SOLIX®
Empowering Data Management

A SOLIX WHITEPAPER

EXTENDING INFORMATION SECURITY TO NON PRODUCTION ENVIRONMENTS

Julie Lockner
Solix Technologies, Inc.
http://www.solix.com

Contents

Introduction to Securing Data

Information Privacy & Security Laws

HIPAA
Paper and electric based healthcare information

Graham-Leach-Bliley
Financial Privacy Rule

European Union Privacy Laws
Governs the collection and use of individuals' data

California Senate Bill 1386
~50% of states have information privacy laws

With the recent provisions in the Federal Rules for Civil Procedure, many companies are now in reaction mode investigating means for compliance. Several IT professionals have recently received mandates from superiors to implement plans immediately to ensure compliance. These new provisions in the federal legislation, as well as recent changes in The Sedona Guidelines on the Management of Electronic Information have created many challenges for IT departments that manage electronic information.

For structured data, the problem is even more challenging when considering current database management practices. For every production database application, many IT organizations create multiple copies of the database for production support. These copies are used for test, Quality Assurance (QA), standby, training, and new application development.

In many cases, the copies are created in environments that do not have the same security controls as the production environment. If the production copy contains sensitive information, so do all of the copies. This poses a greater risk of insider theft or tampering of sensitive information.

Many application and database vendors provide features that allow IT departments to implement controls to prevent fraudulent activities, but if the features are not deployed properly in the non- production support copies, the risk of theft or tampering still exists.

Examples of controls available in database applications include encryption, digital certification, read-only mode, and auditing features. Many of these controls if deployed improperly may have adverse effects on application performance. The controls may also increase the cost of the application if the features incur additional license fees. To mitigate performance implications, IT departments may upgrade application servers by increasing the number of CPUs, also driving the total cost of ownership higher. When evaluating the type of information stored in these database applications, implementing these controls on all data in the database may not be necessary. Deploying data classification policies on specific data within the database addresses many of these issues.

For sensitive information that resides in the production database copies, a separate data security policy can be deployed to protect the sensitive information in the copies. For example, if a person's Social Security Number (SSN) is stored in a test copy, a data masking or scrambling policy can be executed across all instances of SSN in the database copy protecting the individual's personal information. Another use case for a data security policy involves Human Resources and Payroll applications. Audit controls are common on tables that store a person's pay grade and commission rates. These examples of data security policies further reduce risk associated with data theft and tampering.

This paper continues to discuss best practices associated with creating secure test and development copies of production databases.

Risk of Data Theft Exists Inside the Firewall

Companies are grabbing unwanted headlines when it comes to theft of secure and sensitive data. The source of the theft is predominantly from insiders within the company who have access to data inside the firewall. Employees who have access to sensitive data, such as Application Developers, Database Administrators and System Administrators typically have access to secure passwords and accounts where sensitive information is more easily accessible.

Applications in production typically have additional security measures in place to prevent unauthorized access of sensitive data. This includes encrypting the network between the web and application servers and the database servers where the sensitive data resides. Protecting data in transit, or data in motion, is a common practice for production environments. Within the application, technology such as single sign-on ensures only those who should have access to the data are authenticated. Audit controls should be in place to keep a close eye on the production data access.

Once the production database application is copied for test, patch or training, the same security measures may not be in place. Or even if the encryption between the application and database exists, the data in the database, or data at rest, is still vulnerable if the wrong person gains access to the login accounts in the test and development environment. This is why it is critical to look at solutions where the sensitive data at rest, residing in the database, is protected.

Risk of Data Theft Exists in an Outsourcing Model

Another area of concern is with trusted partners outside the firewall. Outsourcing data center support or application development projects require copies of applications and databases to be replicated to a third party development or support center. Many times it is not necessary for these organizations to have access to original corporate data for testing and training.

Extra measures should be in place to protect sensitive data once it is outside the firewall. Encrypting backup tapes is not adequate security. In order to run tests against the copied data, the encrypted backup files need to be decrypted and data restored into a working environment. Once the data is restored, there may be limited security controls in place, placing sensitive data now in risk.

Database Security Tools

The database management system tools for security are categorized into four buckets: vulnerability assessment, encryption, monitoring and auditing.

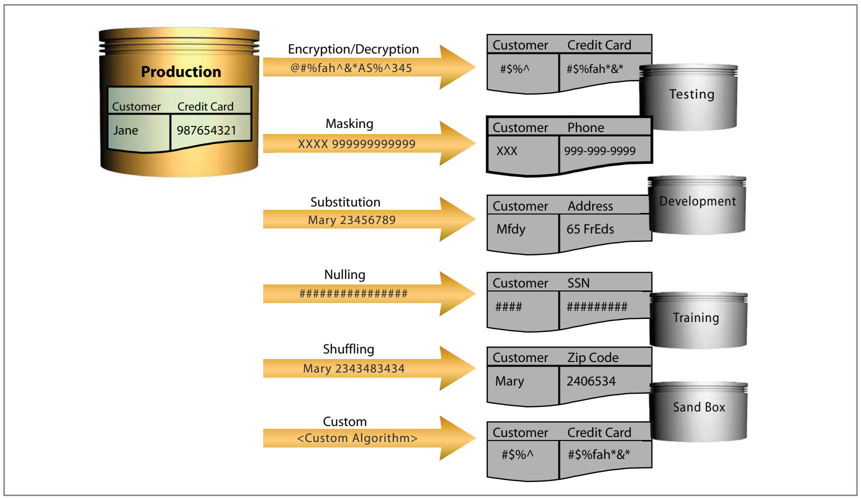
Vulnerability assessment offers solutions to evaluate an application environment for security holes, such as default passwords not changed. Encryption includes protecting data in motion as well as data at rest. Data masking and obfuscation falls into this market category, Monitoring and auditing include solutions that review database traffic for unauthorized access and auditing for logging who accessed what data and when.

Many point solutions exist for each set of functions; however firms are looking to centralize database security policies across heterogeneous DBMS data center. The ability to define a single data security policy for a set of transaction tables adds significant value to the overall solution because the business context is tied with the actual data security service. Many vendors in each specialized area are starting to merge either through adding complementary functionality or through partnerships.

When reviewing options for data security, specifically masking sensitive data in test and development database copies, the following features are required in a complete solution.

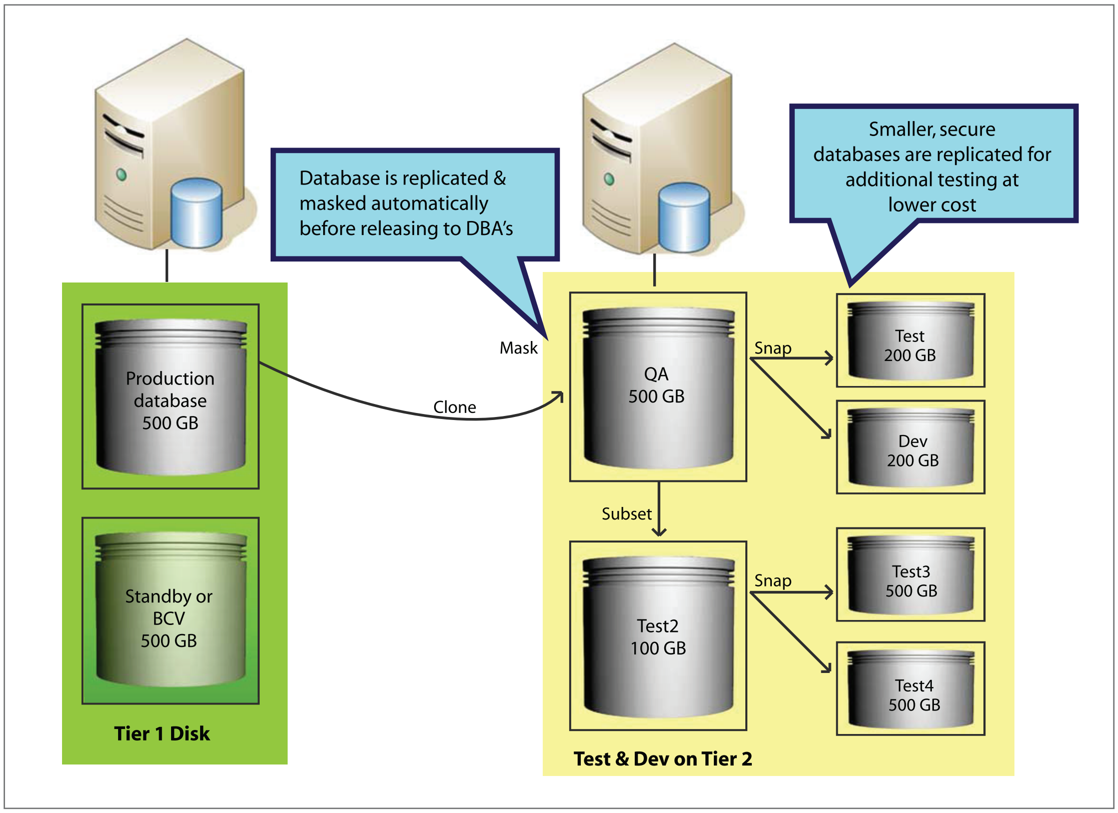
Required Data Masking Features

- Alter data so people who have access would not be able to determine actual values
  - This can be accomplished through one way data scrambling and/or random data generation
- Maintains functional appearance to not impact QA and development processes
  - Substitute values, i.e.
    Dave Robert, Dave_robert@solix.com => xxxx xxx, yyy@xyz.com
    Dave Robert, Dave_robert@solix.com => Jane Doe, Doe_Jane@xyz.com
- Supports Encryption and Decryption capabilities (data at rest)
  - For when the app server incorporates encryption during reads / writes
- Maintains Transaction Relational Integrity
  - For when sensitive data is a Primary/Foreign Key
- Easy to use and to set up policies
  - hose who set up the policies should be different than those who execute them



Optional Database Instance Subsetting

In addition to masking sensitive data in test and development copies, removing complete sets of data is another option. Leveraging a solution that provides database instance subsetting provides the ability to select sets of transactions or application modules and remove the data either through a deletion or truncate process. By removing the data completely from the copy, risk of exposure is completely eliminated. Another significant benefit of instance subsetting is the reduced storage requirements because now the copy of the database is significantly smaller.


Database is replicated & masked automatically before releasing to DBA's
Smaller, secure databases are replicated for additional testing at lower cost
Production database 500 GB
Standby or BCV 500 GB
Tier 1 Disk
Clone
Mask
QA 500 GB
Snap
Test 200 GB
Dev 200 GB
Subset
Test2 100 GB
Snap
Test3 500 GB
Test4 500 GB
Test & Dev on Tier 2

Summary

Combining the best practices of data security and creating test and development copies in an automated process reduces the exposure of sensitive data. Different solutions exist in the market to address these challenges, each with unique benefits and challenges. When evaluating vendor technology, it is important to keep in mind that database applications change constantly. The ability to maintain a policy definition in a constantly changing environment requires a tool that is easy to use and can be easily updated without redeveloping scripts or code. In addition, make sure the solution can adapt to technical changes that may occur at the database and application level such database versions and supported operating systems, application upgrades and migrations. So whether your data center is consolidating vendor technologies to a homogeneous environment, or implementing best of breed solutions, the policy definitions and data security technology you choose should adapt to your changing needs.

JULIE LOCKNER is vice president of sales operations for Solix Technologies. For more informati o n on Solix and its products and services please visit www.solix.com or call (888) GO-SOLIX.

About SOLIX

Solix Technologies, Inc., a leader in enterprise data management solutions for Information Lifecycle Management, helps businesses improve application performance, reduce storage costs and meet their compliance requirements. As an ORACLE Certified Partner and SAP Complementary Software Provider (CSP), Solix is dedicated to delivering world-class software with quality at its core. With an extensive global client base, including many Fortune 500 companies, Solix is considered a pioneer in providing a complete infrastructure platform to manage data across all segments (Application, Email and Documents) in an enterprise.

Solix Technologies, Inc.
4701 Patrick Henry Dr.,
Building 20
Santa Clara, CA 95054
Phone: 1.888.GO.SOLIX (1.888.467.6549)
1.408.654.6400
Fax: 1.408.562.0048
URL: http://www.solix.com

This document is provided for information purposes only and the contents hereof are subject to change without notice.

This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchant- ability or fitness for a particular purpose.

We specially disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Solix is a registered trademark of Solix Technologies and/or its affiliates. Other names may be trademarks of their respective owners.