What is Data Governance

Data Governance is the orchestration of people, process and technology to enable an organization to leverage data as an enterprise asset.

The core objectives of a governance program are:

- Guide information management decision-making
- Ensure information is consistently defined and well understood
- Increase the use and trust of data as an enterprise asset
Without Data Governance

- People make mistakes...
- Those mistakes more commonly result in losses than hackers...
- Those losses effect every aspect of IT and business
- But data is still an abstract concept and governance needs technology to be improved...

Corporate Sloppiness Is the Real Culprit for Data Loss, Not Vilified Hackers

By Lisa Vaas
3/28/2007 1:25:00 PM

Expect to see the 2 billionth personal record compromised by year's end, according to recent research from the University of Washington. But don't blame it on rogue hackers; sorry to say, it's your own fault, Corporate America.

Researchers at the university in Seattle estimate that electronic records—those containing Social Security or credit card numbers, academic grades or medical history—are bleeding out of North American organizations at the rate of 6 million a month so far in 2007—up some 200,000 a month from last year.

Excluding the exceptional 2003 incident that involved 1.6 billion records stolen from information aggregator Axxiom, hackers have been responsible for only about 550–31 percent—of confirmed breaches between 1980 and 2006.

The majority, 60 percent, of incidents of compromised records were attributed to organizational mismanagement. That includes missing or stolen hardware, administrative errors, insider abuse or theft or accidental posting of sensitive information online. The balance of 9 percent of breaches were due to unspecified circumstances. Even with Axxiom removed from the picture, the commercial sector still accounts for about 252 million individual compromised records, four times that of the next-highest contributor, the government.
The 11 Disciplines of Data Governance

**Outcomes**
- Data Risk Management & Compliance
- Value Creation

**Enablers**
- Organizational Structures & Awareness
- Stewardship
- Policy

**Core Disciplines**
- Data Quality Management
- Information Life-Cycle Management
- Information Security and Privacy

**Supporting Disciplines**
- Data Architecture
- Classification & Metadata
- Audit, Logging & Reporting

Requires

Enhance

Supports
The key activities of a governance program to achieve the objectives are:

- Building governance infrastructure, technology and supporting organization
- Defining data governance policies and standards
- Defining processes and business rules for ongoing governance
- Developing common and standard data domain definitions
- Developing architecture practices and standards
- Developing the capability to monitor and improve the quality and usefulness of data
11 Themes of Data Governance

- Risk Management
- Audit
- Policy
- Security
- Organizational Awareness
- Stewardship
- Data Quality
- Metadata
- Value Creation
- Architecture
- ILM
## Summary of Requirements to Offerings

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Feature</th>
<th>Applicable Regulation</th>
<th>Description</th>
<th>Available Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prevent Data Intrusion</td>
<td>Access Control</td>
<td>All</td>
<td>Assigns unique userid and passwords, privileges assigned based on userid</td>
<td>Built-in Access Control</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Label Based Access Control</td>
</tr>
<tr>
<td>Auditing</td>
<td>Audit Database Privileges</td>
<td>Sarbanes, HIPAA, PCI</td>
<td>Audit privilege granting</td>
<td>IBM Audit Expert (DB) Consul (Enterprise)</td>
</tr>
<tr>
<td>Auditing</td>
<td>Audit Database Access</td>
<td>All</td>
<td>Provides audit trail to data access</td>
<td>IBM Audit Expert (DB) Consul (Enterprise)</td>
</tr>
<tr>
<td>Protect Privacy</td>
<td>Encryption</td>
<td>SB1386, GLBA, HIPAA, PCI</td>
<td>Encrypts data to ensure privacy when unauthorized access occurs</td>
<td>IBM Encryption Expert IBM DB2 and IMS Encryption</td>
</tr>
<tr>
<td>Protect Privacy</td>
<td>Test Data Generation with Data Privacy</td>
<td>SB1386, GLBA, HIPAA, PCI</td>
<td>Ensure test data masks sensitive data</td>
<td>IBM Optim Data Privacy Solution</td>
</tr>
<tr>
<td>Data Retention and Retirement</td>
<td>Data Archiving</td>
<td>Sarbanes, HIPAA</td>
<td>Archive data not being accessed</td>
<td>IBM Optim Archive Solution</td>
</tr>
</tbody>
</table>
Optim is a critical cornerstone in IBM’s Enterprise Data Governance Strategy

- Enterprise Data Governance is an integrated discipline for securing and protecting data as an enterprise asset. This involves implementing, monitoring and sustaining data protection policies and standards in order to improve and ensure data is secure while promoting operational efficiency, transparency, and enabling regulatory compliance and business insight.

The top challenge for 43% of CFOs is improving governance, controls, and risk management

CFO Survey: Current state & future direction, IBM Business Consulting Services
IBM Optim™

- Market leading Enterprise Data Management (EDM) Solution and Platform:
  - Data Growth
  - Retention & Discovery
  - Data Privacy
  - Test Data Management
  - Application Upgrades, Migrations & Retirements

- 2400 clients worldwide; c. 50% of Fortune 500

- Princeton Softech acquired by IBM, September 2007
- **Optim Data Growth Solution (Archiving)**
  - Improve performance
  - Control data growth, save storage
  - Support retention compliance
  - Enable application retirement
  - Streamline upgrades

- **Optim Test Data Management Solution**
  - Create targeted, right sized test environments
  - Improve application quality
  - Speed iterative testing processes

- **Optim Data Privacy Solution**
  - Mask confidential data
  - Comply with privacy policies
Single, scalable, interoperable EDM solution provides a central point to deploy policies to extract, store, port, and protect application data records from creation to deletion.
The Easiest Way to Expose Private Data …
Internally with the Test Environment

- 70% of data breaches occur internally (Gartner)
- Test environments use personally identifiable data
- Standard Non-Disclosure Agreements may not deter a disgruntled employee
- What about test data stored on laptops?
- What about test data sent to outsourced/overseas consultants?
- How about Healthcare/Marketing Analysis of data?
- Payment Card Data Security Industry Reg. 6.3.4 states, “Production data (real credit card numbers) cannot be used for testing or development”

* The Solution is Data De-Identification *
Optim™ Data Privacy Solution

- Substitute confidential information with fictionalized data
- Deploy multiple masking algorithms
- Provide consistency across environments and iterations
- Enable off-shore testing
- Protect private data in non-production environments
Optim™ Test Data Management Solution

- Create targeted, “right-sized” subsets faster and more efficiently than cloning
- Easily refresh, reset and maintain test environments
- Compare data to pinpoint and resolve application defects faster
- Accelerate release schedule
The Problem

- Mergers & acquisitions
- Organic business growth
  - eCommerce
  - ERP/CRM
- The digital revolution
- Records retention
  - Basel II
  - SOX
  - Euro-SOX
- Data multiplier effect
- Forrester estimates that 85% of data stored in databases is inactive

* Source: Noel Yuhanna, Forrester Research, Database Archiving Remains An Important Part Of Enterprise DBMS Strategy, 8/13/07
The Answer – The Optim™ Data Growth Solution

- Production
- Current
- Retrieved
- Archives
- Reference Data
- Historical Data
- Reporting Data

Open Access to Application Data

- Application
- ODBC / JDBC
- XML
- Report Writer
Archiving a Complete Business Object
Why Optim™ Data Growth Solution?

- Manage data across the enterprise including multiple applications, databases, and platforms
- Segment and manage data at the complete business object level
- Increase database performance/response time and minimize batch windows
  - Remove historical business records from Production
- Archive to selected target format
  - Compressed, indexed file
  - XML file
  - Archive database
- Implement tiered storage strategies to maximize ILM efficiencies
  - CAS devices (EMC Centera, IBM DR550)
  - Existing tape libraries
  - Optical disk
- Multiple access methods to archived business records
  - Native Application access
  - Self-Help Access (Canned Reports, Query Tools)
  - Application Independent access (Original app/version is not needed)
What Customers are Saying

“Optim has already yielded the returns we were looking for, and we have just touched the tip of the iceberg…”

“We can easily comply with data privacy regulations without incurring additional costs…”

“The bottom line is that Optim's archiving capabilities will help us exceed our SLA…”

“Our backup times are 20% faster…”