



Data Obfuscation in Non-Production Environments

SCOAUG

September 25, 2006

Chuck Kennedy (7-Eleven)

John Stouffer (Solution Beacon)



O-B-F-U-S-C-A-T-I-O-N Defined

- **ob-fus-cate:**
- **To make so confused or opaque as to be difficult to perceive or understand: “A great effort was made... to obscure or obfuscate the truth” (Robert Conquest)**
- **To render indistinct or dim; darken: *The fog obfuscated the shore***
- **to confuse, bewilder, or stupefy**



7-Eleven Application Install

- **General Ledger (1996)**
- **Accounts Payable and Project Costing (1998)**
- **Procurement (2000)**
- **Human Resources and Payroll (2004)**
- **Version 9i RDBMS, HR Family Pack K and Release 11.5.10.2 Technology Stack Upgrade (2005)**
- **Release 11.5.10.2 / ATG RUP #3 Upgrade (2006)**
- **Fixed Assets and Accounts Receivable (2006)**
- **Over 1500 CEMLI's**
- **10 - 2.1 TB Non-Production Environment Footprint**



Colliding Dynamics

- **Historical Practice to Create Full Copies from Production**
- **Emergence of Offshore Software Factory**
- **Increased Visibility and Penalties from Regulatory Agencies**
- **Recent Implementation of Oracle HR/Payroll**
- **Multiple, Diverse Project Teams**
- **Basic Security Steps Not Necessarily Performed**
 - **Users**
 - **Responsibilities**



DBMS_OBFUSCATE?

- **Discussed with Oracle Database and AOL Security Teams – Any Out of the Box ERP Solutions?**
 - What about DBMS_OBFUSCATE Package?
- **Metalink Pronouncement**
 - Oracle allows database data to be encrypted and decrypted using the built in package DBMS_OBFUSCATION_TOOLKIT
 - The package contains four procedures
 - Two procedures that Encrypt VARCHAR2 and RAW data
 - Two procedures that Decrypt VARCHAR2 and RAW data.
 - To install the package
 - Connect as SYS and run dbmsobtk.sql and prvtobtk.plb
 - Grant execute on dbms_obfuscation_toolkit to public
 - The functions accept two parameters
 - the data to encrypt or decrypt
 - the key used for the encryption or decryption algorithm.
- **Only Problem =====> Apps Hurl-age Occurs!**



Problem Approach

- **What's Showing That's Better Off Not Being Shown?**
 - ❑ **Identified "Sensitive" Tables/Columns**
 - **Bank Accounts and Routing Information**
 - **Customer Information**
 - **Employee Information**
 - **Vendor Information**
 - **Payments**
 - **Payroll Information**
 - **SSN**
- **Exposure Is Occurring Where?**
 - ❑ **Applications Layer and Database**
- **Gotta Know your A's and C's! (Attributes and Constraints)**



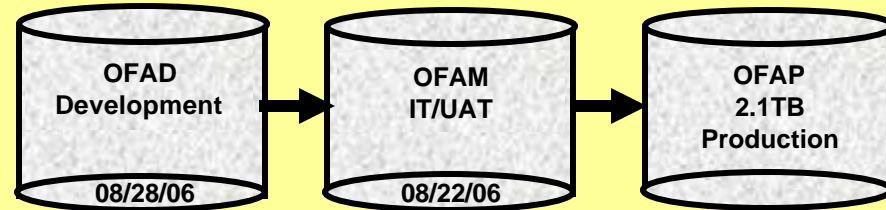
It's A SAD, SAD, SAD, SAD World

- **Meaningless Values Assigned (We Excel At This!!!!)**
- **SAD (Search and Destroy) Scripts**
 - Takes About a Day – Table Driven**
 - All Data Scrambled Unless Otherwise Requested / Approved**
 - Scorched Earth for Interface Tables**
- **Target Instance Strategy**
 - Development vs. Test**

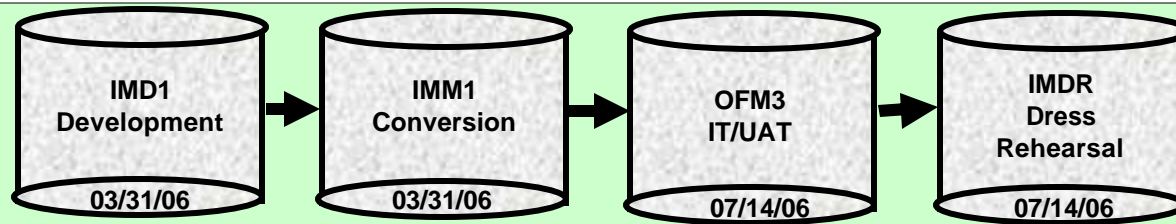


7-Eleven Instance Diagram

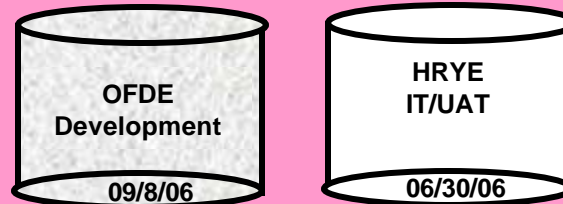
Level 1 Production Support



Level 2 Assets and Tax



Level 3 Enhancements and EOY Patching



Level 4 Projects



3/26/2007

➔ Automated Migration

 Denotes 11.5.10 Instance



What About Prod Options?

- **SAD Not A Very Viable Option!**
- **New Database Read Roles**
 - xxAA_readall_role**
 - xxAA_readltd_role**
 - **Where “AA” = Application Code (i.e. GL, AP, PO, et al)**
- **Audited Apps Users and Responsibilities**
- **Don't Forget Discoverer and Discoverer 4i Desupport**
- **Incremental Business Process Owner Approvals**
- **Role Based Access Controls (RBAC) – UMX Module**



Hot Off The Press!

- **Virtual Private Database – What is it?**
 - **Row Level Security**
 - **Database Security Policy**
 - **Appends Additional “Where” Clause**
 - **Tie Database Security Policies to Apps Responsibilities**
 - **Ongoing Maintenance of Security Policies**
 - **ATG RUP 4**
 - <http://www.securityfocus.com/infocus/1743>
 - <http://otn.oracle.com/deploy/security/oracle9ir2/pdf/VPD9ir2twp.pdf>



Last Minute Advice From Chuck

- **Proverbs 17:28**
**“Even a fool is thought wise if he keeps silent,
and discerning if he holds his tongue.”**



Keeping It Real

- **Questions?**