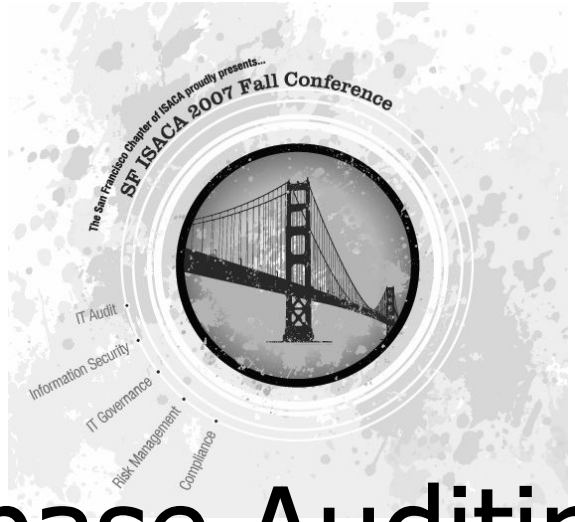


Database Auditing for Compliance, Security, & Reputation Management

Scott Hayes – DBI

Database-Brothers, Inc.

www.Database-Auditing.info

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Audience Warm Up

- Please silence your mobiles phones
- Please, no smoking or…
- Have Fun
- Ask EASY Questions [grin]
- Visit www.Database-Auditing.info
- How many of you have been impacted by Identity Theft?
  - Austin TX, 65% of ISACA Audience
  - Tampa FL, 42% of ISACA Audience
  - North Jersey Shore, 18% of IBM Audience

About Scott Hayes

- IBM GOLD Consultant
- Trade Journals - Published Author
- Internationally Recognized Conference Speaker on Database Performance, Security, and Auditing Topics
- Inventor US Patent #6,772,411 and Database Security Patents Pending
- President & CEO, DBI.

About DBI

- **Focus**: Accountability Solutions that hold privileged users accountable and aid audit and compliance staff with monitoring and reporting

- **Philosophy**: Maximum effectiveness with minimal overhead

- **Credibility**: Company was founded on expertise in database auditing, compliance and performance tools consulting

WE MAKE ACCURATE DATABASE AUDITING EASY AND EFFICIENT

Agenda for Today

- Common database auditing, monitoring, & reporting requirements for compliance ***from the field***
- Security Vulnerabilities in your databases
- DB2 & Oracle Examples
- Database Auditing Approaches
- Questions for you to ask your IT department

Data Breach Costs (Data Insecurity)

- Some Stats From The Field
  - Average cost per breach $4.8M*
  - Total cost to the company $182/record
  - Marketing & Customer Support most affected groups; where's IT?
  - 30% of breaches originate with external partners, CONSULTANTS, outsourcers, or contractors
  - 90% of breaches were digital in nature

*14 Separate Incidents Reviewed Source: Ponemon Institute

Data Breach Prevention & Consequences of Failure

- IT Preventative Measures
  - Cost 4% of the total breach cost, $180K
  - Not all respondents had electronic protections in place
  - 70 – 80% of issues come from the *inside*
- Lost Customers
  - After receiving notification of a breach, 20% of customers terminated their relationship with the company
  - 40% were considering it
- How much does an identity (first name, last name, DOB, SSN) cost on the black market?
  - $14-18, Symantec Study, fall 2006

The “TJX Effect”

» Slashdot
» News Stories

By Larry Greenemeier
InformationWeek
August 11, 2007 12:02 AM (From the August 13, 2007 issue)

TJX will be glad when this year is over. The $17 billion-a-year parent company of T.J. Maxx, Marshall's, and several other discount retail chains has spent the past eight months dealing with the largest breach of customer data in U.S. history, the details of which are starting to come to light.

Last December, TJX says it alerted law enforcement that data thieves had made off with more than 45 million customer records. Since that time, at least one business, Wal-Mart, has lost millions of dollars as a result of the theft, while TJX has spent more than $20 million investigating the breach, notifying customers, and hiring lawyers to handle dozens of lawsuits from customers and financial institutions. Should TJX lose in the courts, it could be on the hook for millions more in damages.

But there's an even broader TJX Effect: The data breach, which actually took place over a period of years, has put the entire retail industry on the defensive and stirred up demands for all businesses that handle payment card information to do a better job of protecting it. Legislators are invoking TJX's name to fast-track data-security bills.

Business Requirements - Auditing for Compliance & Security

- Regulatory Compliance
  – A rose by any other name
- Security –Threats from the inside
- Protection of most precious corporate asset
- Auditing is a *business* requirement
- Identify/Expose material weaknesses

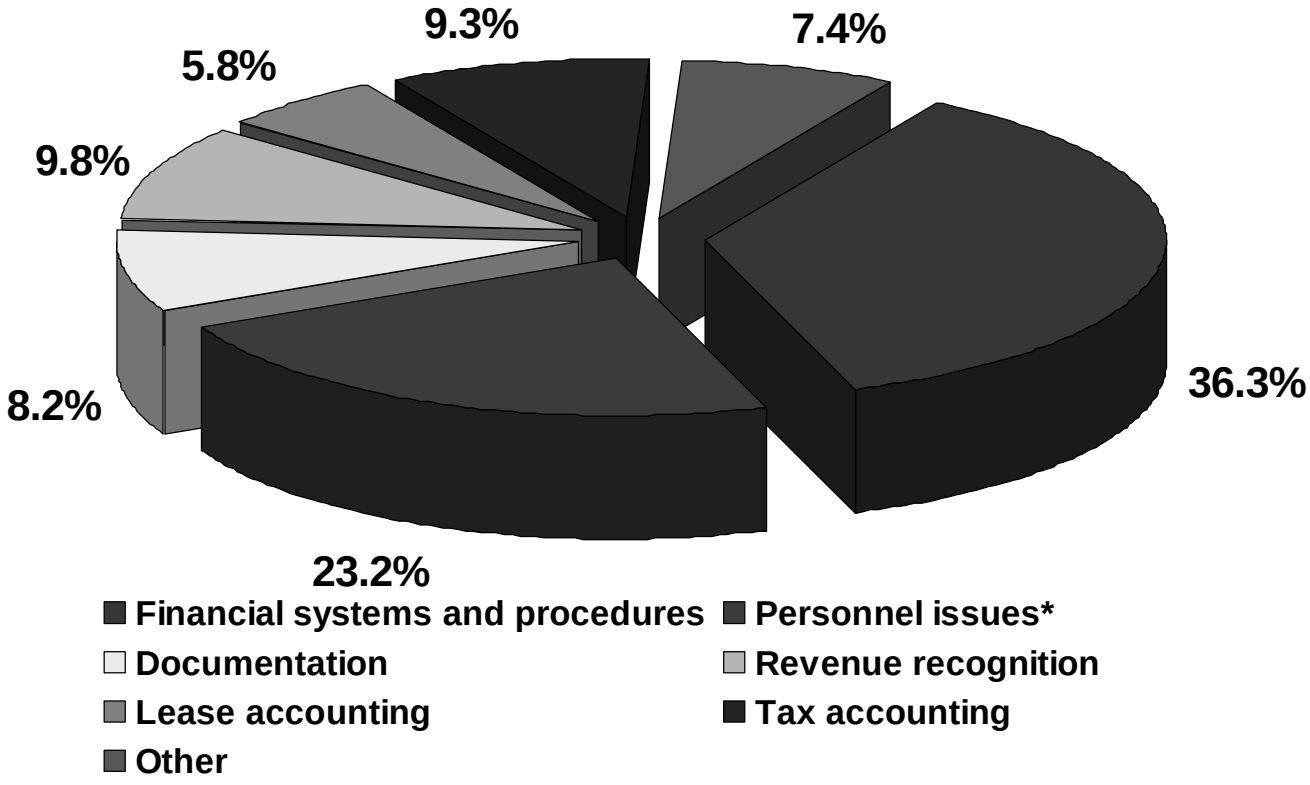
"Business Speak" for Compliance

- Avoid Headlines
- Avoid FTC Fines
- Avoid Stock Drops
- Avoid Lawsuits and/or Business Closure
  - CardSystems, 40M Records, 7/26/2005
  - Contracts terminated by Visa and AMEX

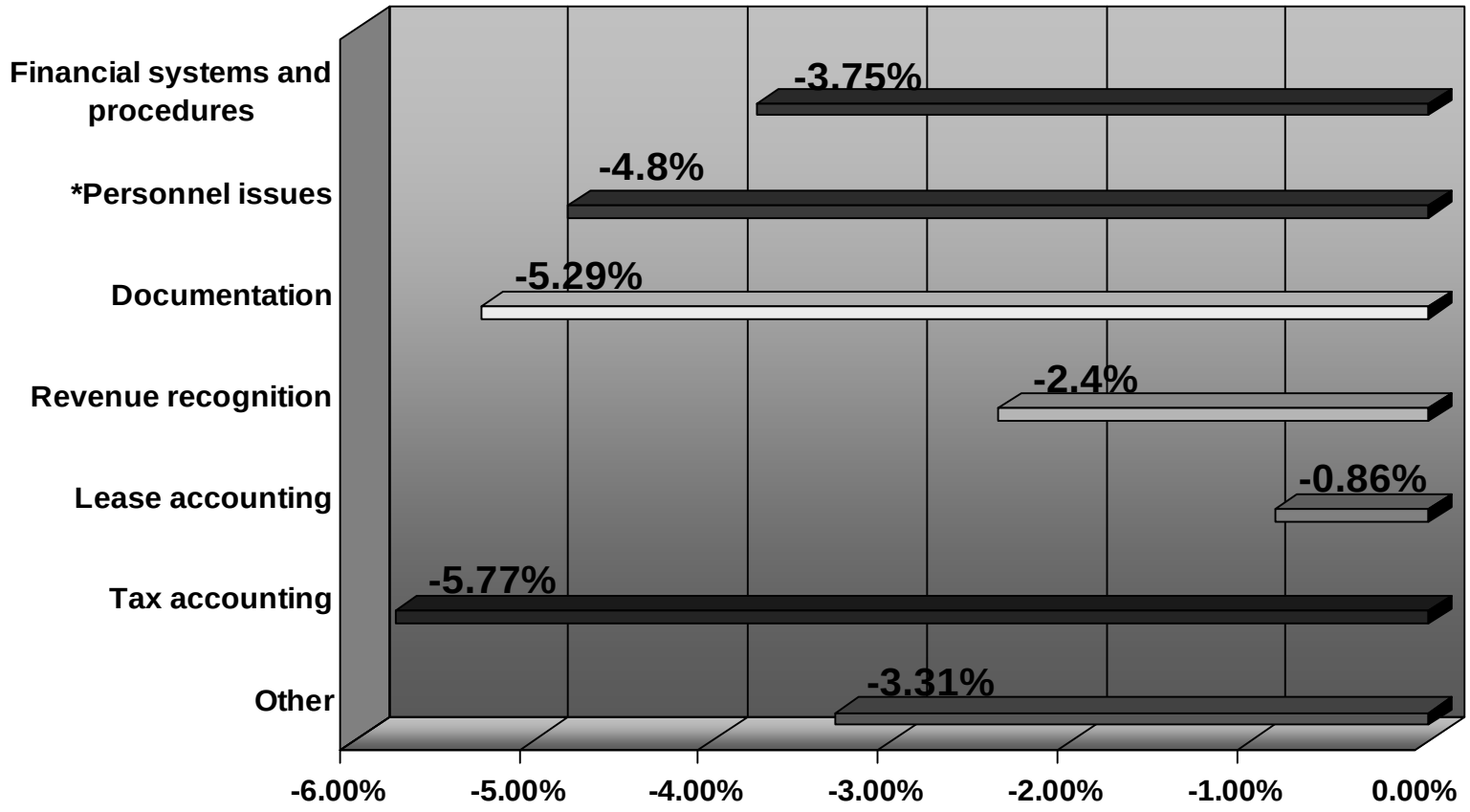
*** "Personnel issues" refers to lack of competent finance/accounting staff or insufficient staffing levels.**

Source: Glass, Lewis & Co.; company filings

Classification of 899 Companies Disclosing Material Weaknesses in 2004-2005



Average stock-price movement relative to market from 7 days prior to announcement to 60 days after.



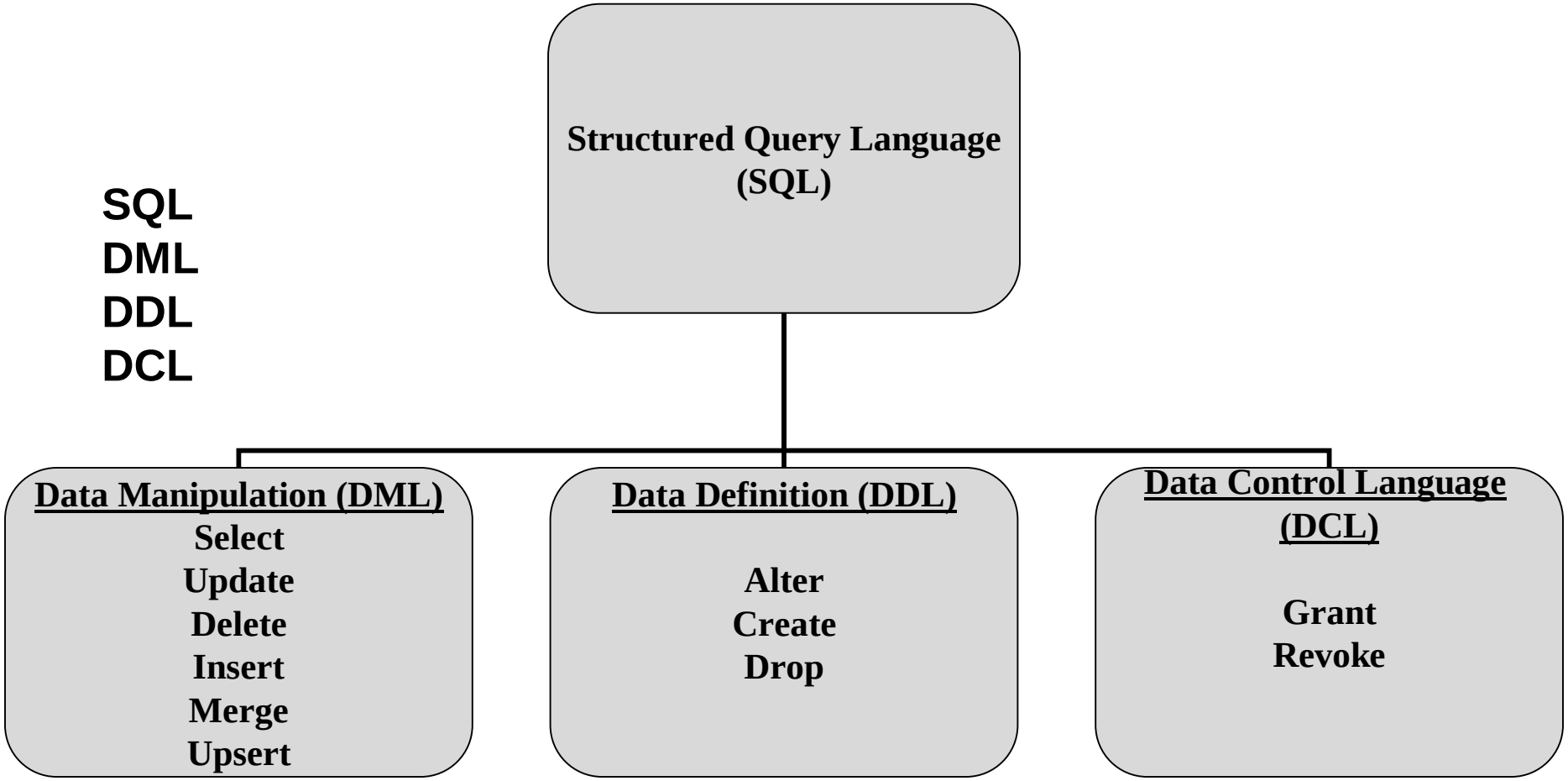
Note: Averages include companies over $75m in market capitalization.
Source: Glass, Lewis & Co.; FactSet

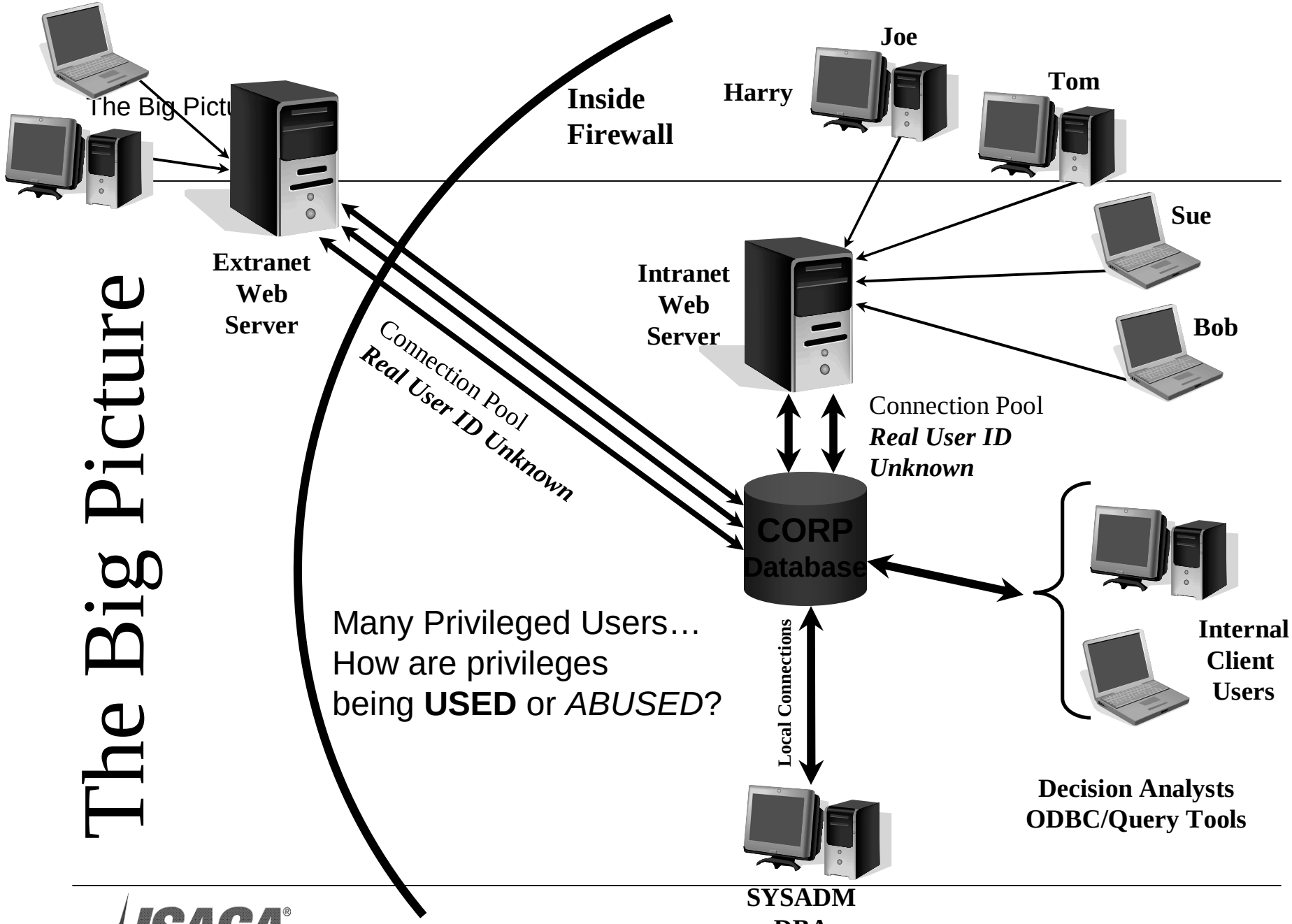
"Audit Speak" for Compliance

- Basel II
- Sarbanes-Oxley
- HIPAA
- Gramm-Leach-Bliley (GLBA)
- PCI
- California SB1386 ...
  - **The California Security Breach Notification Act (SB 1386)**

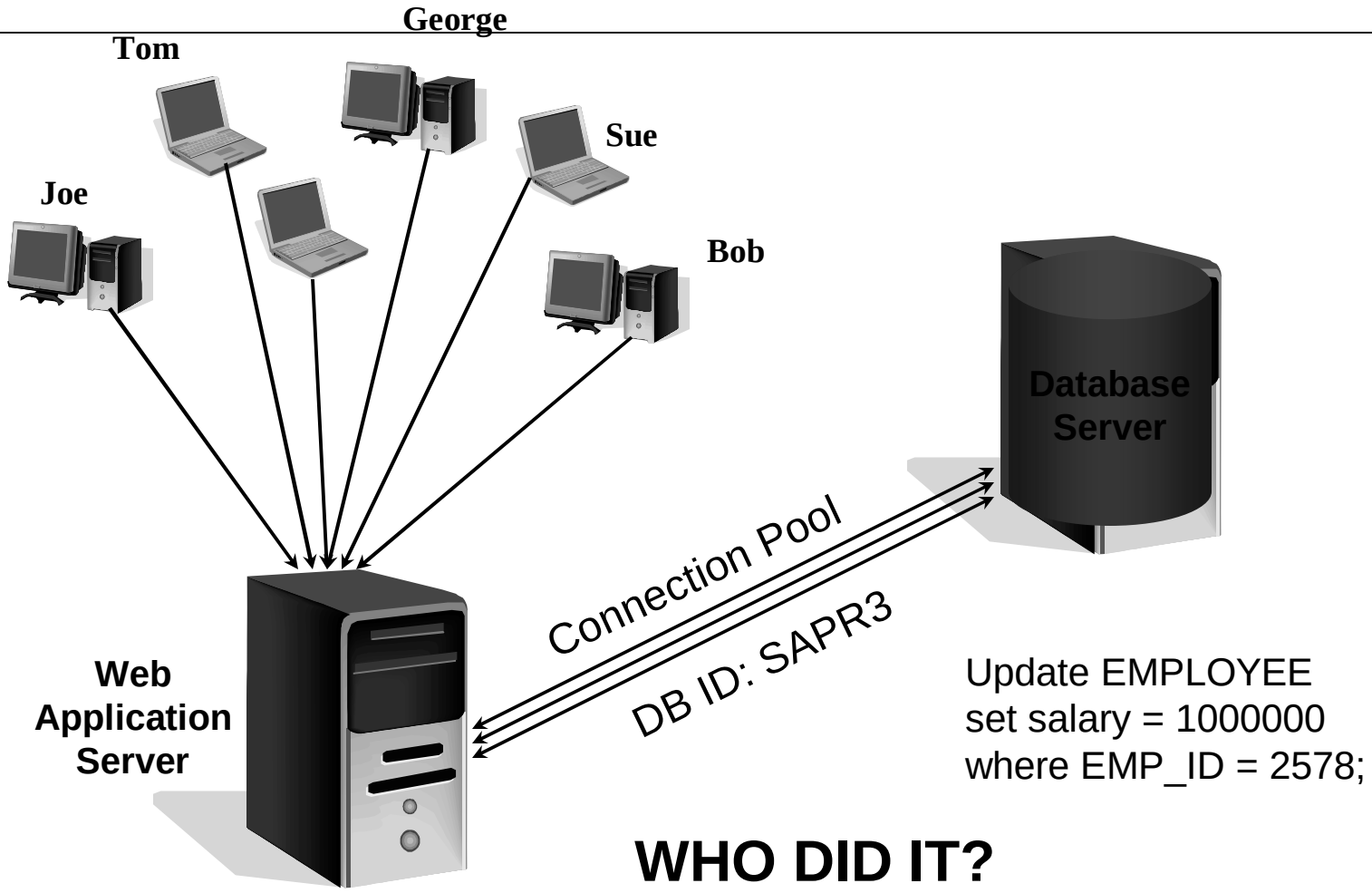
"Geek Speak"

SQL
DML
DDL
DCL




The Big Picture
The Big Pictu
Inside Firewall
Joe
Harry
Tom
Sue
Bob
Extranet Web Server
Intranet Web Server
Connection Pool
Real User ID Unknown
Connection Pool
Real User ID Unknown
CORP Database
Many Privileged Users…
How are privileges being USED or ABUSED?
Local Connections
Internal Client Users
Decision Analysts
ODBC/Query Tools
SYSADM
DBA
(Super Users)

The Anonymous User Problem



Consequences of Anonymity

earnings next week. Nissan Motor reported Tue. had a 4.2% increase in quarterly profits. (GM earn. 1B.)

IRS workers could get unofficial access to data

By Kevin McCoy
USA TODAY

IRS employees could be gaining unauthorized access to confidential taxpayer information because many of their supervisors aren't checking on them, a new government audit reported Wednesday.

On average, 42% of IRS supervisors sampled in the audit certified that they had reviewed security reports showing whether their staffers gained access to taxpayer information without authorization.

The certification rate ranged from a low of 15% for IRS supervisors in Austin to a high of 75% for their Brookhaven, N.Y., counterparts, according to the audit by the Treasury Inspector General for Tax Administration.

"As a result, employees may be browsing their spouses' or other employees' tax information with little chance of detection," the audit concluded.

Underscoring the potential danger, auditors report-

Musel
tempt
"Nobo
The
the fin
sorted
ness, M
Amo
▶ Te
be bui
its two
The
tery w
and a t
Tesl
Musk,
capital
rocket
By
start,
tion of
Musk
person
early 1
"Ou
nies o
petitiv

Typical Audit Requirements

- Who did what, when?
- Notification of access to certain tables or columns
  - When over/under a certain amount/conditions
  - (Even when through a View, MV or Synonym)
- Protect the audit data from tampering; and *prove* that it is authentic

What do Auditors Want?

- "Separation of duties" employed
- "Principle of Least Privilege" employed
- Transaction Documentation
- Notification of issues
- Reporting
- Integrity of audit data
  - Database
  - Report

What does IT want?

- Application Reliability
- Application Performance, Performance, Performance...
- Minimal constraints to get job done
- And PERFORMANCE!

The Challenge

To adequately guard against internal security threats without restricting business.

The Bad News

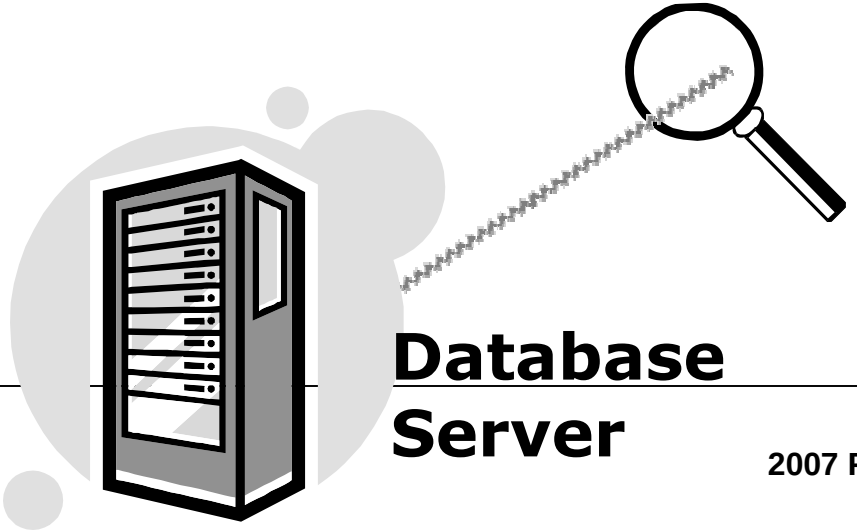
There's a lot of different ways to reach same data

- The Application itself
- End user query tools
  - WebFOCUS, Business Objects, Cognos, Excel, MDAC etc.
- Remote connections to the database
  - TOAD, SQL*Plus, CLP, Terminal Services, etc.
- Direct connections to the database
  - TOAD, SQL*Plus, CLP, Terminal Services, etc.

The Good News

The data is in one spot – the database.

This is where the defense mechanisms should be in place.



Database Server

DB Security – The Stakes

- Attacks from legitimate users
  - Users of a database gaining DBA privileges
- Elevation of privileges
  - Using functions internal to the database
  - Equivalent of local attacks on Unix
- Attacks from employees not granted access
  - Disgruntled or curious employees
- Attacks from DBAs and SYSADM/SYSDBA (SuperUsers)

What do we need to audit?

- ***NEED, Not Want!***
- All activity ?
- All “power user” or “super user” activity ?
- Activity against certain tables ?
- Connections and disconnections (odd hours) ?
- DML and DDL and SQL ?
- Grants & Revokes (DCL) ?

“Just because you can, doesn’t mean you should”

Let business requirements dictate policies.

User Activity

- Everything done by a particular user
- Keep an eye on Bill
- Keep an eye on anyone with _____ role
- Auditing everything by everyone could be more intensive than the application itself!

```
SQL> audit all by bgates;
```

Privileged User Activity

- What is a privileged user?
- How many should you have?
- What can and can't they do?
  - Should be able to do things within the scope of their job
  - Should not be able to view data
  - Should not be able to cover own tracks

Table Access

- Granular or not?
- INSERT / UPDATE / DELETE / SELECT
- Limit to sensitive tables only
- Limit to sensitive columns only
  - even better!

```
audit update on employees;
```

Connections / Disconnections

- Audit all logon and logoff activity

Can be used to determine …

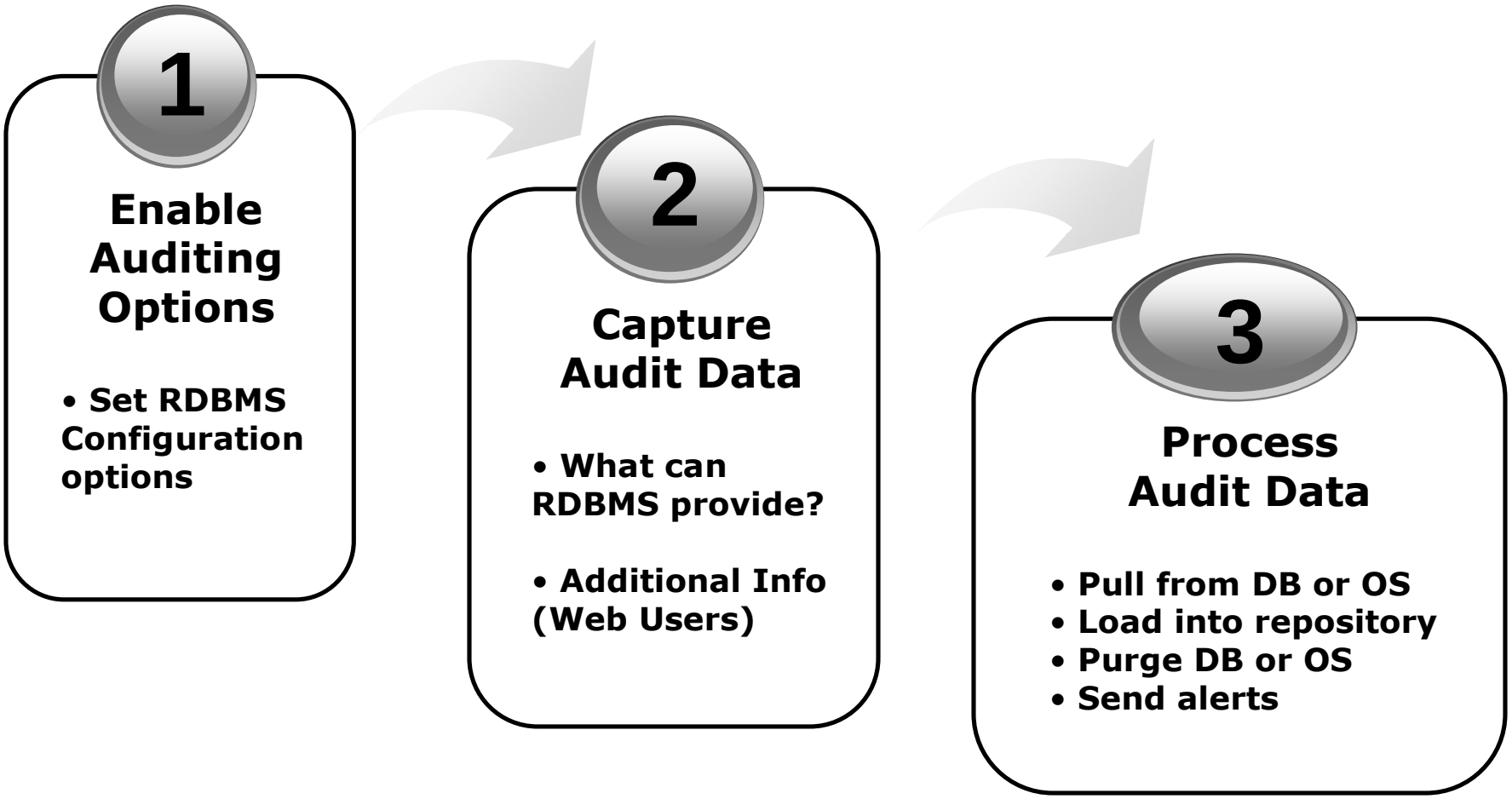
- Many invalid logon attempts *(= password guessing)*
- Sharing of USERID by different people *(=userid sharing)*
- Accessing database from many machines
  (=multiple access points)
- Accessing database during non-core business hours
  (=after hours via multiple access points)

DDL

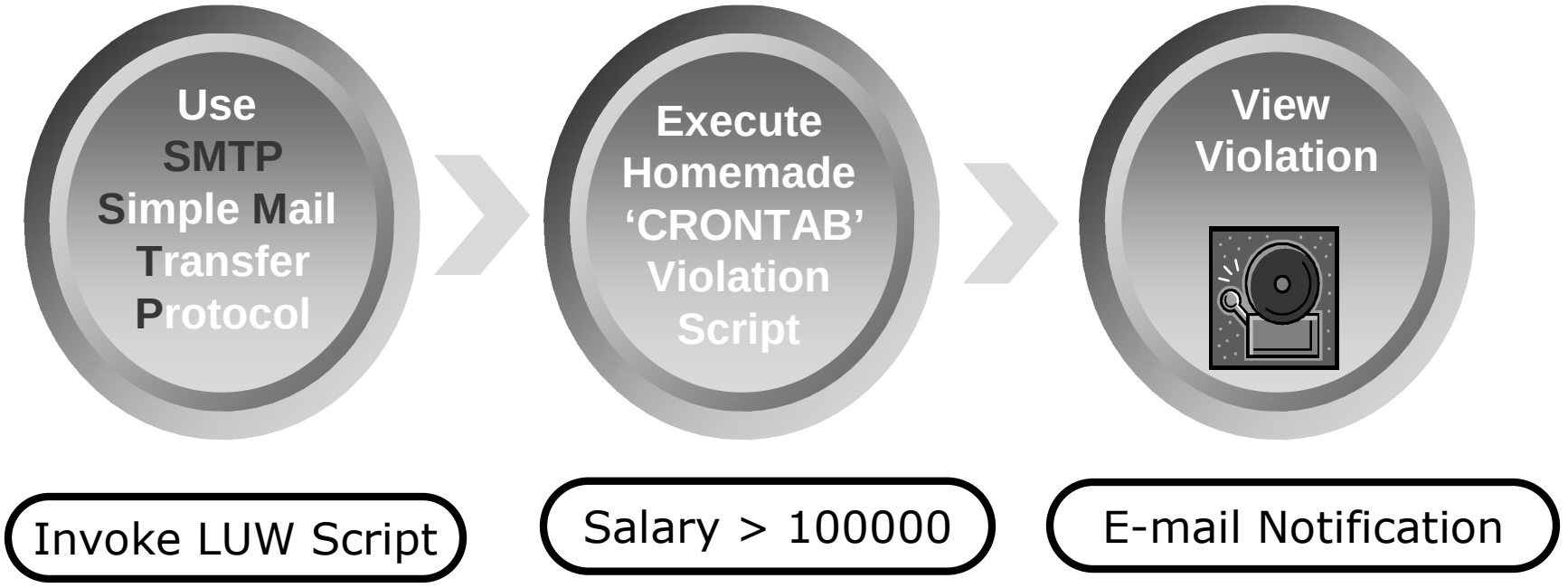
- What is Data Definition Language?
- DDL tasks should be scheduled
- Watching for structural changes is important
  - Create
  - Alter
  - Drop
- After Application is in production and stable

```
SQL> create view alex_emps as select * from employees;
SQL> create trigger … or synonym or materialized view …
```

Auditing Workflow

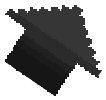


DB2 LUW Example ...



DB2 Notification E-mail
- (SMTP) – CRONTAB Example

```
db2 "select 'X1X', count(*) from syscat.TRIGGERS  " | grep X1X | while read lit mycount
do
  if [[ $mycount -gt 250 ]] then
    print "There are more than 250 TRIGGERS in the DB2 Catalog! " | mail -s "DB2 Alert" alexander.kopac@database-brothers.com
    print "There are $mycount TRIGGERS in the DB2 Catalog "
  else
    print "There are $mycount TRIGGERS in the DB2 Catalog "
  fi
done
db2 "select userid, appname, authid, appid, conntime, stoptime, fetchcount, rowsread, rowswritten, totalsorttime, cputime, sqlcode,'X1X' from
S_ADAMS_XYZ900D6_SAMPLE. AUDIT_EMPLOYEE where ((rowsread > 1000) or (fetchcount > 1000) or (rowswritten > 1000)) and (appname not in
('DB2HMON','db2hmon')) order by appname, fetchcount, rowsread desc with ur" | grep X1X | \
while read myuserid myappname myauthid myappid myconntime mystoptime myfetchcount myrowsread myrowswritten mytotalsorttime mycputime  mysqlcode myX1X
do
  if [[ $myrowsread -gt 1000 ]] then
    print "This is an Expensive SQL stmt " | mail -s "DB2 Alert - Expensive rowsread SQL" alexander.kopac@database-brothers.com
    print "This is an Expensive SQL stmt Greater_than_1000_rowsread with rowsread as $myrowsread "
  fi
  if [[ $myfetchcount -gt 1000 ]] then
    print "This is an Expensive SQL stmt!" | mail -s "DB2 Alert - Expensive fetchcount SQL" alexander.kopac@database-brothers.com
    print "This is an Expensive SQL stmt Greater_than_1000_fetchcount with fetchcount as $myfetchcount "
  fi
  if [[ $myrowswritten -gt 1000 ]] then
    print "This is an Expensive SQL stmt!" | mail -s "DB2 Alert - Expensive rowswritten SQL" alexander.kopac@database-brothers.com
    print "This is an Expensive SQL stmt Greater_than_1000_rowswritten with rowswritten as $myrowswritten "
   else
     print "This is a SECURITY VIOLATION SQL stmt!" | mail -s "DB2 Alert – SECURITY VIOLATION SQL" alexander.kopac@database-brothers.com
     print "This is a SECURITY VIOLATION SQL stmt "
  fi
done
db2 -v "terminate"
exit
```



Oracle Example ...

Oracle Exception Handler:

```
CREATE OR REPLACE PROCEDURE SAL_MODULE      IS
          V_SESSION_ID          number;
          V_TIMESTAMP           date;
          V_DB_USER             varchar2(30);
          V_OS_USER             varchar2(255);
          V_USERHOST            varchar2(128);
          V_CLIENT_ID           varchar2(64);
          V_ECONTEXT_ID         varchar2(64);
          V_EXT_NAME            varchar2(4000);
          V_OBJECT_SCHEMA       varchar2(30);
          V_OBJECT_NAME         varchar2(128);
          V_POLICY_NAME         varchar2(30);
          V_SCN                 number;
          V_SQL_TEXT            varchar2(2000);
          V_SQL_BIND            varchar2(2000);
          V_COMMENT$TEXT        varchar2(4000);
          V_STATEMENT_TYPE      varchar2(7);
          V_PROXY_SESSIONID     number;
          V_GLOBAL_UID          varchar2(32);
          V_INSTANCE_NUMBER     number;
          V_OS_PROCESS          number;
          V_ENTRYID             number;
BEGIN
  select
          SESSION_ID  ,
          TIMESTAMP   ,
          DB_USER     ,
          OS_USER     ,
          USERHOST    ,
          CLIENT_ID   ,
          EXT_NAME    ,
```

Oracle Create Policy

```
begin
DBMS_FGA.ADD_POLICY(
          object_schema       => ‘ALEX',
          object_name         => 'EMPLOYEES',
          policy_name         => 'SAL_TOO_HIGH',
          audit_condition     => ‘SALARY > 100000',
          audit_column        => ‘SALARY',
          enable              =>  TRUE,
           handler_schema      => ‘ALEX',
          handler_module      => 'SAL_MODULE',
          statement_types     => 'INSERT, UPDATE');
end;
```

Oracle Notification E-mail

Subject: Auditing Alert from Database HR_PROD

The database HR_PROD on host hr001 has reported the following auditing alert:

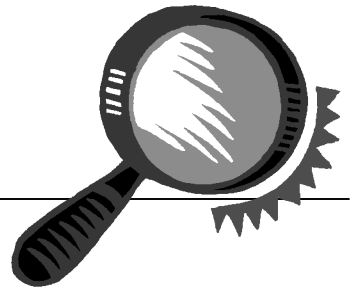
Alert Information

Date:	Jan-05-2007
Time:	11:30 p.m. CST
DB User:	DMOORE
App User:	dave_moore
IP Address:	172.18.25.144

Policy Information

Policy Name:	SAL_TOO_HIGH
Table Owner:	HR
Table Name:	EMPLOYEES
Column Name:	SALARY
Statement Type:	UPDATE

Auditing Best Practices



- Employ a selective auditing approach
- Use database privileges as first line of defense
- Monitor critical data and empowered users
- Monitor size of audit table and available space
- Monitor the enabling/disabling of auditing – Drops!
- Use test data in TEST and QA environments

Strive for each audit record to be meaningful!

Auditing Best Practices

- **Design databases with auditing in mind:**

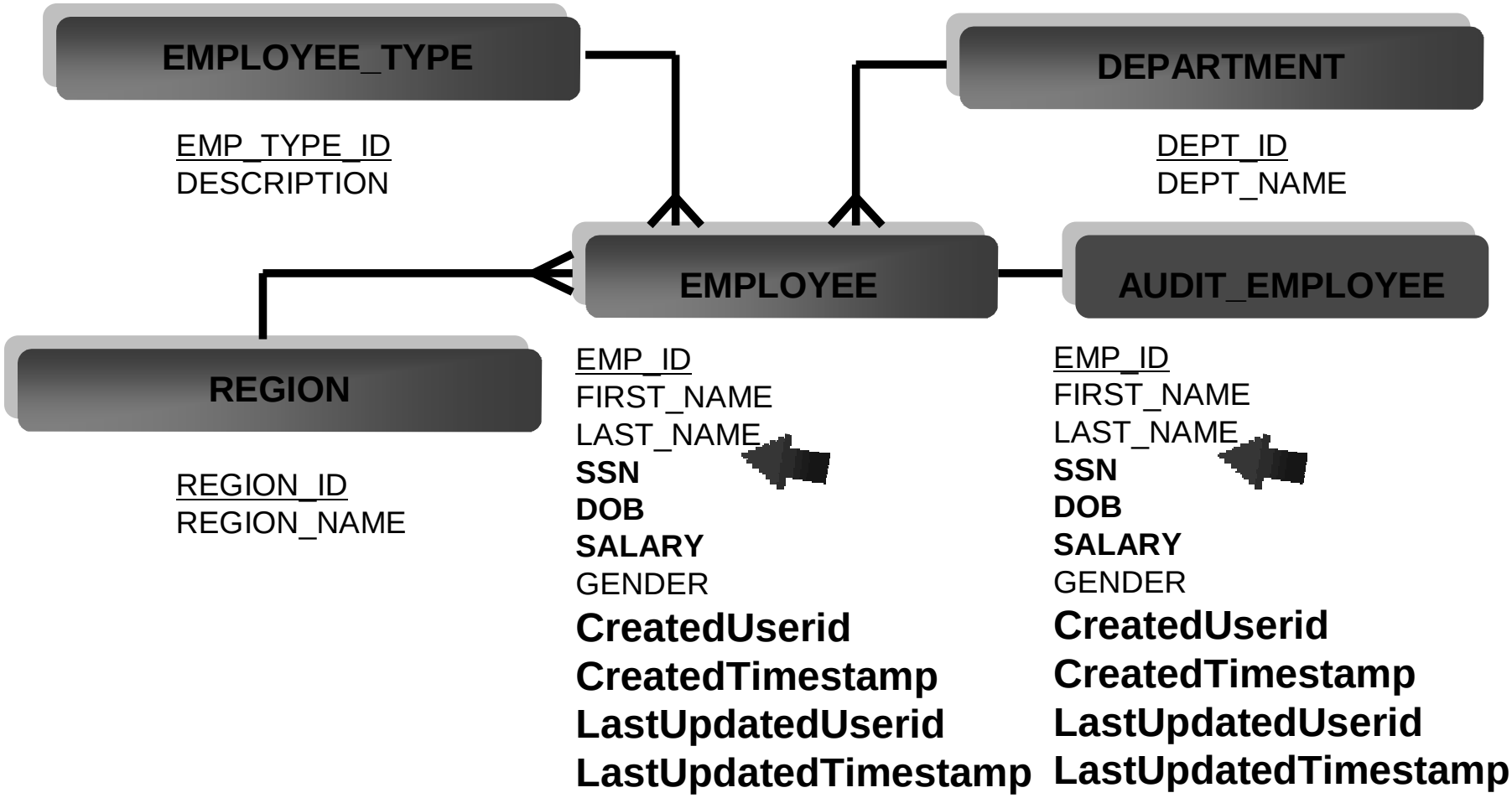
Sample database table with AUDIT columns definitions:

```
CREATE EMPLOYEE TABLE (
EmployeeId              integer         not null,
EmployeeAddress         VARCHAR (40)    not null,
EmployeeSalary          DECIMAL (7,2)   not null,
.
.
CreatedUserid           VARCHAR(128)    not null with default userid,
CreatedTimestamp        TIMESTAMP       not null with default,

LastUpdatedUserid       VARCHAR(128)    not null with default userid,
LastUpdatedTimestamp    TIMESTAMP       not null with default
);
```

Strive for each audit column to be meaningful!

Know Your Data



Who Knows the Data the Best?

1. Data Analysts
2. Business Process Analysts
3. Application Programmers
4. DBAs

Data Analysts and DBAs should be the Auditors best friend…

Minimizing Overhead

- Nothing is free!
- Know what the overhead is on your system
- Employ selective auditing / Know Thy Data!
- Choose the right architecture for you

Strive for each audit record to be meaningful!

Auditing Approaches

- Network traffic monitoring (aka Sniffers)
- Log Recovery Readers
- Triggers
- Application Auditing
- Native Database Transaction Auditing

Network Traffic Monitor

- Misses Server Side access code (SuperUsers)
  - (Direct DB connections, PL/SQL code, access through Synonyms or Materialized or simple Views)
- Misses encrypted network traffic (ssh, native database encryption)
  - Your network is encrypted, isn't it?
- Doesn't require Database Restart (Impact Customers)

Log Recovery Reader

- Database changes are kept in log files
- Platform dependencies
- Available data usually more limited
- **No SELECT (Read) statement auditing**
  - **No HIPAA or PCI Compliance without ACCESS audit trails**

Triggers

- Cause a copy of data to be saved in audit tables upon Insert/Update to defined tables

- Triggers can have high overhead, audit data in tables isn't "secure" or "hardened" from tampering

- **No SELECT (Read) statement auditing**
  - **No HIPAA or PCI Compliance without ACCESS audit trails**

Application Auditing

- May work well if all access is only through the application
- Does not audit activity outside of the application – Business Objects, MS-Access, Excel, Cognos, etc.
- Audit trail is expressed in "application transactions" – not database

Native Database Transaction Auditing

- Incrementally, more overhead (CPU) on Database
- Requires disk space on the Database Server (Compression?)
- Captures **all** database activity per configuration (Application, SQL*Plus, TOAD, Business Objects, Cognos, Excel, direct connections, etc.)
- Capture database activities by IP Address, Domain Name, Host-Name, Logonid, Userid
- Should be implemented selectively!

Extending the Value of Native Database Auditing

- Automated & Simplified Configuration via Graphical User Interface
- Performance Optimized Audit Data Collection
- Automated Space Management
- Audit Reports – Standard & Custom
- Audit Data Must Be Hardened
  - Look for Tamper Evident Seals, Digital Signatures, or other means to make audit data tamper proof

Thinking Like a Criminal

- Gain access
- Get what I want
- Cover my tracks

or …

- Disable controls/triggers
- Get what I want
- Enable controls/triggers

Thinking Like a Criminal

Was this car stripped on the side of the road or in a warehouse?

Prevention

- Eliminate default passwords
- Have complex password rules; (utilize DBMS password mgmt features, they have them!)
- Limit direct connections (outside of the application)
- Employ the "Principle of Least Access" or "POLA"
- Track utilities (backup, restore, export, datapump)
- Track blackout periods and who enabled them
- Keep current with DB security patches:
  - www.microsoft.com/security/
  - www.oracle.com/technology/deploy/security/alerts.htm
  - http://www-306.ibm.com/software/data/db2/support/db2_9/

SUMMARY
10 Questions for Your IT Dept

1. Do we have any default passwords?
2. How would I be automatically notified if an update were made to a financial table?
3. How would I be notified if a user selected 15,000 credit card or SSN numbers?
4. How would I know if a SYSDBA/SYSADM granted this privilege to someone else?
5. How can I guarantee that the audit trail is authentic?

SUMMARY
10 Questions for Your IT Dept

6. How do we log all DBA activity?
7. How do we tie Database transactions to end users (Web IDs, I/P addresses, etc)?
8. How are database structure changes logged?
9. How is GRANT/REVOKE activity logged?
10. How are RDBMS utility functions logged **(backup, restore, export, datapump)?**

QUESTIONS?

Database Auditing for Compliance & Security

Scott Hayes
WWW.DATABASE-BROTHERS.COM
www.Database-Auditing.info

DATABASE-BROTHERS, INC.
Austin, Texas 78726-1708
512-249-2324

dbi
Accountability Starts Here

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

BACKUP SLIDES

- The following slides contain additional details not found in the presentation slides
  - This information is provided as a professional courtesy to our audience members
  - Feel free to read and browse at your discretion

Market data on “The Problem”

- A study conducted by Ponemon Institute covered 14 separate incidents estimates an average cost of $4.8 million per security breach incident, with costs ranging as high as $22 million.
  - **Total cost estimates include the actual cost of internal investigations, outside legal defense fees, notification and call center costs, public relations and investor relations efforts, discounted services offered, lost employee productivity and lost customers.**

More on the Ponemon Institute, LLC Study (2006 Annual Study: Cost of a Data Breach)

- **Total costs: averaged $182 per lost customer record,** an increase of 30% over 2005 results. The average total cost per reporting company was $4.8 million per breach and ranged from $226,000 to $22 million.
- **Direct incremental costs: averaged $54 per lost record,** an 8% increase over 2005 results for unbudgeted, out-of-pocket spending. Includes free or discounted services offered; notification letters, phone calls, and emails; legal, audit and accounting fees; call center expenses; public and investor relations; and other costs.
- **Lost productivity costs: averaged $30 per lost record,** an increase of 100% over 2005 results, for lost employee or contractor time and productivity diverted from other tasks.
- **Customer opportunity costs**: averaged $98 per lost record, an increase of 31% over 2005 results, covering turnover of existing customers and increased difficulty in acquiring new customers. Customer turnover averaged 2% and ranged as high as 7%.
- **Breach location:** Almost **30%** of all reported breaches originated with **external** partners, consultants, outsourcers, or contractors.

Some specific case findings…

Both UNPROVEN and PROVEN Breaches Draw Fines and Suffer Stock Drops:

- In June 2005, **Kaiser Foundation Health Plan**. The California Department of Managed Health Care (DMHC) fined Kaiser $200,000 for exposing private health information of approximately 150 people. The health plan created a web site, containing information on the names, addresses, telephone numbers and lab results of patients, to be used as a testing portal. Kaiser did not receive the prior consent of the affected patients.

- In May 2005, **Time Warner** reported that information, such as names and Social Security numbers, on 600,000 past and present employees of the company were lost while being shipped to an offsite storage facility. The ensuing probe **did not find any unauthorized access or use**. The company paid for credit monitoring services for those whose information had been lost. a Spokeswoman Kathy McKiernan for **Time Warner (down $0.01 to $16.80, Research),** told CNN that the tapes contained names and Social Security information on current and former Time Warner employees and some of their dependents and beneficiaries dating back to 1986. McKiernan said the Secret Service is investigating the matter, working closely with the company and **Iron Mountain Inc. (down $0.38 to $29.32, Research**), the data storage firm that lost the tapes. McKiernan said the investigation has not found any evidence that the tapes or their contents have been accessed or misused.

Some specific case findings…

Both UNPROVEN and PROVEN Breaches Draw Fines and Suffer Stock Drops:

- There was the possibility that the information was accessed by unauthorized people. Compare these two breaches with the well publicized case of **BJ's Wholesale Club**. In early 2005, thieves monitored unencrypted data transmitted over BJ's wi-fi network. The system was furthermore accessible via a default username and password, and thieves gathered the credit and payment card information of BJ's customers. BJ's was alerted by card issuers that its customers were being victimized with fraudulent purchases in their name.

- The FTC investigation revealed that BJ's had not taken reasonable security measures to protect the sensitive information of its customers and had been negligent. BJ's is party to a consent decree with the FTC that requires that they implement a comprehensive security system that will be subject to biannual external audits for the next 20 years.

- According to a May securities and Exchange Commission filing, **BJ's recorded charges of $7 million in 2004 and an additional $3 million in 2005** to cover legal costs incurred in this matter.

CardSystems – Out of Business

- http://www.vnunet.com/vnunet/news/2140332/credit-card-processor-crumbles **CardSystems faces closure after record hack** - Visa and American Express abandon credit card processor following last month's theft. Tom Sanders in California, vnunet.com 26 Jul 2005 - Credit card processor CardSystems is likely to close following last month's theft of 40 million client records. The company lost two of its main customers last week, Visa and American Express. CardSystems chief executive John Perry told the US House of Representatives last week that the firm will "be forced to permanently close its doors" unless the two credit card companies reconsider. Perry testified in a hearing about the security of credit card processing for a subcommittee on financial services. Visa sent a memorandum last week to inform banks that the credit card provider plans to cancel its contract with CardSystems. "In violation of Visa's rules [CardSystems] did not have the appropriate controls in place to protect cardholder information," Rosetta Jones, vice president for Visa, told vnunet.com. "Despite some remediation actions taken by the processor since the initial reporting of the data compromise, Visa cannot overlook the significant harm that the data compromise, and CardSystems' failure to maintain the required security protection, has had on Visa member financial institutions, merchants and cardholders." American Express followed Visa's example, while MasterCard has extended its deadline until 31 August for CardSystems to prove that it complies with the firm's security requirements. In what is believed to be the largest case of identity theft in history, hackers stole 40 million client records from CardSystems' database. MasterCard made the case public after its fraud fighting tools pointed out the hack. CardSystems stored data in such a form that the hackers were able to trace the information back to individual accounts. Perry acknowledged that this was in violation of the security standards demanded by Visa and MasterCard, and testified that the firm no longer stores such 'track data'. The breach of CardSystems' computers dated back to September 2004, when a script was installed on its servers that periodically looked for specific file types. "We know for certain that three files were wrongfully removed from the CardSystems platform," said Perry. The three files contained a total of 263,000 records for 239,000 account numbers.

- http://www.eweek.com/article2/0,1895,1833209,00.asp - **Lawsuit Seeks Payback for Major Credit Card Breach** By Libe Goad June 28, 2005 Following the recent revelation that a security breach potentially exposed 40 million credit cards to data theft, a class-action suit was filed Monday against CardSystems Solutions, MasterCard and Visa on the behalf of California credit card holders and businesses accepting credit card payments. The lawsuit, filed in San Francisco Superior Court, alleges that CardSystems Solutions, an Arizona-based credit card processing company, failed to keep consumers' credit card data safe, breaking Visa and MasterCard's "Data Security Standards," which forbid storing certain consumer information. Also, the suit says CardSystems is liable for the security breach because the company failed to "maintain a proper firewall and computer security system [and failed] to properly encrypt data, [and for] its unauthorized storage of consumer data." The unprotected data purportedly included credit card holder names, credit card account numbers, bank names, information about credit card transactions, magnetic-stripe data, PIN verification codes and "other personal identifying information." The suit also says CardSystems, along with Visa, MasterCard and credit card processor Merrick Bank didn't disclose the information in a timely manner.