

September 28, 2009

# Your Enterprise Database Security Strategy 2010

by Noel Yuhanna

for Application Development & Program Management Professionals



September 28, 2009

## Your Enterprise Database Security Strategy 2010

Stronger Measures Have Become Essential To Defend Against Growing Attacks

by Noel Yuhanna

with Mike Gilpin and Adam Knoll

### EXECUTIVE SUMMARY

With increasingly sophisticated attacks and rising internal data theft, database security merits a stronger focus that goes beyond traditional authentication, authorization, and access control (AAA). A single intrusion that compromises private data such as credit card numbers, social security numbers, or other financial data can cause immense damage to an enterprise's reputation, not to mention initiating lawsuits and regulatory fines that can have long-term impact. Database security is the last line of defense, so it deserves greater focus on the protection of private data from both internal and external attacks than IT pros have traditionally given it. Database security professionals and information security and risk management professionals crafting a security strategy should: 1) align database security policies with information security policies; 2) ensure well-defined and formalized database security procedures; 3) enforce role separation; and 4) apply advanced security measures such as database auditing, monitoring, database encryption, data masking, and vulnerability assessment to all critical databases that store private data.

### TABLE OF CONTENTS

#### 2 Databases Need Tighter Security To Protect Against Threats

Basic Database Security Measures Are No Longer Sufficient To Protect Private Data

#### 2 Enterprises Must Establish A Comprehensive Database Security Strategy

Discovery, Classification, Database AAA, And Patch Management Provide The Foundation

Preventive Measures Build On Top Of The Foundation, Offering Added Layers Of Protection

Detecting Anomalies And Performing Routine Security Checks Completes Your Strategy

#### 7 Don't Forget Security Policies, Standards, Role Separation, And Availability

#### RECOMMENDATIONS

#### 8 All Enterprises Need A Database Security Strategy

### NOTES & RESOURCES

Forrester interviewed 17 vendor and user companies, including IBM, Microsoft, Oracle, and Sybase.

#### Related Research Documents

["The Forrester Wave™: Enterprise Database Management Systems, Q2 2009"](#)

June 30, 2009

["Market Overview: Database Security"](#)

February 27, 2009

## DATABASES NEED TIGHTER SECURITY TO PROTECT AGAINST THREATS

Today, all enterprises use database management system (DBMS) technology to store critical business data. All data is important, but private data matters most. A single intrusion that compromises private data such as credit card numbers or financial data can cause immense damage to an organization, whether big or small. Databases are often the prime target of such attacks, largely because they hold the most-valuable data and are vulnerable unless carefully secured. Recently, in the largest data theft in US history, a Florida man pleaded guilty to stealing more than 170 million credit and debit card account numbers from large retailers such as Sports Authority, OfficeMax, and Barnes & Noble.<sup>1</sup> He used various techniques including SQL injection to locate and crack into databases after he identified security holes. More recently, Network Solutions made headlines when it disclosed that hackers planted rogue code that resulted in compromising more than 573,000 debit and credit card accounts. Hackers will find new ways to break into databases; therefore, enterprises need to be more vigilant and take proactive measures to safeguard their data.

## Basic Database Security Measures Are No Longer Sufficient To Protect Private Data

Although many enterprises employ basic database security measures such as authentication, authorization, and access control to secure critical databases, the growing number and sophistication of attacks means that these measures alone are no longer good enough to protect private data. Today, many database attacks occur without warning or enterprises even being aware that an attack took place. Forrester recently interviewed a large retail firm's database administrator (DBA) who claimed that someone broke into the company's critical database system and stole private data and that the breach went undiscovered for 45 days. All databases can be vulnerable, even those that implement advanced security measures, but soft targets are often the first to fall victim to attack.<sup>2</sup> Internal threats — which can be difficult to detect — remain at an all-time high.<sup>3</sup>

According to the Forrester Research/TechTarget November 2008 Global Database Management Online Survey, 90% of respondents claimed that database security features are important when choosing a DBMS. In this survey, 58% of respondents indicated that securing private data in databases was challenging.<sup>4</sup> Interestingly, compared with Forrester's July 2005 Data Management Online Survey, this percentage did not decline during the three years between the surveys, as challenges and demands for improved database security are continuously changing. In addition, according to the 2008 survey, only 21% of enterprises are pursuing advanced security measures, while the others remain soft targets for hackers.

## ENTERPRISES MUST ESTABLISH A COMPREHENSIVE DATABASE SECURITY STRATEGY

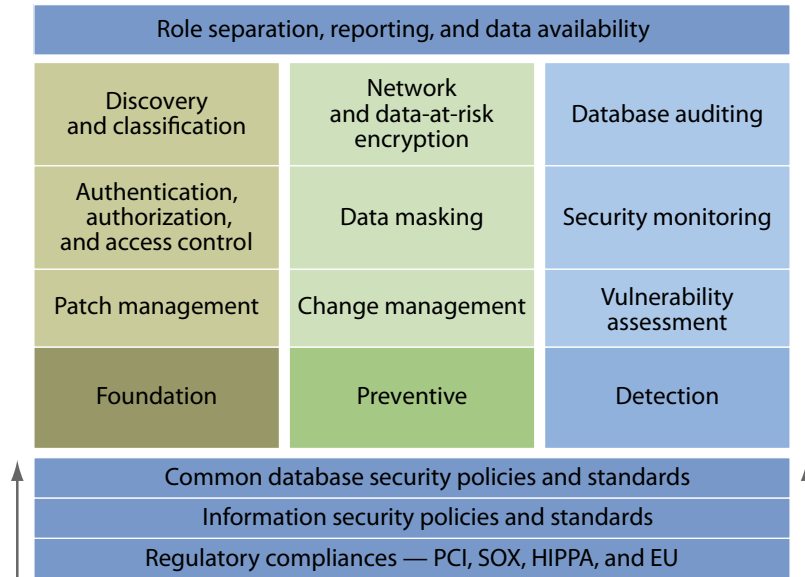
The key to any successful database security strategy is knowing why you're protecting each database, which databases to protect, and how best to secure data against all types of threats. To develop your database strategy, you should: 1) understand applicable regulatory compliance standards such as Sarbanes-Oxley (SOX), Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPAA), and European Union (EU) regulations as well as what data needs to be protected, such as credit card numbers, financial data, employee data, engineering data, and

personnel information; 2) inventory all databases including those for nonproduction uses such as testing, development, and training; 3) discover and classify these databases into highly sensitive, sensitive, and nonsensitive categories; 4) establish common policies for the databases in each of these categories; 5) integrate database security with your overall information security framework; and 6) where appropriate, take advanced security measures such as encryption, masking, auditing, and monitoring.

Build your comprehensive database security strategy on three pillars (see Figure 1):

- **Build a strong foundation with AAA, discovery and classification, and patch management.**  
Understanding which databases contain sensitive data is a fundamental requirement for any database security strategy. Enterprises should take a complete and ongoing inventory of all databases, including production and nonproduction, and classify them into categories that should observe the same security policies. All databases, especially ones that hold private data, should have strong AAA, even if the application tier does authentication and authorization. The lack of a strong AAA foundation weakens other security measures such as auditing, monitoring, and encryption. In addition, database security professionals should patch all critical databases on a regular basis to eliminate known vulnerabilities.
- **Take preventive measures with encryption, data masking, and change management.**  
Preventive security is desirable for all databases but essential for those that hold sensitive data. The goal is to prevent unauthorized access to and exposure of confidential data. Preventative security measures include: 1) using network and data-at-rest encryption to prevent data exposure to prying eyes, including those on internal networks; 2) masking private data in nonproduction databases such as those for testing, development, and training to prevent data exposure to privileged users such as testers, developers, and outsourcing vendors; and 3) requiring changes to schema structures made as part of application development to follow formal procedures that ensure that only approved changes are allowed into production.
- **Establish intrusion detection with auditing, monitoring, and vulnerability assessment.**  
Whenever critical data changes unexpectedly or suspicious data access activity takes place, it is critical that the organization launches a quick investigation to determine what happened. Database auditing provides the ability to answer tough questions such as “who changed what data?” and “when was it changed?” In addition, database security monitoring provides real-time alerting and protection, which is essential to defend against sophisticated attacks. Finally, a vulnerability assessment reports security gaps in the database environment, such as weak passwords or excessive access privileges, supplementing DBA and security group monitoring.

**Figure 1** Three Pillars Of Enterprise Database Security



55357

Source: Forrester Research, Inc.

**Discovery, Classification, Database AAA, And Patch Management Provide The Foundation**

Without a strong database security foundation, other security measures are less effective. All DBMSes come with AAA capabilities that secure the basic functions that store, retrieve, and update data, and organizations should leverage these capabilities as much as possible. Regardless of the type of application, AAA remains critical to ensure that only authorized users, including programmatic interfaces and automated processes, have access to private data. To establish a strong database security foundation, organizations should use:

- **Database discovery and classification as a starting point.** Most large enterprises today have hundreds or thousands of databases to support their business. Some have as many as 15,000 production databases, a volume that often creates a major security challenge, especially if a large number of these databases contain sensitive data. Some enterprises only implement advanced security measures on databases that are visible to auditors, leaving other databases vulnerable to attacks. Many large enterprises find it very challenging to keep track of how many databases exist and which production and nonproduction databases, tables, and columns contain sensitive data. This is even more problematic when supporting legacy applications with little or no database documentation, leaving DBAs and security personnel unsure of which columns or tables they should secure.

- **Authentication and authorization to control database access.** Authentication is the process of verifying the user's identity. A database identity can be linked to an LDAP directory or to Microsoft's Active Directory so that users do not have to enter their credentials again if they have already been authenticated. DBAs should check all login names used in databases on a regular basis to ensure that only authorized users exist, disabling those that are not in use. Ideally, to enforce role separation, a group other than DBAs should create user logins. Even if an application performs authentication and authorization, DBAs should protect databases by ensuring that only active user accounts exist in each database. In addition, DBAs should not use the DBA user account as a default, but only when necessary; organizations should give DBAs individual accounts and have their activity tracked by security and risk management professionals, just like other users.
- **Access control to nail down access to private data.** Access control ensures that only authorized personnel have access to information and have the ability to change or delete data. DBAs should create roles that group users together according to their security privileges and govern them by assigning appropriate privileges to each role. Web-based applications that use a generic administrator-level database identity to gain access to data in databases pose a security threat and should be monitored regularly or changed to user-level security if possible. Otherwise, the growing number of SQL injection attacks will mean an increased risk of exposure of private data and even database corruption, as such applications execute SQL commands on databases at administrator-level privilege.
- **Advanced access control to track usage of privileged users.** Beyond traditional data access control, enterprises should also take advanced security access control measures to protect data from privileged users such as administrators, developers, testers, and architects. In addition, organizations should segregate duties to ensure that no privileged user has complete access to private data, and they should enable multifactor-policy-based authorization wherever possible. Security and risk management professionals should track DBA and other privileged user activity.
- **Patch management to protect against vulnerabilities.** All DBMS products are vulnerable and often release security patches quarterly or as needed as the vendor discovers vulnerabilities. Failing to apply all current security patches weakens all other security measures and procedures. All enterprises should apply patches on a regular basis, but only after testing affected database applications for issues. Security and risk management professionals should also track security-related DBMS patches and notify DBAs of their likely impact on security.

### Preventive Measures Build On Top Of The Foundation, Offering Added Layers Of Protection

After establishing a good database security foundation, you should take preventive measures to secure critical databases. These preventive measures provide an added layer of protection for production and nonproduction databases, ensuring that you have protected private data from all unauthorized users, including hackers. Preventive measures include:

- **Database encryption to protect production databases.** Encryption is the process of transforming data by using an encryption algorithm to make it unreadable. You can implement database encryption in two different layers: 1) at the network layer, which secures data packets in motion between the database and other nodes, such as users or applications, protecting private data against prying eyes that might be snooping on network traffic, and 2) data-at-rest encryption, which focuses on data stored in the database. As they address different threats, these encryption approaches can be implemented independent of each other. Usually, neither has an impact on application functionality. Unlike network encryption, data-at-rest encryption has several implementation options, including column-level, tablespace-level, page-level, and file-level. Data-at-rest encryption keeps anyone who has access to the underlying operating system file from viewing the data, as DBMSes typically store data in clear text.
- **Data masking to protect data in nonproduction databases.** Using or copying customer, employee, or company confidential data from production databases to develop or test applications violates data privacy laws and regulations. Data privacy does not stop with production systems; it needs to extend to nonproduction environments too, including testing, development, quality assurance (QA), staging, and training instances — wherever private data could reside. Database security professionals should evaluate the use of data masking and test data generation to protect private data in test environments or when outsourcing application development.<sup>5</sup>
- **Change management procedures to protect critical database structures.** Most databases undergo schema changes on a regular basis to support application and business requirements. In the past, schema or other database changes in the production environment required a database shutdown, but newer DBMS releases are now allowing many such changes while the database is online, creating a new security risk. Database security professionals should follow a formalized change management procedure to ensure that administrators change production databases only after approval from management and that they track all changes. In addition, organizations should update their recovery and availability plans to deal with the new contingency of corruption to data or metadata that such changes bring.

### Detecting Anomalies And Performing Routine Security Checks Completes Your Strategy

Checking databases regularly for data and activity anomalies is a critical component of a comprehensive database security strategy. Data and metadata in databases can be accessed, changed, or even deleted in a matter of seconds. To support regulatory compliance standards such as PCI, HIPAA, SOX, and EU, security and risk management professionals should track all access

and changes to private data such as credit card numbers, social security numbers, and names and addresses for critical databases. If private data was changed or accessed without appropriate authorization, organizations should hold someone accountable. Detection layer security includes:

- **Database compliance auditing and alerting on data anomalies.** Although database auditing has been around for decades, its importance was not as great until recently. Auditing checks and reports any access to, updates to, and deletions of data. It produces an audit trail that is essential to comply with regulations such as SOX, PCI, and HIPAA. Auditing helps answer questions such as “Who changed sales data?” “Who accessed credit card numbers?” and “Why was that sales transaction value changed after delivery of goods?” These are typical questions essential to support any regulatory compliance requirement. Not all databases need auditing; therefore, security and risk management professionals should only enable auditing for selective databases. The issue of auditing taking significant system overhead has diminished over the years thanks to innovation from DBMS and third-party vendor solutions. Today, many enterprises perform extensive database auditing with a system overhead of less than 10%.
- **Security monitoring and protection defending against real-time attacks.** Database monitoring and real-time protection checks for suspicious activities and alerts database security professionals and security and risk management professionals when they occur. Database monitoring proactively protects against attacks on databases. Often, large, critical databases have hundreds or even thousands of connections per second, so it is humanly impossible to view and detect security anomalies.<sup>6</sup> Security monitoring and protection not only alerts DBAs but also blocks connections in real time.
- **Vulnerability assessment checking for the integrity and configuration of databases.** Simply installing DBMS software does not create a secure environment, even if the software comes from a leading DBMS vendor. Database security professionals must harden the environment by defining user accounts (rather than using default accounts), ensuring database-file protection, enabling enforcement of access control, and installing security patches on a regular basis. Database vulnerability assessments look for security holes in database implementations that result from failing to follow security procedures correctly and highlight issues that need attention. For example, an assessment will highlight weak passwords as well as tables that have excessive privileges.

## DON'T FORGET SECURITY POLICIES, STANDARDS, ROLE SEPARATION, AND AVAILABILITY

Database security strategy is not just about auditing and monitoring; it's an end-to-end strategy that focuses on minimizing risk, meeting regulatory compliance requirements, and defending against internal and external attacks. Database security needs a broader focus that fills security gaps, works with common policies, and formalizes security approaches. Database security strategy must:

- **Integrate with overall information security policies.** Security policies are critical for any successful database security strategy. Security and risk management professionals should understand overall information security policies and use them as the basis of all database security policies. In addition, they should prioritize database security solutions that come with an extensive set of policies, especially customizable ones, as these can help reduce effort and cost. They should also consider deploying different policies for databases that hold private data than for ones that don't. In addition, they should integrate the database security solution with the help desk ticketing system to support compliance initiatives.
- **Focus on security standards.** Standards are very important when developing a database security strategy. Security and risk professions should look at industry standards such as Control Objectives for Information and Related Technology (COBIT) and Information Technology Infrastructure Library (ITIL) to help define strategy. They should modify these standards to serve their organization's needs, taking into account the impact of compliance with various standards such as SOX, HIPAA, Gramm-Leach-Bliley Act (GLBA), and PCI as well as their organization's existing applications and infrastructure. In addition, organizations should define their own standards and deploy them throughout the organization.
- **Implement role separation.** Regulatory compliance and auditors stress the importance of role separation, whereby different personnel manage databases than those who audit or monitor security activity. Forrester estimates that DBAs spend less than 5% of their time on database security, which creates a security threat unless the organization implements role separation. Typically, security professionals monitor DBAs' and other privileged users' activity, review database audit logs, and create logins. Security professionals should staff the database security analyst role that overlooks database security strategy including policies, standards, and operations.<sup>7</sup>
- **Ensure data and database availability.** Security and risk management professionals should plan for contingencies and clearly articulate in the database security strategy recovery and data availability procedures should a database goes down because of an attack. Steps should include how to recover databases, what servers and systems to use to ensure availability for affected applications, and how to ensure that hackers will not pose a threat to the recovered databases.

## RECOMMENDATIONS

### ALL ENTERPRISES NEED A DATABASE SECURITY STRATEGY

Database security professionals should not skimp when it comes to securing databases. Database security is the last line of defense; therefore, organizations should focus on it to ensure protection from attacks. With the evolution of database security threats and related security capabilities in recent years, enterprises should revisit their database security strategy and look for opportunities

to apply new security features and functionality such as encryption, auditing, masking, vulnerability assessment, and monitoring to help protect databases against new threats. An organization's database security strategy should:

- **Protect all critical databases.** Don't just focus on one or two critical databases, but on all databases that hold private data. Discover and classify your databases, noting which ones hold private data such as credit card numbers, social security numbers, and names, and use advanced security measures such as auditing, encryption, vulnerability assessment, and data masking where appropriate.
- **Standardize on one or two DBMSes to minimize security risk.** Enterprises that standardize on one DBMS are likely to have a more secure database platform because their common policies and advanced security implementations will use common security tooling. When standardization is not possible because of legacy applications or other constraints, consider standardizing the configuration of each DBMS with a set of related database security tools.
- **Patch databases regularly to minimize risk.** Enterprises should adopt a policy of applying all database security patches on a regular basis and only consider skipping based on exception and sign-off by the CISO. Investigate rolling patch or clustering solutions from DBMS and other vendors to minimize downtime of databases due to applying patches. Always test the security patches in test environments, running regular test scripts to ensure that the patches don't affect application functionality or performance.
- **Centralize database security administration wherever possible.** Standardizing policies across data centers and databases will ensure consistent and stronger database security. This is especially critical for enterprises that have hundreds of databases that span more than one data center. Although different countries may have different compliance requirements, enforce local security policies only after global policies have been enforced.
- **Protect nonproduction databases, too.** Regulatory compliance requires you to protect *all* databases, including nonproduction databases such as those for testing, development, and training, at all times. It also compels organizations to ensure that only authorized users are allowed to view private data. Data masking helps protect such data in nonproduction environments from privileged users such as testers, developers, and outsourcing vendors.

## ENDNOTES

<sup>1</sup> A Florida man was arrested for stealing credit and debit card numbers of more than 170 million accounts from many retailers. Source: Tamara Lush, "Fla. man in credit card data theft accepts plea," Associated Press, Aug 28, 2009 ([http://www.google.com/hostednews/ap/article/ALeqM5i8XW66VLO5uQTgUW-ha\\_8H6QmBZAD9AC50NG0](http://www.google.com/hostednews/ap/article/ALeqM5i8XW66VLO5uQTgUW-ha_8H6QmBZAD9AC50NG0)).

<sup>2</sup> In the case of the largest data theft in US history, a Florida man and his accomplices looked for soft targets, especially retailers that had holes in their security implementations. Source: Tamara Lush, "Fla. man in

credit card data theft accepts plea,” Associated Press, Aug 28, 2009 ([http://www.google.com/hostednews/ap/article/ALeqM5i8XW66VLO5uQTgUW-ha\\_8H6QmBZAD9AC50NG0](http://www.google.com/hostednews/ap/article/ALeqM5i8XW66VLO5uQTgUW-ha_8H6QmBZAD9AC50NG0)).

- <sup>3</sup> Forrester estimates that more than 70% of attacks are internal, which makes database security even more challenging. See the February 27, 2009, “[Market Overview: Database Security](#)” report.
- <sup>4</sup> Forrester and TechTarget conducted a joint survey in November 2008 on database management. The survey gathered information from IT professionals at 148 enterprises. See the February 27, 2009, “[Market Overview: Database Security](#)” report.
- <sup>5</sup> Although most enterprises secure production data when dealing with private data, only a few secure such data when it’s used for application development and testing or when it’s sent out to outsourcing or offshore vendors. All enterprises should look at data masking technology to help protect private data in test environments. See the March 21, 2006, “[Protecting Private Data With Data Masking](#)” report.
- <sup>6</sup> It takes less than 10 seconds for a hacker to break into a database and steal confidential data. As each database has hundreds and thousands of connections, humans cannot manually defend against such attacks. See the February 27, 2009, “[Market Overview: Database Security](#)” report.
- <sup>7</sup> The DBA is often too busy maintaining and optimizing various enterprise databases to assume responsibility for managing database security implementations, while the information security group often does not have the expertise. The new role of database security analyst (DSA) fills this gap. See the April 4, 2008, “[A New Role Is Emerging Within IT: Database Security Analyst \(DSA\)](#)” report.

# FORRESTER®

Making Leaders Successful Every Day

## Headquarters

Forrester Research, Inc.  
400 Technology Square  
Cambridge, MA 02139 USA  
Tel: +1 617.613.6000  
Fax: +1 617.613.5000  
Email: [forrester@forrester.com](mailto:forrester@forrester.com)  
Nasdaq symbol: FORR  
[www.forrester.com](http://www.forrester.com)

## Research and Sales Offices

Australia	Israel
Brazil	Japan
Canada	Korea
Denmark	The Netherlands
France	Switzerland
Germany	United Kingdom
Hong Kong	United States
India	

*For a complete list of worldwide locations, visit [www.forrester.com/about](http://www.forrester.com/about).*

For information on hard-copy or electronic reprints, please contact Client Support at +1 866.367.7378, +1 617.613.5730, or [clientsupport@forrester.com](mailto:clientsupport@forrester.com).

We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Research, Inc. (Nasdaq: FORR) is an independent research company that provides pragmatic and forward-thinking advice to global leaders in business and technology. Forrester works with professionals in 20 key roles at major companies providing proprietary research, customer insight, consulting, events, and peer-to-peer executive programs. For more than 26 years, Forrester has been making IT, marketing, and technology industry leaders successful every day. For more information, visit [www.forrester.com](http://www.forrester.com).