Auditing Data Access Without Bringing Your Database To Its Knees

Black Hat USA 2006
August 1-3

Kimber Spradlin, CISA, CISSP, CPA
Sr. Manager Security Solutions

Dale Brocklehurst
Sr. Sales Consultant
Agenda

• Auditing Requirements In The Regs
• Accessing Data in the Database
• Native vs. Network Data Access Auditing
• Live Demo
Auditing Requirements In The Regs
IT Compliance Chaos

Industries
- Financial Services
- Healthcare/Pharma
- Federal Government
- Retail
- Energy

Mandates
- Sarbanes-Oxley
- GLBA
- Basel II
- HIPAA
- 21 CFR Part 11
- PCI DSS
- State Data Breach Disclosure Laws
- FISMA
- Int’l. Data Privacy Laws
- FERC/NERC

Guidance
- PCAOB
- COSO
- CobiT
- FFIEC
- ISO 17799
- NIST 800-66
- NIST 800-53
- DoD STIG
- ITIL
<table>
<thead>
<tr>
<th>What to Log</th>
<th>CobiT (SOX)</th>
<th>PCI DSS</th>
<th>HIPAA</th>
<th>CMS ARS</th>
<th>21 CFR Part 11</th>
<th>GLBA</th>
<th>ISO 17799</th>
<th>NERC</th>
<th>NIST 800-53 (FISMA)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Access (Successful/Failed SELECTs)</td>
<td>(I)</td>
<td>(I)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Changes</td>
<td>(I)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Access</td>
<td>(I)</td>
<td>(I)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Successful/Failed Logins; User/Role/Permissions/Pswd changes</td>
<td>(I)</td>
<td>(I)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privileged User Activity</td>
<td>(I)</td>
<td></td>
<td>(I)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(I)</td>
<td></td>
</tr>
<tr>
<td>(All)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Changes</td>
<td>(I)</td>
<td>(I)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Enable/Disable Logs, Services, Configs; Reboots, Errors)</td>
<td>(I)</td>
<td>(I)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Schema Changes</td>
<td>(I)</td>
<td>(I)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Create/Drop/Alter Tables, Columns)</td>
<td>(I)</td>
<td>(I)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

NIST 800-53 (FISMA)
Data Breach Notification Law

PII = Name + SSN/DL/CC/BA Number

Specifies notification requirements
- When – X days after discovery
- Who – everyone who’s data was lost
- Most offer exemption if data encrypted
- Some offer exemption if “unlikely” the data will be used

Does NOT specify how to PREVENT a breach
- If you aren’t monitoring data access, hard to know if there’s a breach (except in the case of physical loss)
- Complete audit trail will give clear picture of exactly what data was taken and which customer records were affected

Are you better off not knowing?
- “If I don’t know a breach occurred then I’m not in violation when I don’t notify anyone”
- Willful ignorance doesn’t fly with the regulators
- Do you really want to learn about the breach from your TV?
- Tens-of-thousands of customer calls you aren’t prepared to handle
Where is my PII?

• Many locations:
  • E-mail – content security
  • Excel & Word – Help!
  • Paper – physical security
  • Databases – largest concentration

• Scan your network!
  • Like all other types of IT assets, you will likely be surprised by how much is out there
  • Must handle devices (e.g. laptops) that aren’t always connected to the network
  • Must be able to tell you what applications are installed on each device
  • Must be able to traverse network devices (bridges, routers, firewalls, etc.)

• Tricky part – what kind of data is in those databases you didn’t know about?
  • Reverse-engineering tools will build a data model for you
  • Have to gain access to the db first though
Accessing Data in a Database
SELECT Statement

- Used to retrieve data from the database
- Typically generated by an application and “removed” from the business user

- SELECT name, address, ssn FROM cust_tbl
  - Retrieves all records from that table
  - SQL itself does not contain any sensitive data (so neither does the log file)

- SELECT WHERE acct=1231231123 FROM acct_tbl
  - Retrieves only one record
  - SQL statement contains account number
## Protecting Logs

<table>
<thead>
<tr>
<th></th>
<th>CobiT (SOX)</th>
<th>PCI DSS</th>
<th>HIPAA</th>
<th>CMS ARS</th>
<th>21 CFR Part 11</th>
<th>GLBA</th>
<th>ISO 17799</th>
<th>NERC</th>
<th>NIST 800-53 (FISMA)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limit Read Access</td>
<td>(I)</td>
<td></td>
<td>(I)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Separate from DBs/DBAs Being Monitored</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prevent Changes</td>
<td>(I)</td>
<td></td>
<td>(I)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sufficient Storage Capacity</td>
<td>(I)</td>
<td></td>
<td>(I)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encrypt Sensitive Data</td>
<td></td>
<td>(I)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alert on Changes, Capacity, and Errors</td>
<td>(I)</td>
<td></td>
<td>(I)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: The chart indicates compliance with various standards and frameworks. The symbols (I), (II), (III), etc., represent different levels of compliance or criteria, while the filled circles (●) indicate specific requirements met by certain standards. The absence of symbols suggests no specific criteria are met for those entries.
Other Data Access/Retrieval Commands

• Additional methods:
  • Stored Procedures
  • Insert into
  • Bulk Copy Programs
  • Unload utilities
  • Backup routines
  • Replication services
  • Proprietary APIs

• Watch for:
  • Unexpected application IDs
  • Unusual syntax
  • Unusual source IP
## Review and Retention Requirements

<table>
<thead>
<tr>
<th>CobiT (SOX)</th>
<th>PCI DSS</th>
<th>HIPAA</th>
<th>CMS ARS</th>
<th>21 CFR Part 11</th>
<th>GLBA</th>
<th>ISO 17799</th>
<th>NERC</th>
<th>NIST 800-53 (FISMA)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Review Logs Regularly</strong></td>
<td>At least Monthly</td>
<td>Daily</td>
<td>At least Monthly</td>
<td>1-14 Days</td>
<td>Daily</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>“On-line” Retention</strong></td>
<td>1-7 Years</td>
<td>3+ Month</td>
<td>1 - 6 Years</td>
<td>90 Days</td>
<td></td>
<td></td>
<td></td>
<td>90 Days</td>
</tr>
<tr>
<td><strong>“Off-line” Retention</strong></td>
<td>1+ Years</td>
<td>1 Year</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Back-up Audit Trails To Separate Media</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Native vs. Network Data Access Auditing
Database Auditing Solutions

Application Users
- Application users login to query and update underlying application data

Privileged Users (DBAs)
- DCL (Grant, Revoke)
- DDL (Create, Drop, Alter)
- DML (Insert, Update, Delete)
- DBAs access and update, accounts, schemas, and data

Enterprise Application

Corporate Data Assets
- (1) Database Auditing
- (2) Database Auditing
- (3) Database Auditing
Gaps in Native Auditing

• PERFORMANCE!
  • Data access auditing can significantly slow down existing system performance affecting end-user SLAs

• Vulnerable to insiders
  • DB privileged users can disable or alter logs stored on the database being monitored

• Insufficient visibility, control
  • Database platforms are highly variable in audit records

• Complex to manage
  • Multi-platform environments require multiple skill sets
  • Variable platforms mean inconsistent reports

• No aggregation
  • Separate logs for each db instance
Comparing DBMS Data Access Logging

<table>
<thead>
<tr>
<th>Platform</th>
<th>SELECT Auditing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle</td>
<td>Fine Grain Auditing (FGA) – enhanced w/ 10g</td>
</tr>
<tr>
<td>Microsoft SQL Server</td>
<td>via SQL Server traces</td>
</tr>
<tr>
<td>Sybase</td>
<td>Sp_audit</td>
</tr>
<tr>
<td>DB2</td>
<td>Authorization Checking (CHECKING)</td>
</tr>
<tr>
<td>Informix</td>
<td>Read Row (RDRW)</td>
</tr>
</tbody>
</table>

- 10-30% CPU impact when enabling logging for all SELECT activity
- Often not granular – must audit a group of activities or audit across all tables
- Full info such as user ID, source IP, table name not always included with the SELECT audit record (just reference numbers that must be looked up)
- Full audit log = stopped database
Network-based Auditing Architecture

- Database Users
- Network Tap or Managed Switch
- Collector
- Monitored Database Server(s)

Middleware

- Network Listener
- Dispatcher(s) Data Router
- Database Reader
- Audit Repository
- Summary Routines
- Maintenance (back up, purge)
- Alerting Rules

Presentation

- Alerts
- Console
- Reports
Advantages To Network-Based Approach

- **Transparency**: no changes to Apps or DBs
- **Completeness**: log everything
- **Performance**: no impact to DBMS performance
- **Availability**: logging failure will not affect DBMS
- **Scalability**: monitor hundreds to thousands of DB instances
- **Segregation of Duties**: remove audit trails from control of systems/users being audited
- **Coverage**: consolidate and analyze across instances and platforms
- **Flexibility**: tailor auditing by activity, table, user, role
Live Demo!
Key Reports and Alerting Rules

- Large SELECT statements
- Failed SELECT statements
- Unauthorized source IP
- Unauthorized application ID
- Privileged Users
- Unusual SQL syntax
- Unusual increase in activity

- Audience: Others?
Resources

• Security Benchmarks
  • NIST SP 800-70: [http://csrc.nist.gov/checklists/download_sp800-70.html](http://csrc.nist.gov/checklists/download_sp800-70.html)
  • CIS Configuration Benchmarks: [www.cisecurity.com](http://www.cisecurity.com)
  • NSA: [http://www.nsa.gov/snac/downloads_db.cfm?MenuID=scg10.3.1.2](http://www.nsa.gov/snac/downloads_db.cfm?MenuID=scg10.3.1.2)

• Vendor Guidance:
  • Sybase: [http://manuals.sybase.com/onlinebooks/group-as/asg1251e/sag/@Generic__BookView/39806;td=50#X](http://manuals.sybase.com/onlinebooks/group-as/asg1251e/sag/@Generic__BookView/39806;td=50#X)
Contacts

• www.embarcadero.com

• Kimber Spradlin
  • Kimber.Spradlin@embarcadero.com
  • 303-730-7981 x127

• Dale Brocklehurst
  • Dale.Brocklehurst@embarcadero.com
  • 719-548-7400 x208