Research Brief

Databases at Risk

Date: September 2009 **Author:** Jon Oltsik, Principal Analyst

Abstract: *A recent ESG Research Brief revealed that valuable databases are often protected by an ad hoc combination of IT groups and manual processes. Clearly, these weaknesses make databases vulnerable, but are there specific types of database security threats that increase the risk of a data breach? Yes. ESG's data also points to a pattern of enterprise data breaches and identifies specific database risks concerning security professionals. The good news is that large organizations have made database security a 2009 priority, but the question remains: Is this action a case of too little, too late?*

Overview

In a recent Research Brief,[1] ESG analyzed the current state of database security. Based upon a survey of 179 North American-based security professionals working at organizations with over 1,000 employees, ESG found that:

- **Databases house a higher percentage of confidential data than any other type of data repository.** Though confidential data[2] resides throughout the network, 58% of users believe that databases contain the highest percentage of sensitive information. In fact, other types of data repositories aren't even close: For example, just 15% of respondents said that general-purpose file servers contain the largest percentage of confidential data. Other responses included Web servers (13%), e-mail servers (9%), and general-purpose endpoints like desktops, laptops, and PDAs (5%). As for databases themselves, confidential data is widespread: 43% of respondents claim that more than half of all corporate database instances contain confidential data.
- **Database security remains a cooperative effort.** When asked to identify the various groups that have responsibility for database security within their respective organizations, respondents identified a number of stakeholders. Security administrators drew the biggest percentage of responses (66%), followed closely by the IT operations group (60%), data center managers (58%), system administrators (57%), network administrators (49%), and DBAs (42%) (note: multiple responses were accepted from respondents). Given the fact that no one group seems to "own" database security, ESG concludes that database security is performed "by committee" in a loose confederation. This is not a recipe for strong database security.
- **Database security depends upon too many manual processes.** Like any other IT operations activity, database security depends upon a combination of manual processes and automated tools. In an area as complex, dynamic, and dangerous as database security, process automation is imperative in order to keep up with threats, minimize error-prone hands-on tasks, and maintain an audit trail of all security-related activities. Unfortunately, most organizations are far from this type of model. Sixty-three percent of respondents claim that their organization's database security depends exclusively upon manual processes, is based upon some automated tools but mostly manual processes, or is made up of a combination of automated tools supported by a large number of manual processes. This reliance on manual processes can't scale to meet the volume and sophistication of today's threats.

[1] Source: ESG Research Brief, *Frightening Database Security Realities*, August 2009.

[2] For the purposes of this survey, confidential data was 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

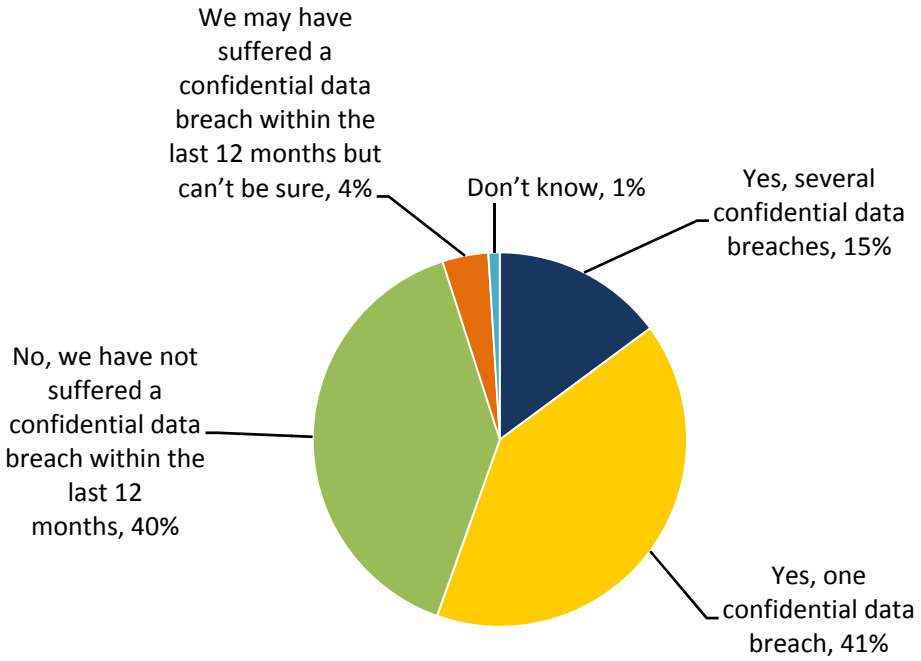
- **Enterprise-class organizations aren't diligent enough about database security.** Assessing the security of multiple revisions of heterogeneous distributed databases should be done on a frequent basis, but ESG's research finds that this is not always the case. Only 27% of organizations claim that they assess their database security technologies and controls on a monthly basis, while 39% do so twice a year or less. Infrequent database assessment can expose sensitive databases to unnecessary software vulnerabilities, mis-configurations, and other types of problems that increase risk.

Is Confidential Data at Risk?

With databases acting as the main repository for confidential data, securing those assets should be part of a comprehensive security strategy for end-to-end confidential data protection. An effective confidential data security strategy would therefore result in few if any data breaches. Unfortunately, this is not the case. ESG's data paints a rather gloomy picture: Confidential data breaches are an all-too often occurrence. An alarming 56% of large organizations surveyed say they suffered data breaches over the past 12 months, with 15% experiencing multiple data breaches and 40% claiming to have a single data breach (see Figure 1).

Figure 1. Large Organizations are Experiencing Data Breaches

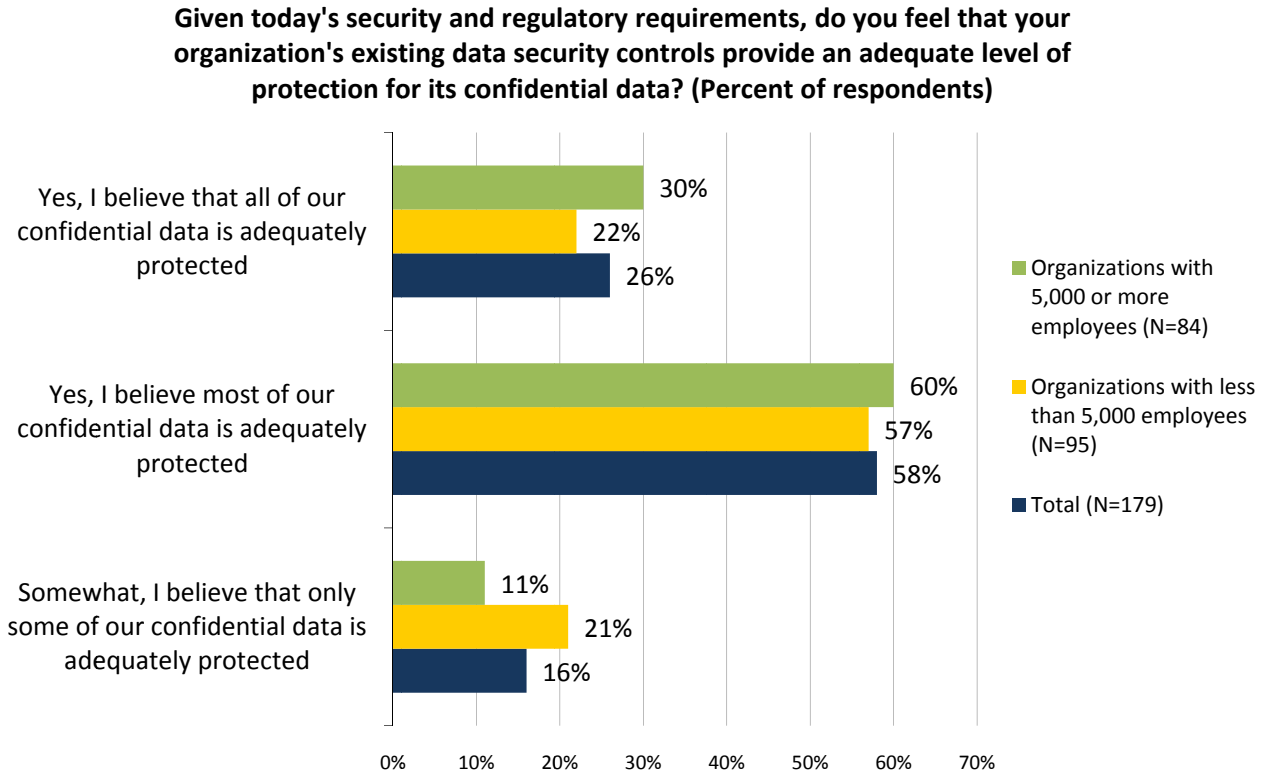
To the best of your knowledge, has your organization suffered a confidential data breach within the last 12 months? (Percent of respondents, N=179)



Source: Enterprise Strategy Group, 2009.

Why is this situation so dire? The data seems to indicate a pattern of fundamental issues with existing security controls. When ESG asked security professionals whether their organization's security controls provide adequate protection for confidential data, only 26% were confident that all of their confidential data was protected, while an alarming 16% of organizations believed that only some of their confidential data was adequately protected (see Figure 2). These shortcomings are magnified based on company size since security control weaknesses are more apparent in smaller organizations (e.g., those with less than 5,000 employees).

Figure 2. Existing Security Controls do not Provide Adequate Protection, by Company Size



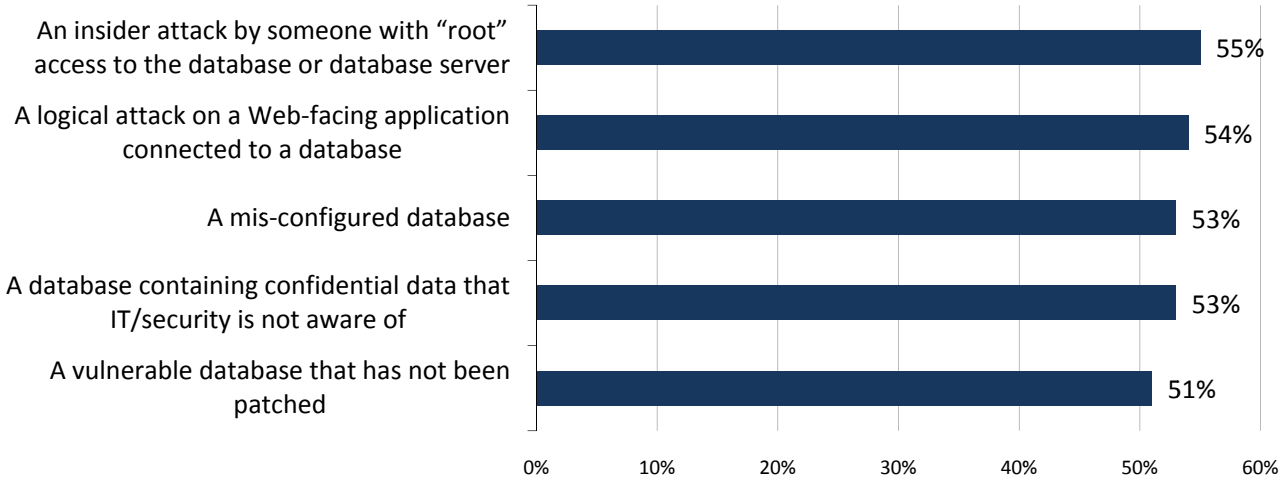
Source: Enterprise Strategy Group, 2009.

Database Risks Abound

The data presented above describes a pattern of controls weaknesses and confidential data breaches throughout the enterprise. What about specific risks with regard to database security? ESG's research finds that these are also ominous and prevalent—more than half of security professionals surveyed say they are concerned about several types of database security risks, including an insider attack by administrators with "root" access; a logical application layer attack; and an unknown, un-patched, or mis-configured database instance (see Figure 3). ESG believes these risks are exacerbated by the vulnerabilities and informal processes described above. After all, if multiple groups collaborate on database security, there will be more IT administrators with "root" access and more opportunities for mis-configuration errors. Likewise, if database security assessments are a rarity, it is less likely that anyone will notice anomalous system behavior or identify an un-patched system.

Figure 3. Database Security Risks

Which of the following types of database security risks are of greatest concern to your organization? (Percent of respondents, N=179, multiple responses accepted)

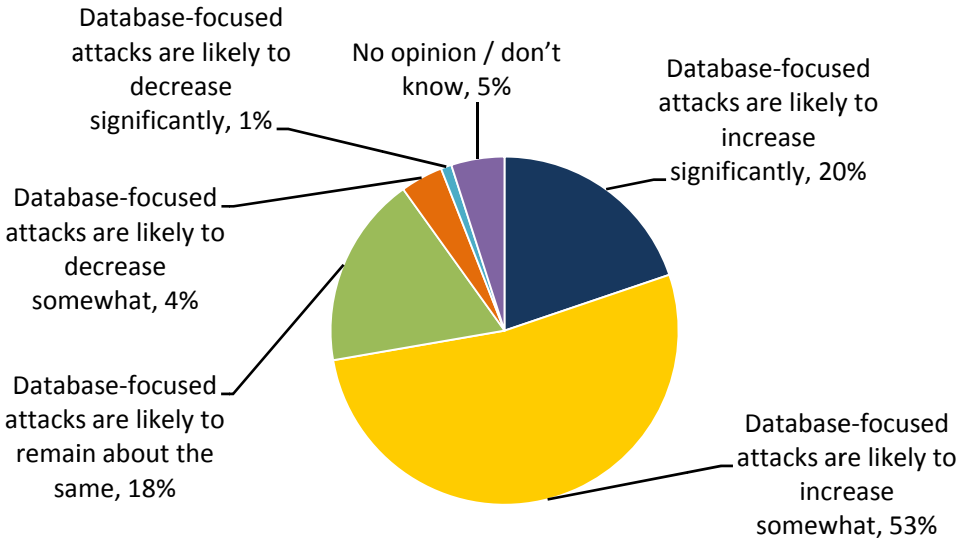


Source: Enterprise Strategy Group, 2009.

Since databases contain valuable data, it is safe to assume that they present an attractive target for cyber criminals. The security professionals surveyed by ESG concur with this hypothesis. Given the general increase in sophisticated and targeted cyber attacks, nearly three-quarters of security professionals anticipate that the volume of database security attacks will continue to increase through 2009 and beyond (see Figure 4).

Figure 4. Security Professionals Anticipate More Database Security Attacks

In your opinion, which of the following is most likely in terms of the number of database-focused attacks in 2009 and beyond? (Percent of respondents, N=179)



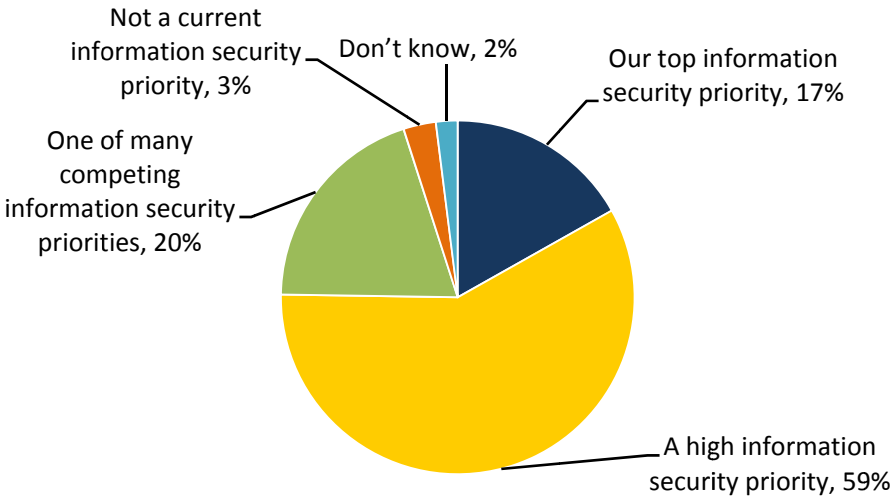
Source: Enterprise Strategy Group, 2009.

The Good News: Database Security is a High Priority

Based upon the data presented in this series of research briefs, ESG concludes that database security is too often neglected or poorly managed, leading to an increased risk of an accidental or malicious data breach. Fortunately, security professionals and large organizations seem to share this opinion. A significant majority of organizations (76%) will make database security their top priority or a high priority throughout the next year (see Figure 5).

Figure 5. Database Security is a High Priority

How would you rank the importance of further improving your organization's database security controls over the next 12 months? (Percent of respondents, N=179)



Source: Enterprise Strategy Group, 2009.

The prioritization of database security leaves ESG cautiously optimistic. Clearly, CSOs (Chief Security Officers) recognize an unacceptably high level of risk and are dedicating resources to close these gaps. The question remains, however: Will remediation activities be enough? Is there still time? Database security appears to be a race between corrective enterprise actions and intelligent and highly-motivated cyber criminals. Large organizations have no time to waste. Proactive firms may gain an advantage while laggards will face additional risks and threats on a daily basis.

Research Implications

ESG's research points to a dangerous and growing security gap. Undoubtedly, databases contain a high percentage of confidential data, yet security controls seem to be a group effort based upon manual processes and infrequent security assessments. This seems especially misguided given the current climate of data breaches, databases risks, and the prospect of more frequent and destructive database attacks predicted by the majority of survey respondents.

The good news is ESG's data foretells that database security changes are rapidly approaching. Most organizations view database security as a top priority and will thus invest in skills, services, and technology safeguards to enhance current security controls.

In order to improve database security across the enterprise, large organizations should:

- **Start with a full database inventory.** It's important to know everything about database assets before implementing tactical safeguards. How many databases are on the network? What type of data do they house? What types of databases are installed? Which revisions? Which patch levels? Which administrators have root access? Don't just assume that you know this information. Scan the network for rogue databases, query the IT staff, and look at network log data to get as accurate a picture as possible.

- **Define policies and best practices.** What types of database security controls, processes, and skills would you opt for if you had unlimited resources? Start with this idea and work backward to achieve a more realistic model.
- **Take an enterprise approach.** While the data on any one database may belong to a single business unit or process, database security benefits can improve across the enterprise with uniform controls and tools. Don't let politics get in the way.
- **Streamline and structure database security.** There are simply too many people with a hand in database security. Policies and procedures need clear and formal guidelines based upon best practice models like COSO, ITIL, and the NIST-800 series. Additionally, database security ownership and accountability must rest with a few highly skilled security professionals rather than with a plethora of IT administrators.
- **Look for integrated specific database security tools.** Database security requirements go beyond basic safeguards offered from IDS/IPS, firewalls, SIM, and identity management tools. Look for database security tools that provide a suite composed of database discovery, vulnerability scanning, penetration testing, user monitoring, logging, encryption, and policy-based enforcement. Use these tools to automate today's error prone manual processes and homegrown scripts.

Given the state of database security, these preliminary steps should be supported by a detailed database security project and undertaken as soon as possible.

This ESG Research Brief is Compliments of Guardium

About Guardium.

Guardium, the database security company, delivers the most widely-used solution for preventing information leaks from the data center and ensuring the integrity of enterprise data.

The company's enterprise security platform is now installed in more than 450 data centers worldwide, including 5 of the top 5 banks; 3 of the top 5 insurers; top government agencies; 2 of the top 3 retailers; 15 of the world's top telcos; 2 of the world's favorite beverage brands; the most recognized name in PCs; a top 3 auto maker; a top 3 aerospace company; and a leading supplier of business intelligence software.

Guardium has partnerships with Accenture, ArcSight, BMC, EMC/RSA, IBM, McAfee, Microsoft, Oracle, Sybase and Teradata, with Cisco as a strategic investor, and is a member of IBM's prestigious Data Governance Council and the PCI Security Standards Council.

Founded in 2002, Guardium was the first company to address the core data security gap by delivering a scalable, cross-DBMS enterprise platform that both protects databases in real-time and automates the entire compliance auditing process.

For more information contact:

Guardium®
SAFEGUARDING DATABASES™

Guardium
230 Third Avenue
Waltham, MA 02451

Tel: +781.487.9400
info@guardium.com
www.guardium.com