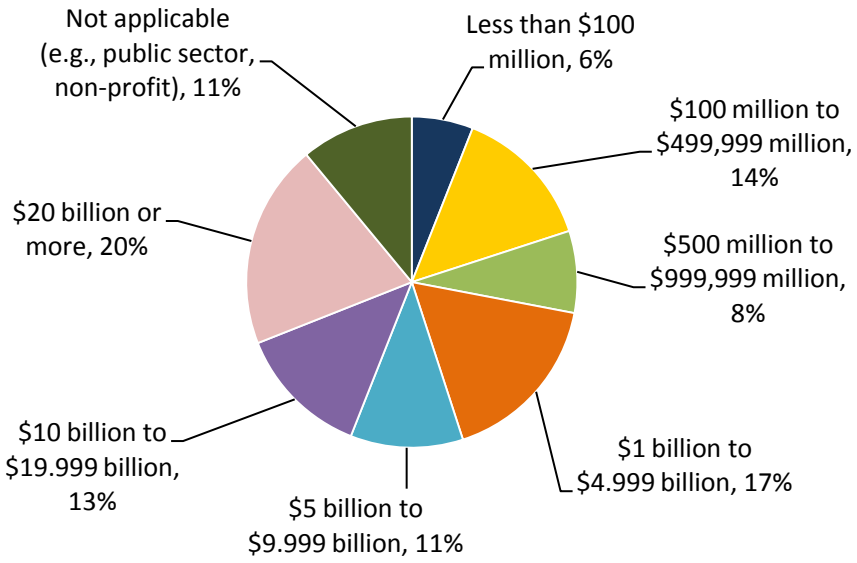
Source: Enterprise Strategy Group, 2009.

Respondents by Annual Revenue

Respondent organizations' annual revenue is shown in Figure 10.

Figure 10. Survey Respondents by Annual Revenue

What is your organization's total annual revenue ($US)? (Percent of respondents, N= 175)



Source: Enterprise Strategy Group, 2009.

Enterprise Strategy Group | **Getting to the bigger truth.**

20 Asylum Street | Milford, MA 01757 | Tel:508.482.0188 Fax: 508.482.0218 | www.enterprisestrategygroup.com