Data Security in the Age of Regulatory Compliance

A Webinar Sponsored

by SoftBase

SoftBase

http://www.SoftBase.com

Craig S. Mullins

Mullins Consulting, Inc.

http://www.CraigSMullins.com

Today's Agenda

- An Introduction to Industry and Governmental Regulations
- The Pervasiveness of Data Breaches
- Data and Database Security Techniques for Compliance, Protection, and Control
  - Database Activity Monitoring and Auditing
  - Long-term Data Retention
  - Database Security and Data Encryption
  - Test Data Management
  - Data Masking
  - Data Quality and Metadata Management

An Introduction to Industry and Governmental Regulations

- ***PCI-DSS***
- ***GLB***
- ***HIPAA***
- ***Basel II***
- ***Sarbanes-Oxley***
- ***Many others…***

PCI DSS: Payment Card Industry Data Security Standards

- The PCI DSS was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally.
- All organizations that accept, acquire, transmit, process, and/or store cardholder data must continuously protect cardholder data to the minimum requirements set forth in the PCI DSS.
- Organizations are required to prove compliance and report their compliance status annually.
- Compliance is the continuous state of adhering to the regulatory standard.
  - There are daily (log review), weekly (file integrity monitoring), quarterly (vulnerability scanning), and annual (penetration testing) activities that an organization must perform in order to maintain this continuous state of compliance.

GLB: Gramm-Leach-Bliley Act

- The Gramm-Leach-Bliley Act (GLB Act), also known as the Financial Modernization Act of 1999, is a federal law enacted in the United States to control the ways that financial institutions deal with the private information of individuals.
- The Act consists of three sections:
  - The Financial Privacy Rule, which regulates the collection and disclosure of private financial information;
  - The Safeguards Rule, which stipulates that financial institutions must implement security programs to protect such information;
  - and the Pretexting provisions, which prohibit the practice of pretexting (accessing private information using false pretenses).
- The Act also requires financial institutions to give customers written privacy notices that explain their information-sharing practices.

HIPAA: Health Insurance Portability and Accountability Act

- **The HIPAA Privacy Rule creates national standards to protect individuals' medical records and other personal health information and to give patients more control over their health information.**
- **The Privacy Rule provides that, in general, a covered entity may not use or disclose an individual's healthcare information without permission except for treatment, payment, or healthcare operations.**
- **The Privacy Rule requires the average healthcare provider or health plan to do the following:**
  - **Notify patients about their privacy rights and how their information can be used.**
  - **Adopt and implement privacy procedures for its practice, hospital, or plan.**
  - **Train employees so that they understand privacy procedures.**
  - **Designate an individual to be responsible for seeing that privacy procedures are adopted and followed.**
  - **Secure records containing individually identifiable health information so that they are not readily available to those who do not need them.**

BASEL II

- **Basel II is a round of deliberations by central bankers from around the world, under the auspices of the Basel Committee on Banking Supervision (BCBS) in Basel, Switzerland.**
  - **Goal: to produce uniformity in the way banks and banking regulators approach risk management across national borders.**
- **The New Basel Capital Accord is about improving risk & asset management to avoid financial disasters. Three pillars of Basel II:**
  1. **minimum capital requirements**
  2. **supervisory review; and**
  3. **market discipline - to promote greater stability in the financial system.**
- **Compliance requires all banking institutions to have sufficient assets to offset any risks they may face, represented as an eligible capital to risk aggregate ratio of 8%.**
- **Part of this compliance dictates data capture requirements and that financial institutions must have three years of data on file by 2007.**

SOX: Sarbanes-Oxley Act

- **The U.S. Public Accounting Reform and Investor Protection Act of 2002**
  - **"...to use the full authority of the government to expose corruption, punish wrongdoers, and defend the rights & interests of American workers & investors."**
  - **Impacts auditors, corporations, and IT**
    - **Public companies with a market capitalization of at least $75M**
    - **Companies listed on a United States exchange even if they are incorporated outside of the United States**
  - **The primary objectives of SOX:**
    - **To strengthen and restore public confidence in corporate accountability and the accounting profession;**
    - **To strengthen enforcement of the federal securities laws;**
    - **To improve executive responsibility;**
    - **To improve disclosure and financial reporting; and**
    - **To improve the performance of "gatekeepers."**

SOX Section 404:
Management Assessment of Internal Controls

- **Section 404 is the largest driver of SOX projects**
  - It is the most important section for IT because the processes and internal controls are implemented primarily in IT systems;
  - …*and* most of the data is stored in a DBMS.
- **Requires CEOs, CFOs, and outside auditors to attest to the effectiveness of internal controls for financial reporting**
  - 404 requires external auditor's opinion on effectiveness of internal controls
  - Ability to demonstrate controls implemented for quarterly certification
  - If controls can be bypassed, management cannot *with certainty* attest to integrity, confidentiality and non-repudiation of financial reporting
  - Standards and repeatability are critical in demonstrating controls for data integrity

Other Regulations?

- Of course, there are other regulations that need to be considered, for example:
  - CA SB 1386
  - FDA 21 CFR 11 (http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/cfrsearch.cfm?cfrpart=11)
  - Can SPAM Act of 2003
  - E-Government Act → FISMA: Federal Information Security Act
  - The Data Quality Act
  - FRCP: Federal Rules of Civil Procedure
- Regulations have brought to light some of the personal financial information that has been compromised (stolen)
- And, there are more regulations to contend with; based upon your industry, location, etc.
- And, new regulations will continue to arise over time…

Compliance is an On-going Concern

- Regulatory compliance cannot be ensured by a single project
- Regulations change… businesses change… systems change
- Compliance needs to become part of the business and therefore, part of IT

Regulations Impacting Security
Governance vs. Privacy

Governance

1. *Basel II*
2. *Sarbanes Oxley*
3. *OFAC*
4. *Turnbull Report*

Protect and control the process

Privacy

1. *EU DPD*
2. *AU/NZ NPP*
3. *SB 1386/AB 1950*
4. *GLBA*
5. *HIPAA*
6. *PCI-DSS*
7. *FCRA -- “Red Flag”*

Protect the data

Data Breaches

- **Regulations have brought to light many of the personal and financial information and data that has been compromised, breached, or stolen**
- **A few recent examples include:**
  - **Reyes Beverage Group – SSN and names exposed – January 4, 2013**
  - **King Drug & Home Care – SSN, names, medical data – January 3, 2013**
  - **State of California Department of Health Care Services – beneficiary information mailed to wrong addresses – December 24, 2012**
  - **Women & Infants Hospital – unecrypted backup tapes missing exposing patient names, date of birth, physicians' names, and other medical information – November 6, 2012**
  - **Symantec - Names, phone numbers, emails, domains, passwords, usernames, and other information exposed – November 4, 2012**
  - **Cornell University – SSN and names exposed – November 2, 2012**
  - **HSBC Bank USA – an employee resigned and left with customer account information – October 30, 2012**

Data Breaches

Privacy Rights Clearinghouse
Empowering Consumers. Protecting Privacy.

According to the Privacy Rights Clearinghouse, the total number of records containing sensitive personal information involved in security breaches in the U.S. since January 2005 is:

605,791,404

3553 breaches

As of January 10, 2013

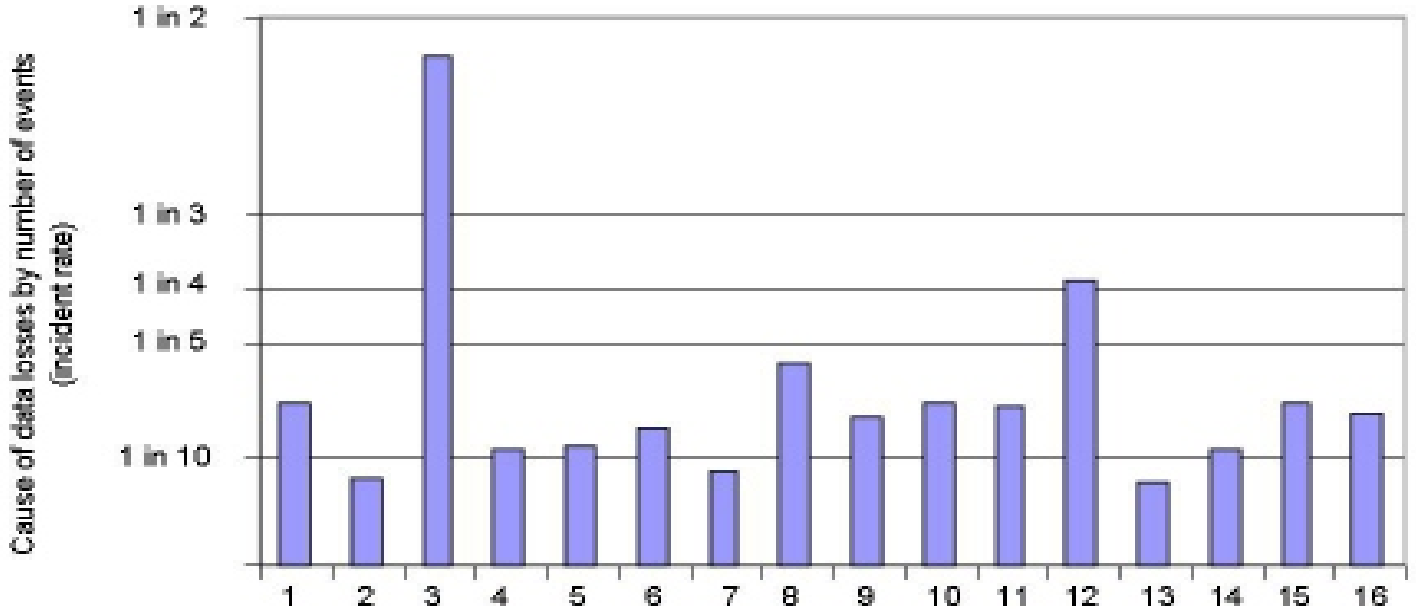
https://www.privacyrights.org/data-breach

Compromised Assets %

Asset	Asset Group	% of Breaches	% of Records
POS system	Online Data	32%	6%
Database server	Online Data	30%	75%
Application server	Online Data	12%	19%
Web server	Online Data	10%	0.004%
File server	Online Data	8%	0.1%
Public kiosk system	Online Data	2%	0.4%
Authentication / Directory server	Online Data	2%	0.1%
Backup tapes	Offline Data	1%	0.04%
Documents	Offline Data	1%	0.000%
Workstation	End-User System	8%	0.01%
Laptop	End-User System	4%	0.000%
PIN Entry Device	End-User System	2%	0.004%

Source: 2009 Data Breach Investigations Report, Verizon Business

Most Prevalent Causes of Data Loss



1: Lost or stolen laptops
2: Improperly disposed of computer equipment
3: User errors
4: Improperly transferred backup media
5: Inappropriate access to IT resources
6: Insufficient controls in business procedures
7: Insufficient controls on IT procedures
8: Internet threats, attacks and hacks
9: Employee manipulation and malfeasance
10: Accidental damage to computing equipment
11: Inappropriate usage of IT resources
12: Violation of policies
13: Unauthorized access to IT resources
14: Insufficient auditing, monitoring and reporting
15: IT vulnerabilities
16: Insufficient IT controls

N: 201

Source: ITPolicyCompliancecom, 2007

Poll question 2

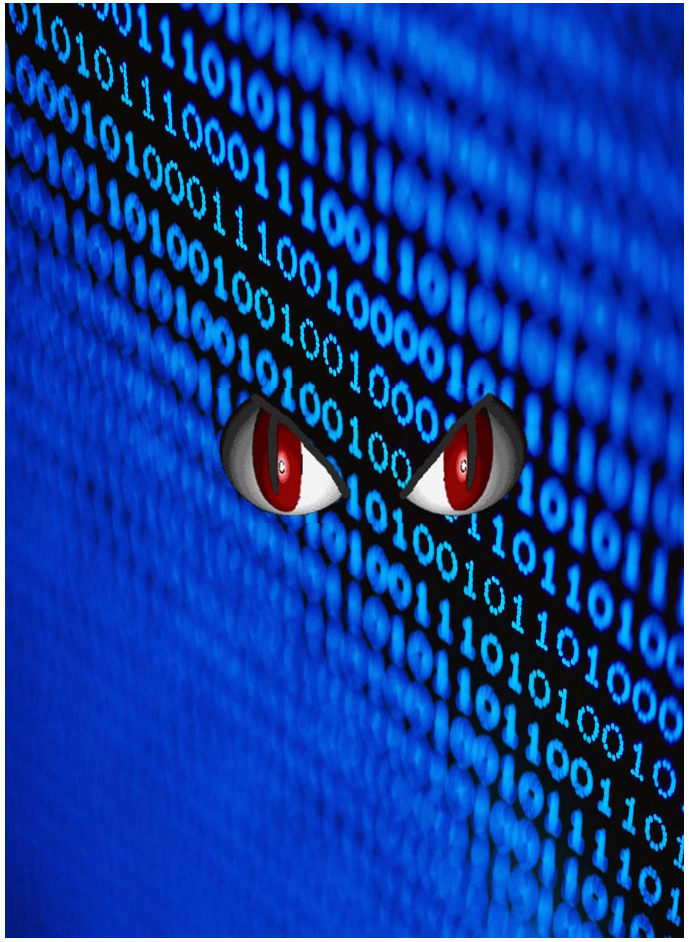
Database-Related Security & Compliance Techniques and Issues

- Database Activity Monitoring and Auditing
- Long-term Data Retention
- Database Security and Encryption
- Test Data Management
- Data Masking
- Data Quality and Metadata Management

Database Activity Monitoring and Database Auditing

- The process of monitoring access to and modification of selected database objects and resources within operational databases and retaining a detailed record of the access where said record can be used to proactively trigger actions and can be retrieved and analyzed as needed.
- There are many names applied to the discipline of database auditing:
  - Data Access Auditing
  - Data Monitoring
  - Data Activity Monitoring (DAM)
- Quick way to remember this topic:

Who did what to which data when and how did they do it?



Top Regulations Impacting DB Security

Audit Requirements	SOX (CobiT)	PCI DSS	HIPAA	CMS ARS	GLB	Basel II (ISO 17799)	FISMA (NIST 800-53)
1. Access to Sensitive Data **(Successful/Failed SELECTs)**		☆	☆	☆	☆	☆	☆
2. Schema Changes (DDL) **(Create/Drop/Alter Tables, etc.)**	☆	☆	☆		☆	☆	☆
3. Data Changes (DML) **(Insert, Update, Delete)**	☆			☆		☆	
4. Security Exceptions **(Failed logins, SQL errors, etc.)**	☆	☆	☆	☆	☆	☆	☆
5. Accounts, Roles & Permissions (DCL) **(GRANT, REVOKE)**	☆	☆	☆	☆	☆	☆	☆

Database and Data Access Auditing

- **An audit is an evaluation of an organization, system, process, project or product.**
  - **Database Control Auditing**
    - **Who has the authority to…**
  - **Database Object Auditing**
    - **DCL: GRANT, REVOKE**
    - **DDL: CREATE, DROP**
  - **Data Access Auditing**
    - **INSERT, UPDATE, DELETE**
    - **SELECT**

Database Auditing Approaches

- What methods are available?
  - Audit trails (columns) in tables
  - Audit within the DBMS (traces)
    - Must start performance trace
      - Overhead as trace records are written by the DBMS
    - DDL changes required to traced tables
    - DB2 10 for z/OS Audit Trace details are available in Chapter 11 of the DB2 Admin Guide
  - Audit from the database transaction log files
    - Modifications are on the log anyway so…
  - Audit over the network
    - Capture SQL requests as they are sent over the network
    - What about non-network requests? (e.g. CICS w/DB2)
  - Audit directly against the DBMS server *(software tap)*

DBA Auditing

- One of the biggest needs for database auditing is privileged user (ie. DBA) auditing?
- In other words, who watches the watchers?
  - *Trust, but verify*
- Super users (SYSADM, DBADM)
  - Can do anything to any data
  - Database auditing can be used to verify the integrity and accuracy of the DBA group

On the Need to Monitor Privileged Users

TECH DISPENSER
Tech blogs filtered by humans, *not* bots

COMPUTERWORLD
Security

IDG

JMP TO More Resources

SEARCH Google™ Custom Search GO

Home
News
E-mail Newsletters
Tech Dispenser
Shark Bait
Knowledge Centers
- Operating Systems
- Networking & Internet
- Mobile & Wireless
- Security
  - Cybercrime & Hacking
  - Spam, Malware & Vulnerabilities
  - Security Hardware & Software
  - Standards & Legal Issues
  - Privacy
  - Intellectual Property & DRM
  - Disaster Recovery
- Storage
- Business Intelligence
- Servers & Data Center
- Hardware
- Software

Database admin steals 2.3M consumer records at Fidelity National subsidiary

The data included names, addresses, birth dates, bank account and credit card information

Jaikumar Vijayan Today's Top Stories ▸ or Other Security Stories ▸

Comments (12) Recommendations: 60 — Recommend this article

July 03, 2007 (Computerworld) -- Call it the case of hiring a fox to guard the hen house. A senior database administrator at a subsidiary of Fidelity National Information Services Inc. who was responsible for defining and enforcing data access rights at the company instead took data belonging to about 2.3 million consumers and sold it to a data broker.

The broker in turn sold a subset of the data to other marketing companies. The stolen data included names, addresses, birth dates, bank account and credit card information, the company said in a **statement** released today.

For the moment at least, it appears that the companies that bought the information have mainly used the data to send marketing solicitations to affected individuals, Fidelity said in its statement.

Fidelity National Information Services describes itself as a provider of "core financial institution processing, card issuer and transaction processing services, mortgage loan processing and related information products and outsourcing services to financial institutions,

MORE RELATED CONTENT
- Data breach? Here's what to do, when and how
- Survey: Most insider-related data breaches go unreported
- Just how much will that data breach cost your company?

TODAY'S TOP STORIES
- Extreme energy makeover: Home office edition
- Exploit code out for Oracle Database 10g vulnerability
- Update: Buggy game DRM puts Windows users at risk

Database Auditing
The Bottom Line

- Database auditing requirements go far beyond the capabilities of today's DBMS software
- Log analysis software does not solve access auditing requirements
- Network sniffing does not provide sufficient auditability for mainframe databases
- Long-term proof of database access not viable without archival of audit surveillance details
- Separation of duties is important
- Be sure to meet the needs of all stakeholders: security operations, compliance/audit, application and DBA

Long-Term Data Retention

- **From the beginning of recorded time until 2003, we created 5 exabytes of data.**
  - **5 billion gigabytes**
- **In 2011 the same amount of data was created every two days.**
- **In 2013, it is expected that the same amount will be created every 10 minutes.**

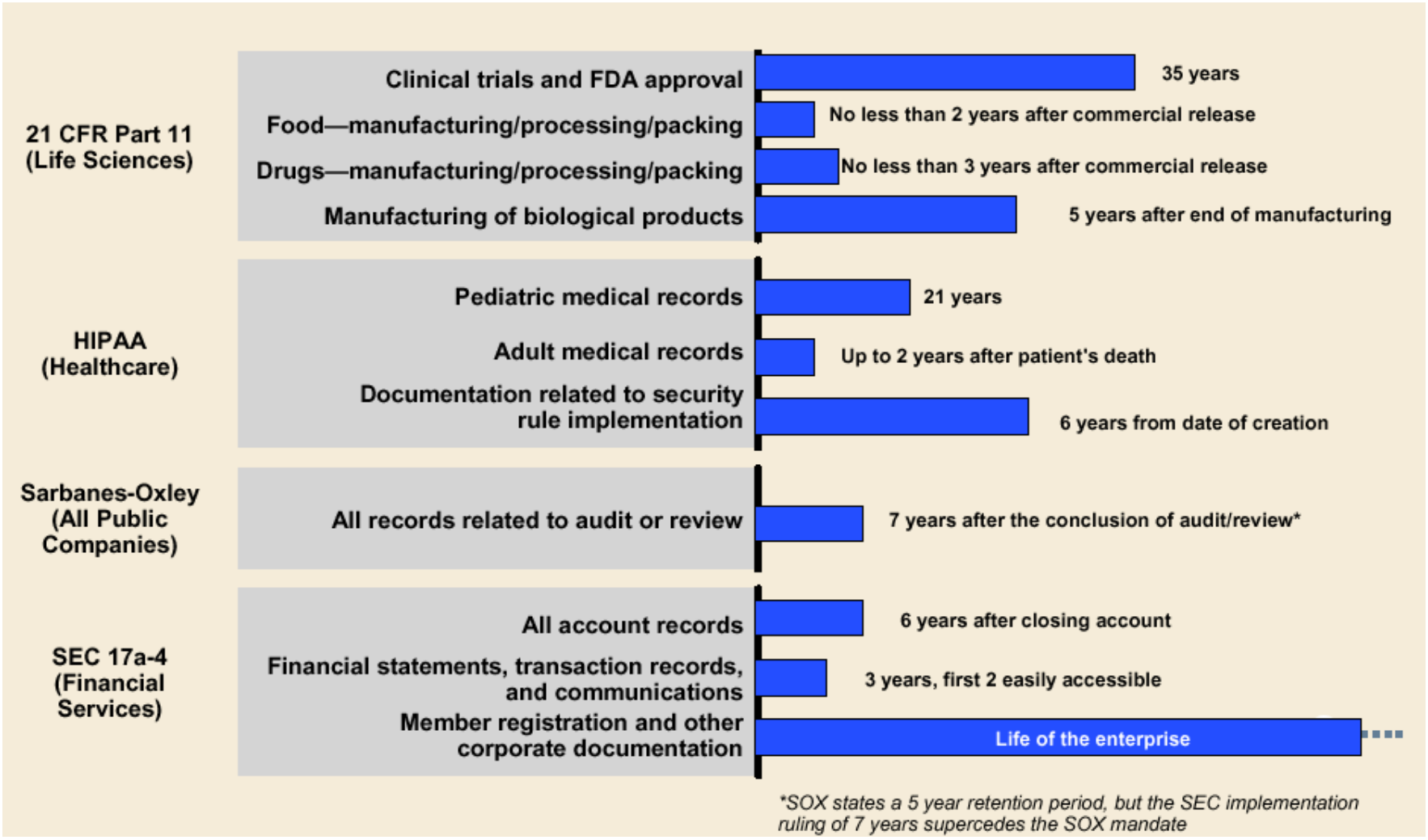
The average installed storage capacity at Fortune 1000 corporations was projected to grow by 24% in 2011.

Data Retention Requirements Drive Data(base) Archiving Needs

- **Data Retention Requirements** refer to the length of time you need to keep data
  - Determined by laws – regulatory compliance
    - *More than 150 state and federal laws dramatically increasing retention periods for corporate data*
    - *The Storage Networking Industry Association surveyed* data retention specialists and reported that 80% of respondents have information they must keep over 50 years and 68% of respondents said they must keep it over 100 years*
      - ✓ *The same study indicated that database information was considered to be most at risk of loss.*
  - Determined by business needs
    - *Reduce operational costs: large volumes of data interfere with operations: performance, backup/recovery, etc.*
    - *Isolate content from changes: protect archived data from modification*

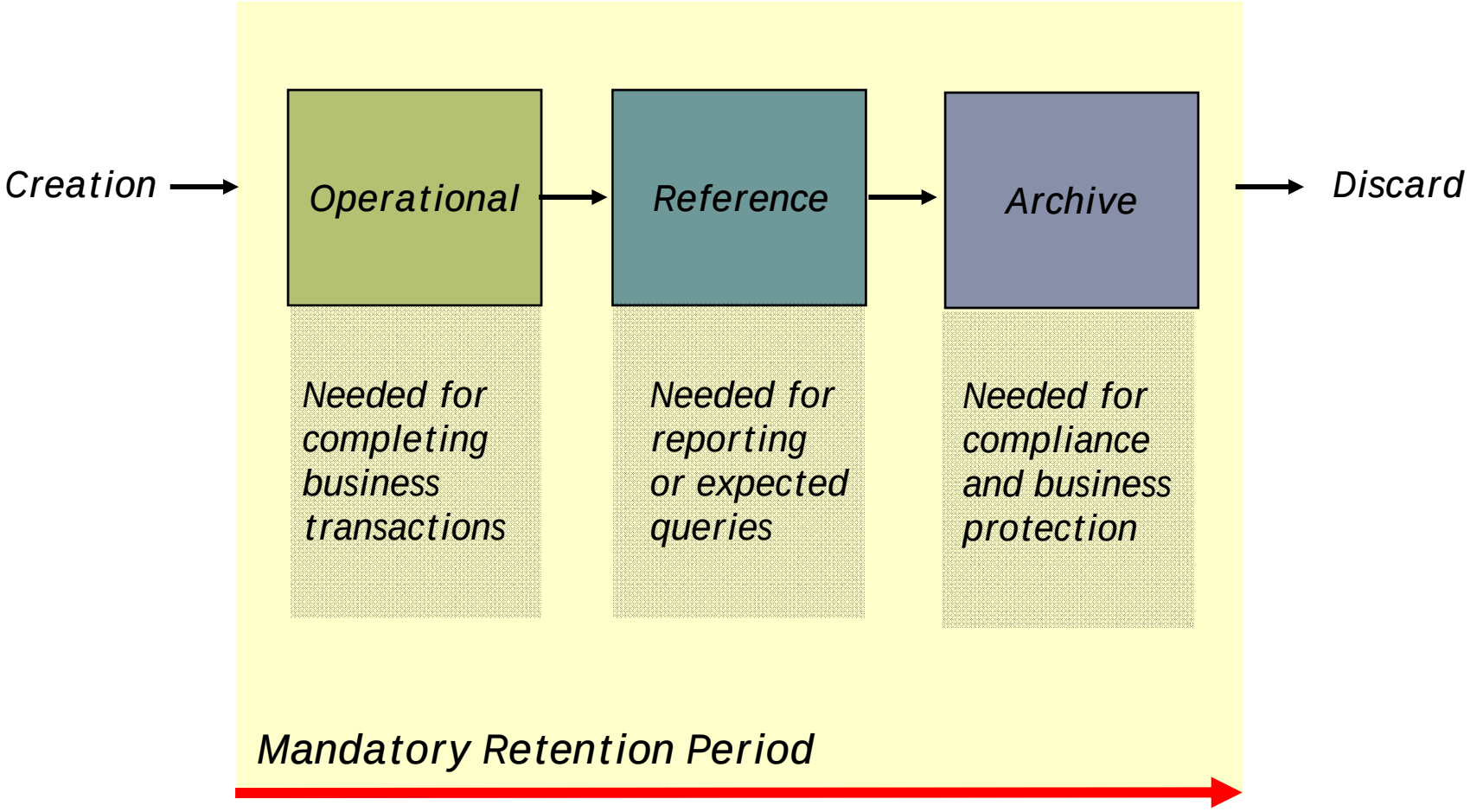
** SNIA Data Management Forum - 100 Year Archive Requirements Survey*

Sample Data Retention Requirements



The Lifecycle of Data

***Database Archiving**: The process of removing selected data records from operational databases that are not expected to be referenced again and storing them in an archive data store where they can be retrieved if needed.*



Requirements for Database Archiving

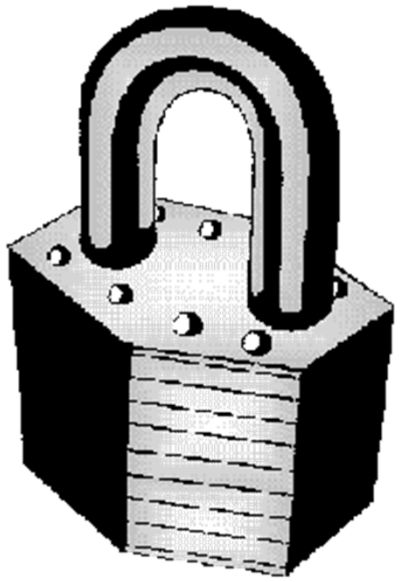
- Policy based archiving: logical selection
- Keep data for very long periods of time
- Store very large amounts of data in archive
- Maintain archives for ever changing operational systems
- Independent from Applications/DBMS/Systems
- Independent from Operational Metadata
- Protect authenticity of data – no changes!
- Access data directly in the archive when needed; as needed
- Discard data after retention period

Why Archiving Can Help to Prevent Data Breaches

- Data is removed from the database
  - If the database is breached, the archived data is not because it is no longer there
- Data cannot be accessed by SYSADM
  - ...or any other database users
- Data is protected against modification
  - Archived data cannot be changed

Data and Database Security

- **75% of enterprises do not have a DBMS security plan.**
- **A single intrusion that compromises private data can cause immense damage to the reputation of an enterprise — and in some cases financial damage as well.**
- **Database configurations are not secure by default, and they often require specialized knowledge and extra effort to ensure that configuration options are set in the most secure manner possible.**



Source: Forrester Research,

Database Security Issues in a Nutshell

- **Authentication**
  - Who is it?
- **Authorization**
  - Who can do it?
- **Encryption**
  - Who can see it?
- **Audit**
  - Who did it?

A Few Database Security Issues

- **Who has access to high-level "roles":**

  Install SYSADM, SYSADM, SYSCTRL, DBADM, etc.

- **Auditors will have issues with this, but it can be difficult to remove all of them**
  (more on this in a moment)
- **Do any applications require DBA-level authority? Why?**
- **Security monitoring**
  - **Audit from the log or an appliance**
  - **Prediction**

SYSADM and Install SYSADM

- **Install SYSADM bypasses the DB2 Catalog when checking for privileges.**
  - **So, there are no limits on what a user with Install SYSADM authority can do.**
  - **And it can only be removed by changing DSNZPARMs**
  - **Basically, needed for catalog and system "stuff"**

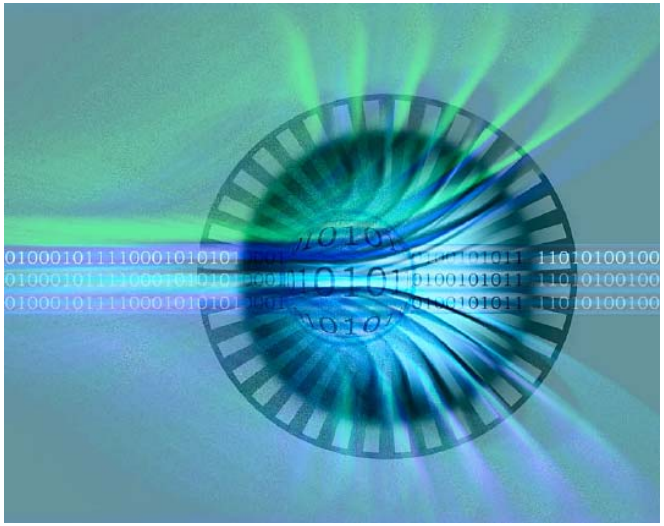
- **SYSADM is *almost* as powerful, but:**
  - **It can be revoked**
  - **Biggest problem for auditors: SYSADM has access to all data in all tables.**

Suggestions

- **Limit the number of SYSADMs**
  - **And audit everything those users do.**
    (We'll discuss auditing issues next)
- **Consider associating Install SYSADM with a RACF group**
  - **Authids that absolutely need Install SYSADM can be connected to the RACF group using secondary authids.**
  - ***similar issues with SYSOPR and Install SYSOPR***
- **DB2 10 for z/OS**
  - **New security option: SECADM**
  - **DBADM without access to the data**
- **Encrypt sensitive data**

Data Encryption Considerations

- **Why encryption is helpful:**
  - **It doesn't matter if encrypted data becomes public because the data is not readable and it is near impossible to decrypt it without the key.**



- **Types of encryption:**
  - **At Rest**
  - **In Transit**
- **Possible issues:**
  - **Performance**
    - **Encrypting and decrypting data consumes CPU**
  - **Applications *may* need to be changed**
    - **See next slide for DB2 V8 encryption functions**

DB2 V8: Encryption / Decryption

- **Encryption: to encrypt the data for a column**

```
ENCRYPT_TDES(string, password, hint)
```

  - **ENCRYPT_TDES [can use ENCRYPT() as a synonym for compatibility]**
  - **Triple DES cipher block chaining (CPC) encryption algorithm**
    - **Not the same algorithm used by DB2 on other platforms**
  - **128-bit secret key derived from password using MD5 hash**

```
INSERT INTO EMP (SSN)
VALUES(ENCRYPT('289-46-8832','TARZAN','? AND JANE'));
```

- **Decryption: to decrypt the encrypted data for a column**

```
DECRYPT_BIT(), DECRYPT_CHAR(), DECRYPT_DB()
```

  - **Can only decrypt expressions encrypted using ENCRYPT_TDES**
    - **Can have a different password for each row if needed**
  - **Without the password, there is no way to decrypt**

```
SELECT DECRYPT_BIT(SSN,'TARZAN') AS SSN FROM EMP;
```

DB2 9 for z/OS: Encryption in Transit

- DB2 9 supports SSL by implementing z/OS Communications Server IP Application Transparent Transport Layer Security (AT-TLS)
- AT-TLS performs transport layer security on behalf of DB2 for z/OS by invoking the z/OS system SSL in the TCP layer of the TCP/IP stack
- When acting as a requester, DB2 for z/OS can request a connection using the secure port of another DB2 subsystem
- When acting as a server, and from within a trusted context SSL encryption can be required for the connection

Test Data Management

- **Test Data Management is fundamental to the success of your data and compliance strategy.**
  - **Data drives the testing process.**
  - **Bad data results in poor testing, untrustworthy results, and wasted time, effort and money.**
- **Furthermore, all of the issues that apply to production data apply to test data… especially if it is created from production data.**

Test Data Management Issues

- Test data generation
  - From production or from scratch
  - Full production volume vs. subset
  - Appropriateness for testing
  - Referentially intact data
- Test data management
  - Reusability of test bed
- Data confidentiality
  - Data masking techniques

On the Importance of Test Data Management

Wednesday, January 2, 2013 | TRAFFIC | 41°F

Follow us:

The Seattle Times
Winner of a 2012 Pulitzer Prize

Local News

Search

Advanced Search | Events & Venues | Obituaries

Home | News | Business & Tech | Sports | Entertainment | Living | Homes | Travel | Opinion | Jobs | Autos | Classifieds | Weekly Ad

IN THE NEWS: 'Fiscal cliff' avoided | Widening I-5 | Minimum-wage gap | SPD Twitter | Rose Bowl

Originally published Sunday, December 30, 2012 at 7:42 PM

Casino customers' personal data stolen

Some customers of Skagit Valley Casino Resort can qualify for credit-report monitoring after their personal information was stolen from one of the casino's vendors.

Share:

Recommend 2

Comments (6)

E-mail article

Print

By Kate Martin
Skagit Valley Herald

BOW, Skagit Valley — Some customers of Skagit Valley Casino Resort can qualify for credit-report monitoring after their personal information was stolen from one of the casino's vendors.

The unencrypted customer information was stolen from a Bally Technologies software engineer's home office, said Harry Chesnin, general counsel for the Upper Skagit Indian Tribe. The tribe owns and operates Skagit Valley Casino Resort.

Information was sent to Bally to be tested with new technology, he said. That information is usually encrypted with a computer program, Chesnin said, but some of the information was not encrypted.

MOST POPULAR COMMENTS

HIDE / SHOW COMMENTS

> engineer's apartment in the Las Vegas area was broken into But ... isn't what... (December 31, 2012, by unkanny) MORE

Most likely just a very small subset of the data used to populate a test database so... (December 31, 2012, by billmr) MORE

Statiscially that "private" information is on about 100 different home... (December 31, 2012, by Don Squeek) MORE

Read all 6 comments ▸ Post a comment ▸

SECTION SPONSOR

Fund For The Needy
100% goes directly to non-profits serving some of the most vulnerable members of our community — children, families and seniors.

ADVERTISING

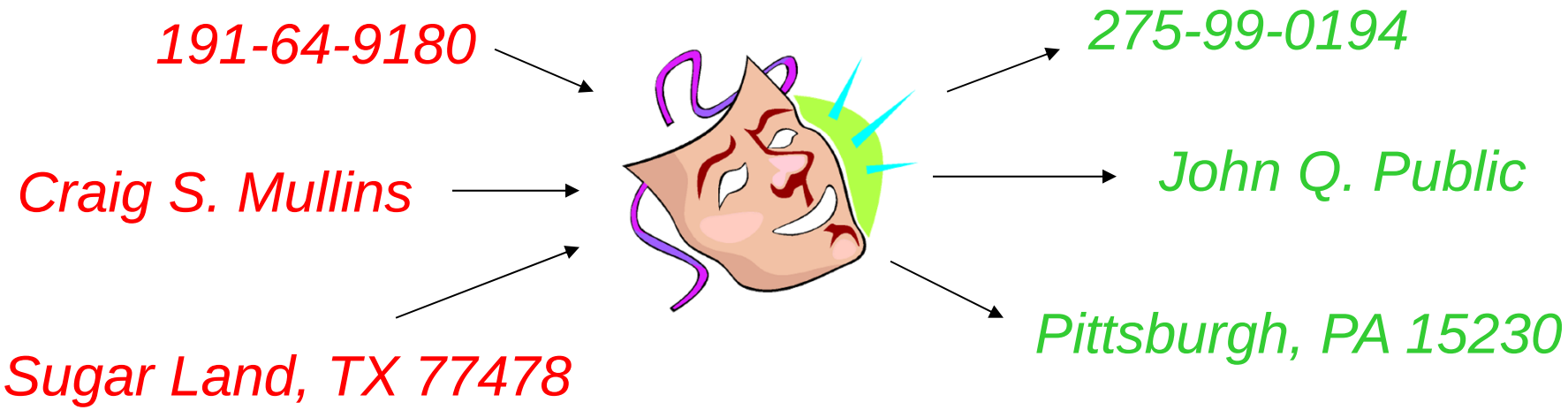
Data Masking

obfuscation

- **Data masking is the process of protecting sensitive information in non-production databases from inappropriate visibility.**
- **Valid production data is replaced with useable, referentially-intact but incorrect and invalid data.**
- **After masking, the test database is usable just like production; but the information content is secure.**

Data Masking *in action*

- **Data Masking can be performed on PII:**
  personally identifiable information



What PII Might Need to be Masked?

Social Security Numbers

Health Records

Driver's License Numbers

Disability Status

Citizenship

Birth Dates

Ethnicity

Payment Data

Names

Phone Numbers

Mailing Addresses

Account Balances

E-mail Addresses

ACH Numbers

Income data

Credit Card Expiry

Bank Account Numbers

Credit Card Numbers

Veteran Status

Facial Photographs

Certificate or License Numbers

Credit Rating

Types of Masking

Data Masking Techniques

Popular Options

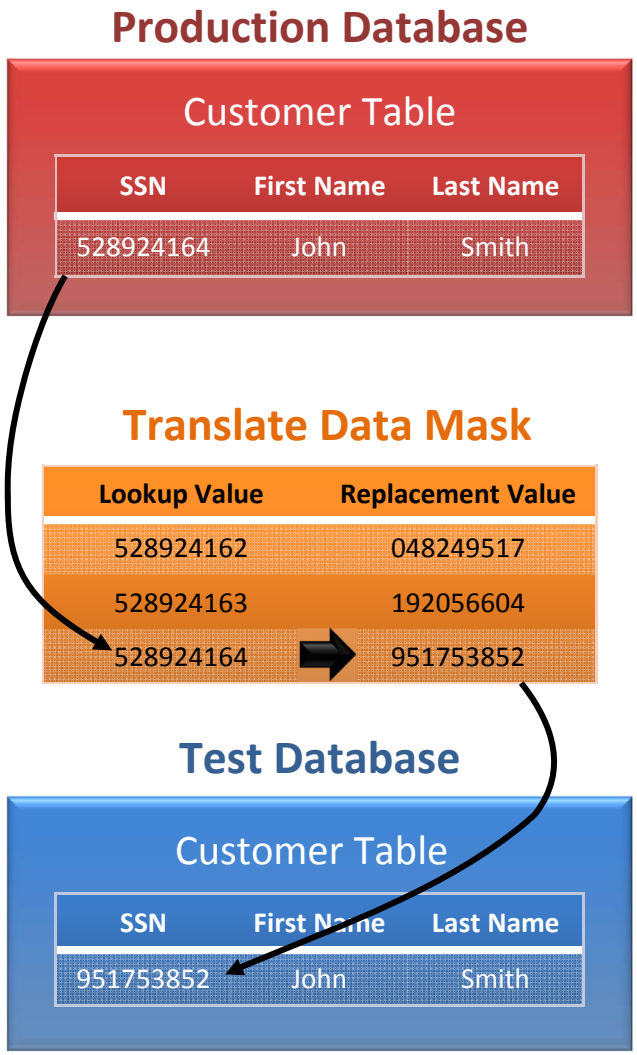
- Translate - Use Translate Value
- Jumble - Jumble Data Positions
- Random Amount - Calculate Random Value
- Supplied Values Tables - (create or use pre-installed)

Advanced Options

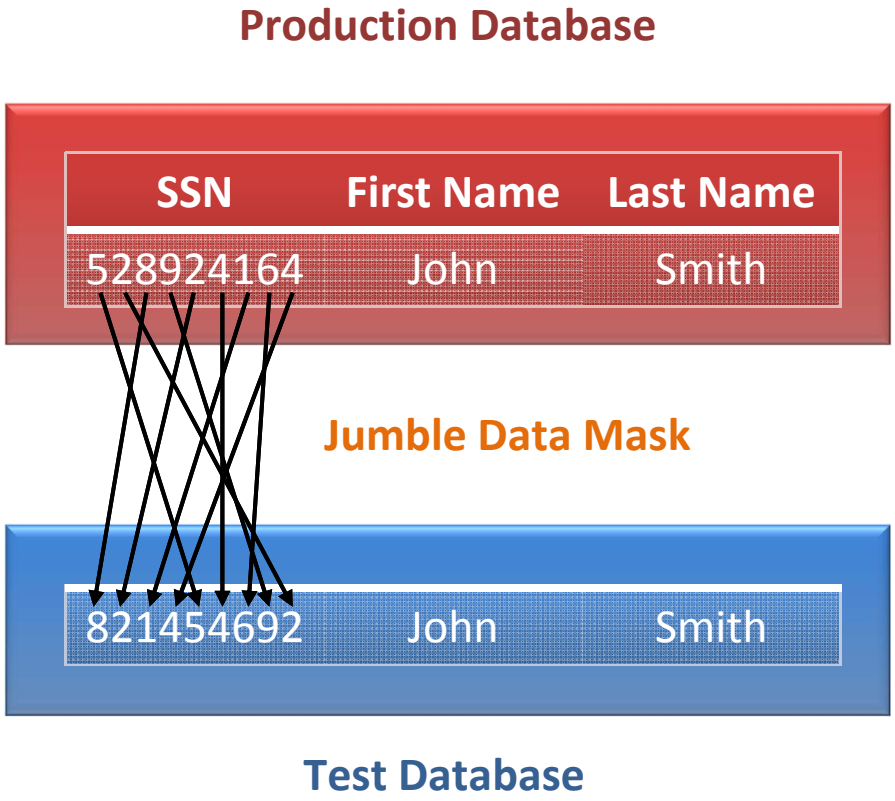
- Referential Masking
- Data Consistency Masking
- 'Delay‘ Masking
- Masking via Exit Routines
- Date Aging Masking
- Data Driven Data Masking

All of these data masking techniques are supported by SoftBase’s TestBase product

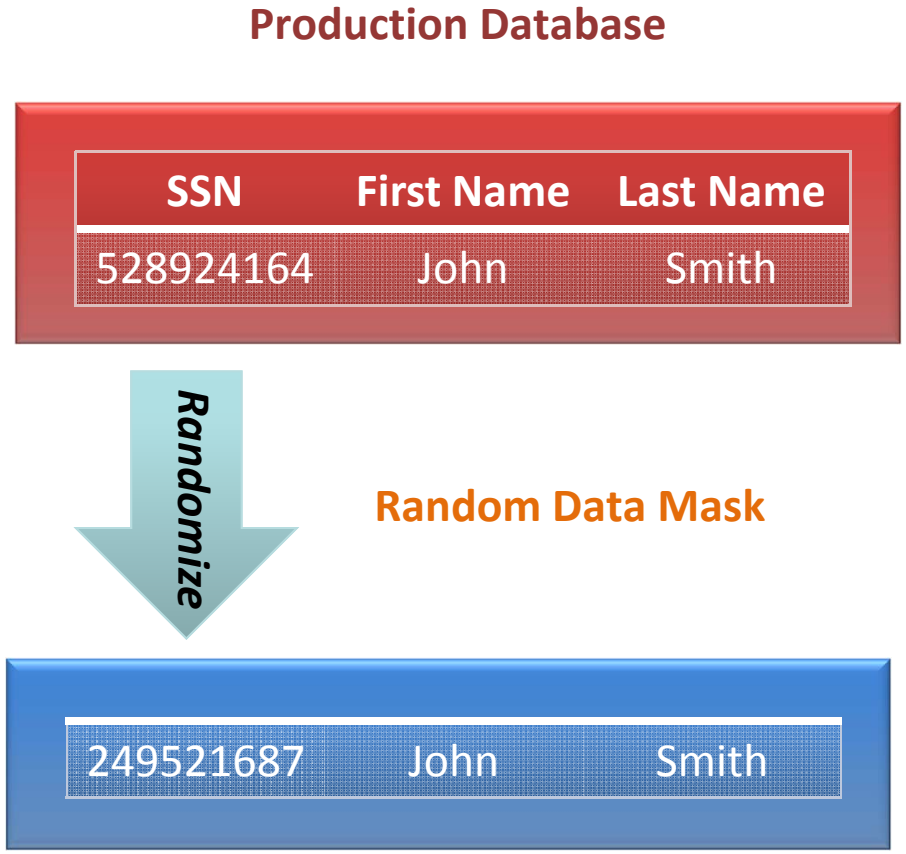
Translation Masking



Jumble Masking

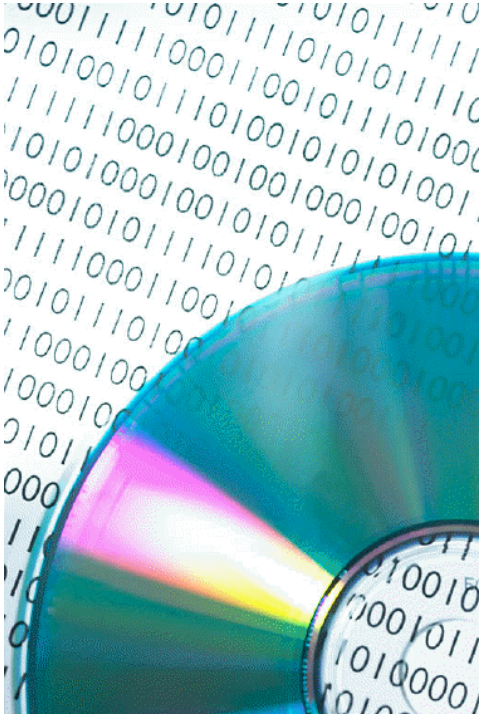


Random Masking



How Data Masking Protects Against Data Breaches

- **If the data has been sanitized by masking it, it won't matter if thieves gain access to it.**



SoftBase's TestBase Offering

A Complete Test Data Management Solution

DB2 Slice

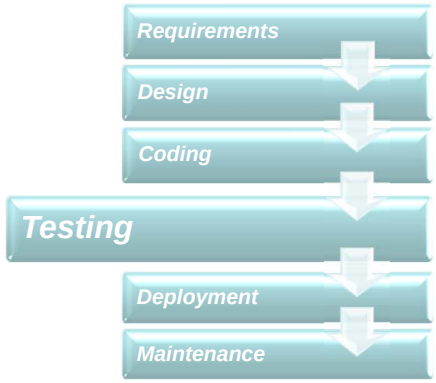
- Allows each tester or group of testers to extract and refresh their own test data without impacting others
- Completely eliminates data corruption and single threading of testing tasks, reducing overall testing time and resources

DB2 Database Population

- Enables DBAs and developers to retrieve manageable subsets of referentially intact data for testing new or updated applications
- Only product to totally eliminate risk of data privacy violations when moving production data to test area, ensuring compliance with Privacy Regulations (e.g. PCI DSS)

DB2 Data Edit

- Allows developers to configure test data for specific testing conditions, improving testing time

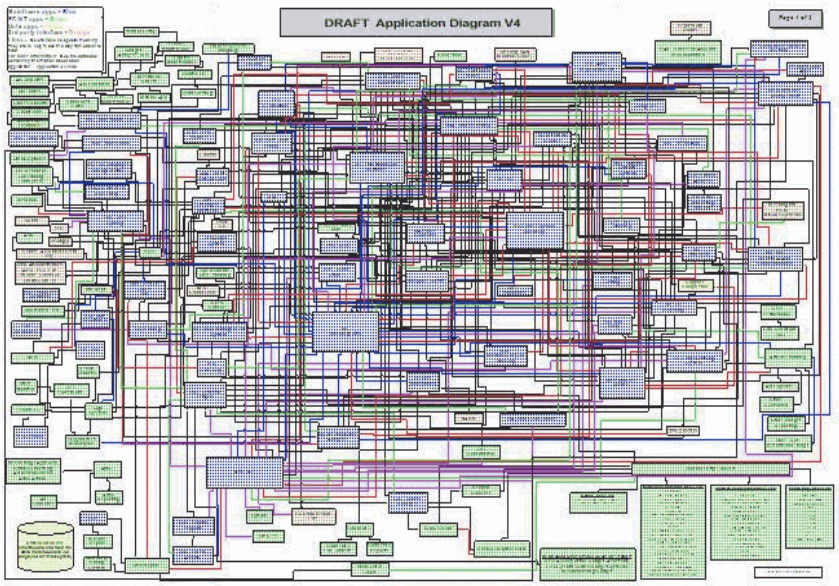


Poll questions 3 and 4

Data Quality

- **A SAS/Risk Waters Group survey indicated that 93% of respondents had experienced losses of $10 million in one year…**
  - **And 21% of respondents said that at some point, their company suffered a loss between $10,000 and $1,000,000 in a single day.**

- **The prime reasons given for such losses were *incomplete, inaccurate or obsolete data*, and inadequate processes.**



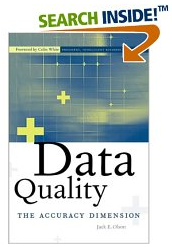
Examples of Data Quality Regulations

- **The Data Quality Act**
  - Careful, it sounds better than it actually is.
  - Written by an industry lobbyist and slipped into a giant appropriations bill in 2000 without congressional discussion or debate
  - Basically consists of two sentences directing the OMB to ensure that all information disseminated by the federal government is reliable.
- **Sarbanes-Oxley**
  - Financial reports must be ACCURATE
  - Without good data quality this is impossible.

Data Quality: Is it Really a Major Concern?

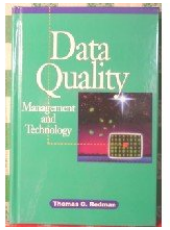
- **How good is your data quality?**
  - **The cost of poor quality is usually hidden and not obvious to those not looking for it.**

    Source: Jack Olsen, *Data Quality: The Accuracy Dimension*, (Morgan Kaufmann).



- **Estimates show that, on average, data quality is suspect:**
  - **Payroll record changes have a 1% error rate;**
  - **Billing records have a 2-7% error rate, and;**
  - **The error rate for credit records: as high as 30%.**

    Source: Thomas C. Redman, *Data Quality: Management and Technology*, (Bantam Books).

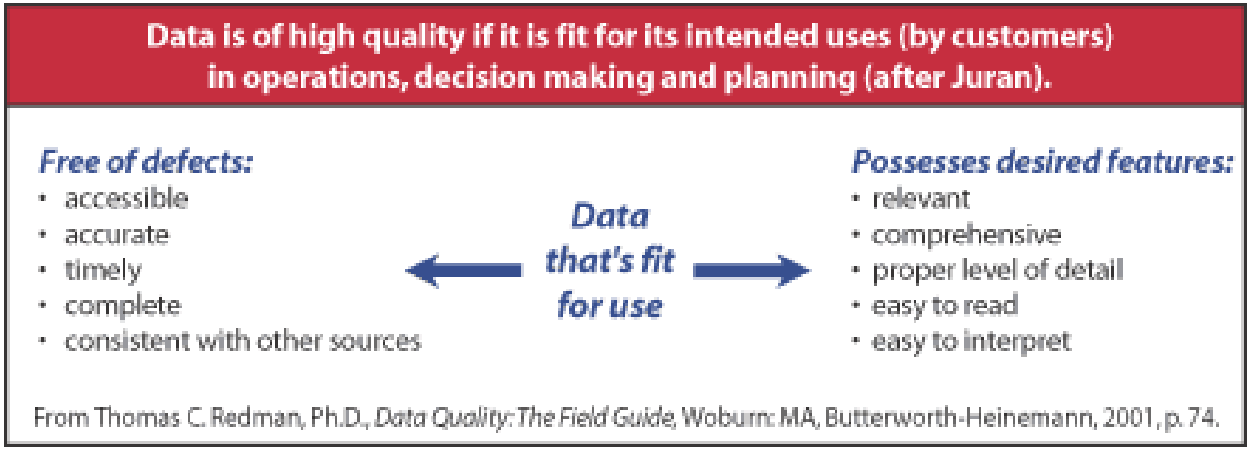


  - **Similar studies in Computer World and the Wall Street Journal back up the assertion that overall data quality is poor.**
    - **W.M. Bulkeley, "Databases Are Plagued by Reign of Error," The Wall Street Journal, 26 May 1992, B2.**
    - **B. Knight, "The Data Pollution Problem," ComputerWorld, 28 September 1992, 81-84.**

The High Cost of Poor Quality Data

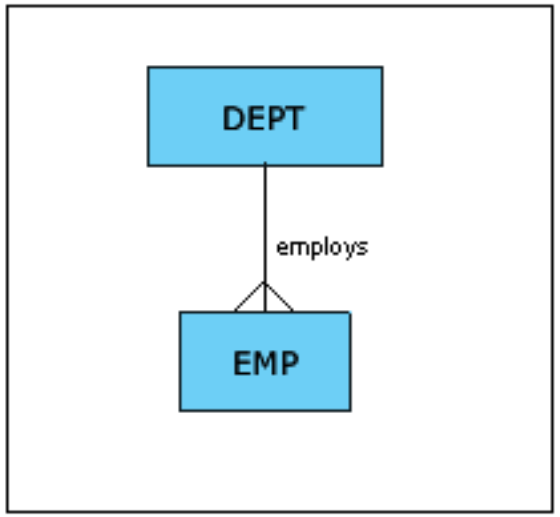
- **"Poor data quality costs the typical company at least ten percent (10%) of revenue; twenty percent (20%) is probably a better estimate."**

Source: Thomas C. Redman, "Data: An Unfolding Quality Disaster", DMReview Magazine



Database Constraints

- **By building constraints into the database, overall data quality may be improved:**
  - **Referential Integrity**
    - **Primary Key**
    - **Foreign Key(s)**
  - **UNIQUE constraints**
  - **CHECK constraints**
  - **Triggers**
  - ***Domains***



Data Profiling and Mapping

- **With data profiling, you can:**
  - **Discover the quality, characteristics and potential problems of information before beginning data-driven projects**
  - **Reduce the time and resources required to find problematic data**
  - **Allow business analysts and data stewards to have more control on the maintenance and management of enterprise data**
  - **Catalog and analyze metadata and discover metadata relationships**

And it all Requires...

Metadata Management

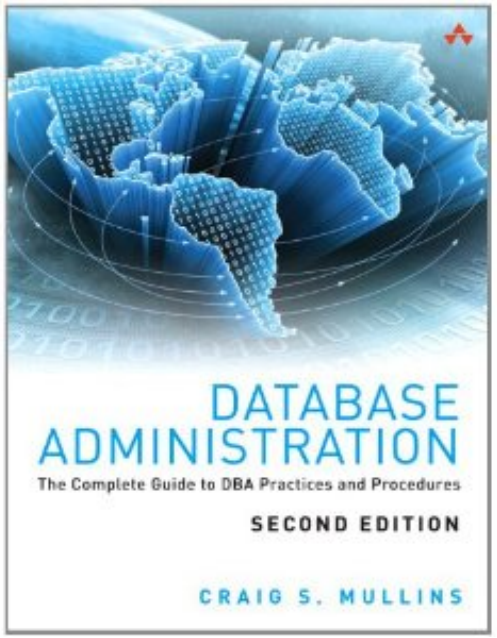
- As data volume expands and more regulations hit the books, metadata will increase in importance
  - Metadata: data about the data
  - Metadata characterizes data. It is used to provide documentation enabling data to be understood and more readily consumed by your organization. Metadata answers the who, *what, when, where, why*, and *how* questions for users.
- Data without metadata is meaningless
  - Consider: 27, 010110, JAN
- Metadata is required to place the data into proper categories for determining which regulations apply
  - Financial data → SOX
  - Health care data → HIPAA
  - PII → HIPAA, PCI DSS

Takeaways & Action Items

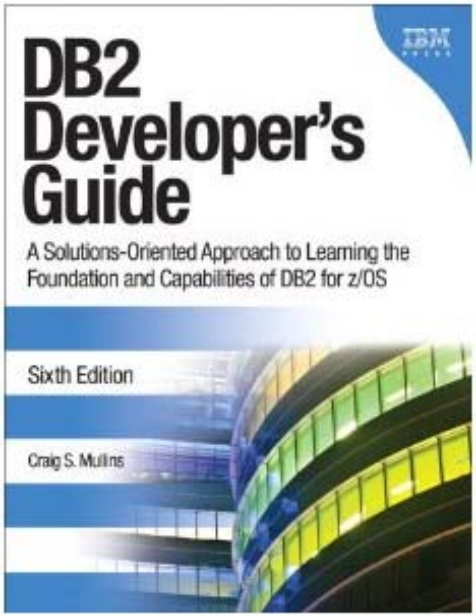
- **Regulatory compliance is mandatory and *must* be followed.**
  - **The specific regulations that you must comply with depend upon your industry, business practices, and company size.**
- **Complexity of business operations, business processes, and enabling technologies are specific areas of concern**
- **Scope is an issue and automation of compliance controls is recommended**
  - **Implement formalized management, monitoring, and measurement tools**
  - **Compliance is not a single project, but an ongoing concern**
- **Use compliance as a driving force to secure the proper tools and technologies for automating your database systems and applications.**
- **There is rarely a better time to install and implement useful technologies than when it helps to adhere to a legal mandate.**

Contact Information

http://www.craigsmullins.com/dba_book.htm



← *2nd edition now available…*



← *6th edition now available… covering up thru DB2 V10!*

http://www.craigsmullins.com/cm-book.htm

Craig S. Mullins
Mullins Consulting, Inc.
15 Coventry Court
Sugar Land, TX 77479

http://www.craigsmullins.com

craig@craigsmullins.com

Phone: (281) 494-6153

SoftBase Contact Information

SoftBase

20 Fall Pippin Lane, Suite 202
Asheville, NC USA 28803
sbsales@softbase.com
support@softbase.com
828-670-9900

http://www.softbase.com

About Candescent SoftBase LLC

SoftBase is a leading provider of application testing and tuning solutions for IBM's DB2® database utilizing the OS/390® and z/OS® operating systems. SoftBase solutions enable our customers to build and maintain high-quality DB2 applications that run as reliably and cost-effectively as possible. SoftBase was founded in 1987 and is recognized globally for our long term service and commitment to our DB2 mainframe customers. SoftBase is a division of Candescent SoftBase LLC.

Take the Survey!

- **The first 25 people who complete the data security and compliance survey will receive a free $10 Starbucks gift card**

https://www.softbase.com/security-survey.php

Web References

- **Industry Organizations and References**
  - www.isaca.org – (auditor's organization)
  - www.privacyrights.org/data-breach – (data breaches)
  - www.soxlaw.com/www.itgi.org – (Sarbanes-Oxley)
  - www.sox-online.com/coso_cobit.html – (CoBIT)
  - www.pcisecuritystandards.org/index.php – (PCI-DSS)
  - www.bis.org/publ/bcbs107.htm – (Basel II)
  - www.hhs.gov/ocr/privacy/index.html – (HIPAA)
  - www.snia-dmf.org/100year – (100 year archive)
  - www.softbase.com – (test data mgmt solutions)
  - www.mullinsconsultinginc.com – (compliance consulting)

Recommended Reading

- *SQL Injection Attacks and Defense* by Justin Clarke (2009, Syngress, ISBN: 978-1597494243)
- *Implementing Database Security and Auditing* by Ron Ben Natan (2005, Elsevier Digital Press, ISBN: 1-55558-334-2)
- *Cryptography in the Database: The Last Line of Defense* by Kevin Kenan (2006, Addison-Wesley, ISBN: 0321-32073-5)
- *Save the Database, Save the World!* by John B. Ottman, Jr. (2010, The Sumo Press, ISBN: 978-1-4583-6368-8)
- *The Database Hacker's Handbook* by David Litchfield, et al (2005, John Wiley & Sons, ISBN: 0-7645-7801-4)
- *Database Administration: The Complete Guide to DBA Practices & Procedures, 2nd edition* by Craig S. Mullins (2013, Prentice-Hall, ISBN: 978-0-321-82294-9)
- *Understanding DB2 9 Security* by Rebecca Bond, et al (2007, IBM Press, ISBN: 0-13-134590-7)
- *Manager's Guide to Compliance* by Anthony Tarantino (2006, John Wiley & Sons, ISBN: 0-471-79257-8)
- *Electronic Evidence and Discovery: What Every Lawyer Should Know* by Michele C.S. Lange and Kristin M. Nimsger (2004, ABA Publishing, ISBN: 1-59031-334-8)