



RESEARCH REPORT

Database Security Controls

By Jon Oltsik

November 2008

Executive Summary

Summary of Report Conclusions

In October 2008, the Enterprise Strategy Group (ESG) conducted a comprehensive survey of 179 North American IT decision-makers from enterprise-class organizations (defined as those with 1,000 or more employees) regarding their database security policies, experiences, and strategies on behalf of Application Security, Inc. Based upon this research, ESG concludes that there are a large number of independent risks to confidential information¹ stored in databases and that many large organizations remain extremely vulnerable to compliance audit failures and data breaches. In many cases, users recognize these security weaknesses, but lack the funding, senior management support, and security skills to address these vulnerabilities adequately.

In total, ESG's data exposes a significant security risk to large organizations, which could have a ripple effect on society at large. Corporate database security weaknesses leave the data of hundreds of millions of people vulnerable to a data breach. As data breach events continue, legislators will feel compelled to pass tighter privacy regulations with more defined guidelines and stiffer penalties. As of this writing, 42 U.S. states have passed their own independent privacy laws. Massachusetts and Nevada laws included stipulations for data encryption while Michigan and Washington State are expected to ratify encryption laws in 2009. There are also several privacy bill proposals in the U.S. Senate and House of Representatives. Clearly, legislators at the state and federal level will mandate tighter confidential data controls if users don't improve them on a voluntary basis.

Report Conclusions

Based on the data in this survey, ESG concludes that:

- **Data breaches are becoming more commonplace.** ESG asked respondents if their organization had suffered a confidential data breach within the past 12 months. This is not an unusual question; in fact, ESG has posed a similar question in several previous research projects. Past data was fairly consistent—on average, about one-third of organizations suffered a data breach in the past year. Alarmingly, the data from this current survey was much higher: 15% of respondents said that their organization suffered “several confidential data breaches,” while another 41% claimed that their organization had suffered “one confidential data breach.” While it is impossible to draw statistically valid conclusions across random sample sets, the data does correspond with greater volume and sophistication of security attacks over the past few years. These ominous trends may be driving an increase in data breach activity.
- **An alarming number of enterprise-class organizations admit to failing a compliance audit.** Common wisdom suggests that regulatory compliance has become relatively easy for large organizations, but ESG's data illustrates that the opposite is true. Over the past 3 years, 38% of respondents say that their organization has failed a security or compliance audit “one time” or “multiple times.”
- **Databases house a higher percentage of confidential data than any other type of data repository.** While confidential data resides throughout the network, 58% of users believe that databases contain the highest percentage. In fact, other types of data repositories aren't even close: 15% of respondents said that general-purpose file servers contain the largest percentage of confidential data, 13% said that Web

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

servers contain the largest percentage of confidential data, 9% said that e-mail servers contain the largest percentage of confidential data, and 5% said that general-purpose endpoints like desktops, laptops, and PDAs contain the largest percentage of confidential data. As for databases themselves, it appears that confidential data is widespread as 43% of respondents claim that more than half of all corporate databases contain confidential data.

- **Database security remains a cooperative effort.** When asked to define which groups are responsible for database security, respondents identified a number of suspects. 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%). 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.
- **Enterprise-class organizations face a variety of database security risks.** When asked to define the database security risks of most concern to their organization, survey respondents presented a laundry list of equally threatening issues. The five types of risks selected most were:
 - An insider attack by someone with “root” access to the database or database server (55%)
 - A database containing confidential data that IT/security is not aware of (53%)
 - A logical attack on a Web-facing application connected to a database (54%)
 - A mis-configured database (53%)
 - A vulnerable database that has not been patched (51%)

With this wide variety of database security risks present, ESG believes that users can only protect their database assets with a combination of formal policies, separation-of-duties, frequent penetration testing, and comprehensive technology controls.

- **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 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 upon manual processes alone, some automated tools but mostly manual processes, or a combination of automated tools supported by a large number of manual processes. In the ongoing race to stay one step ahead of vulnerabilities and would-be attackers, this is a recipe for disaster.
- **Enterprise-class organizations aren’t diligent enough about database security.** Assessing the security of multiple revisions of ever-changing heterogeneous distributed databases should be done on a frequent basis, but the data demonstrates 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. This frequency opens sensitive databases to unnecessary software vulnerabilities, mis-configurations, and other types of risks.
- **Most users believe that database-focused attacks are on the rise.** Nearly three-quarters (73%) of respondents believe that database-focused attacks will “increase significantly” or “increase somewhat” in 2009 and beyond.
- **Database security is a top security priority.** The combination of less-than-adequate database security controls and a future of more direct attacks seem to be motivating users toward action. Most organizations seem to recognize how important database security is moving forward. Seventy-six percent of respondents say that improving their organization’s database security controls is “our top information security priority” or “a high information security priority” over the next 12 months.

- **Database security can be challenged by IT budget constraints.** Why wouldn't organizations invest in database security controls and technologies? When asked to identify the biggest inhibiting factors preventing database security improvements, respondents identified "lack of budget" (40%) as the major bottleneck. Other issues included "lack of senior management sponsorship" (21%), "we do not have an accurate inventory of our enterprise databases" (21%), and "we aren't sure what types of database security technologies and controls we need" (21%). While there seems to be a general lack of knowledge around database security priorities and best practices, ESG remains concerned when database security is disregarded due to monetary constraints. Given the high percentage of confidential data contained in these database repositories, database security should leapfrog other security initiatives as a budget priority.

Research Analysis

ESG's data points to a dangerous and growing security gap. Clearly, 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 variety of risks to databases and the increasing frequency of attacks predicted by the majority of survey respondents. Little wonder why data breaches seem to be on the rise while organizations struggle to meet security and compliance mandates.

The data foretells that change approaching. Most organizations view database security as a top priority in 2009 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 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.
- **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.



20 Asylum Street
Milford, MA 01757
Tel: 508-482-0188
Fax: 508-482-0218

www.enterprisestrategygroup.com