IBM Data Server Security Blueprint

Belal Tassi, DB2 Technical Evangelist
Walid Rjaibi, DB2 Security Architect

March 27, 2008

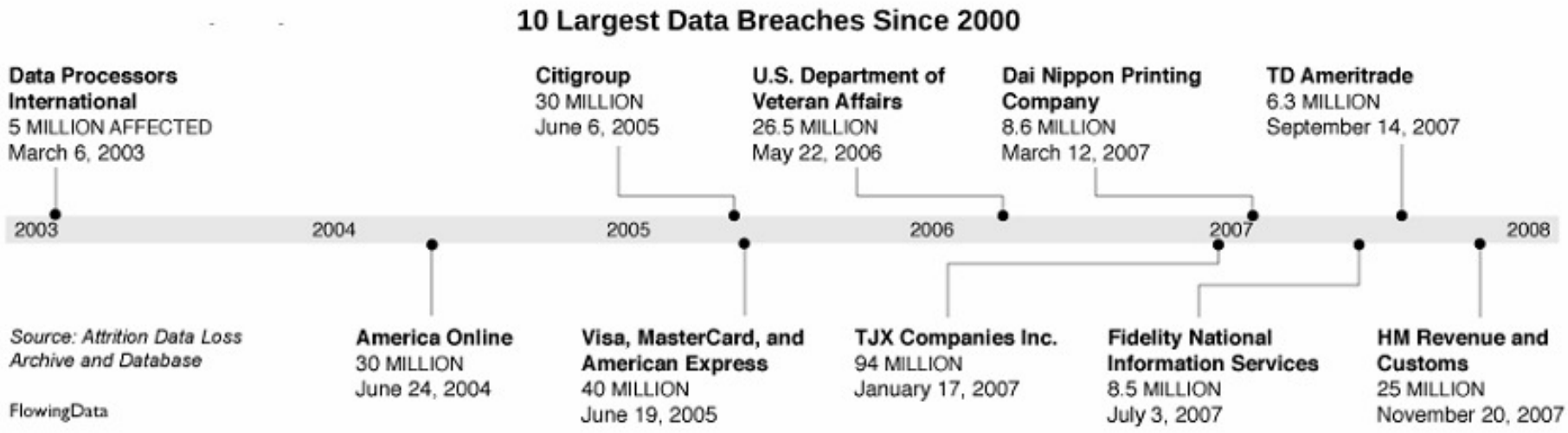
Agenda

- Introduction
- The IBM Data Server Security Blueprint
- Threats
- Countermeasures
- Summary

Introduction

The Importance of Data Security

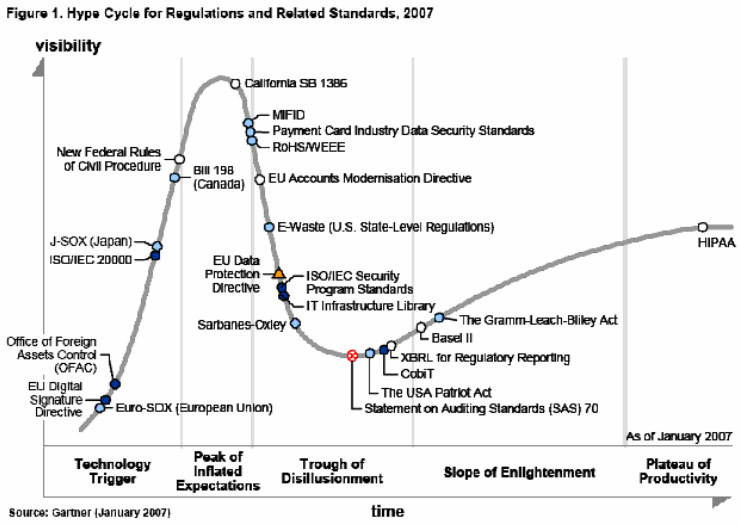
- **Historically focus has been on physical, network, host security**
- **But database is where the valuables are kept!**
- **Data security has now moved to forefront, mostly due to rash of large breaches**



- Source : Flowingdata.com

Regulatory Compliance

- **Many regulations exist today that mandate good practices**
- **Applicability depends on industry and country**
- **Some of the major ones include:**
  - PCI
  - Sarbanes-Oxley
  - HIPAA
  - Data Breach Disclosure Laws
  - Gramm-Leach-Bliley
  - Basel II



Effective Security is Multi-Layered

- **Physical Security**
  - Is the hardware properly protected from unauthorized access?
- **Network Security**
  - Is the network properly protected from unauthorized access?
- **Host Security**
  - Is the machine hosting the database securely configured?
- **Data Security**
  - Is the database secured from both direct and indirect threats?

Security is Multi-Layered (Con't)

- **Business Controls**
  - Are the business controls and processes needed in place?
  - Technology on its own cannot provide security.
  - Ensure compliance to appropriate regulations.

- **Identity Management**
  - Do you have good control over who is using your systems?
  - Cuts across all layers

Data Security is not Trivial

1. **Data Classification**
   - Understand and classify your data
2. **User Classification**
   - Determine who is allowed to access the data
3. **Threat Identification**
   - Understand the threats you face
4. **Countermeasures**
   - Implement effective measures to counter threats applicable to your environment

Data Security is not Trivial

5. **Testing**
   - Validate your countermeasures and security mechanisms
6. **Auditing**
   - Provides the historical trail of access
   - Detecting unauthorized access, and proving compliance
7. **Maintenance**
   - Effective security is not a point in time exercise : everything must be kept up to date

Why Aren't all Databases Secure?

- **Performance and scalability are often the requirements - security is an afterthought**
- **Performance vs. Security - guess who wins?**
- **DBA's are not usually security people, and vise versa**
- **Lack of understanding of the threats**
- **Vendors usually present security as feature / function without context or what it protects against**
- **Security is taken care of in other layers – so why worry?**

The IBM Data Server Security Blueprint

“Complexity is the enemy of security.”

- ***Bruce Schneier***

How to Help Simplify a Complicated Topic?

- **Recognized the need for a "blueprint" that helps database and security administrators implement data security**

- **Design Goals include :**

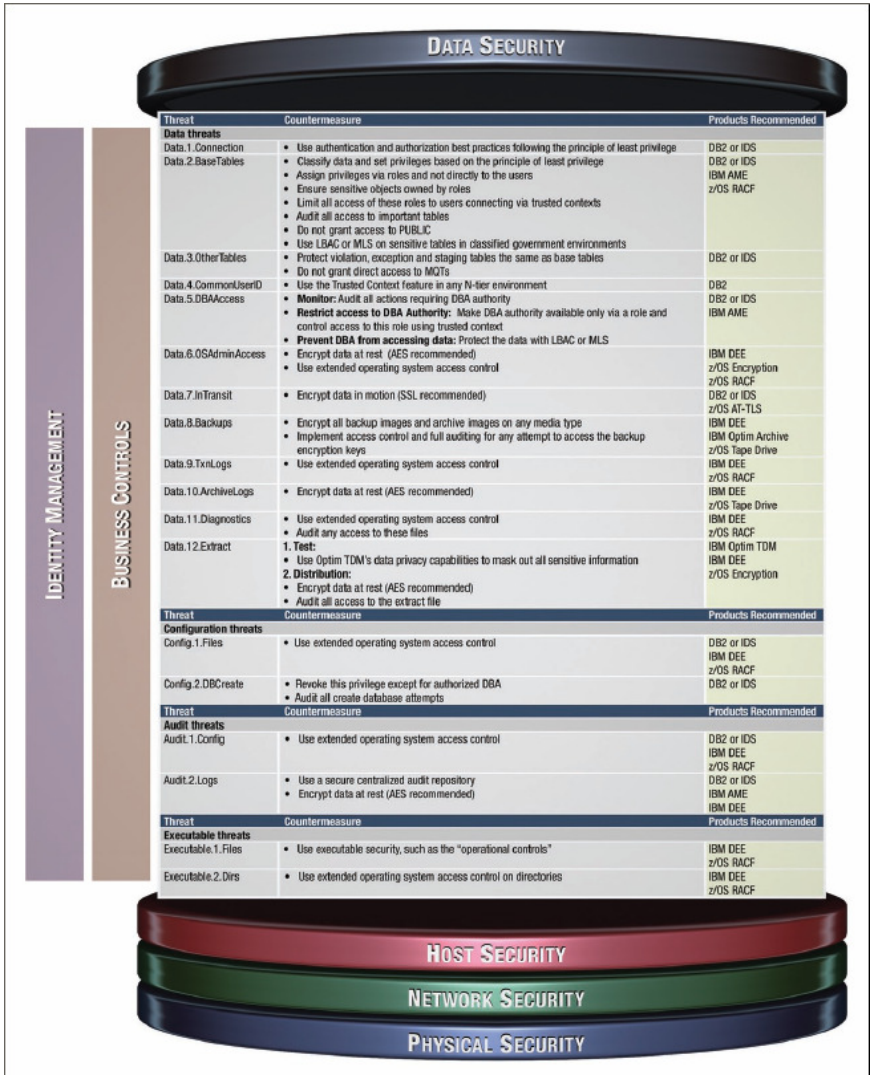
  - Simple to use
    - Fits on 1-2 pages
    - Useable by a novice DBA
  - Accurate
  - Threat focused not feature focused
  - Current recommendations of data server security team
  - Kept up to date as threats and technologies evolve

How to Help Simplify a Complicated Topic?

- **Countermeasures selected from data server features and IBM's data governance and security tools**
- **Applicable to all major IBM Data Servers**
  - DB2 for z/OS
  - DB2 for LUW
  - IDS
- **Input from product security teams and database experts in the field**
- **Focused exclusively on data security layer**

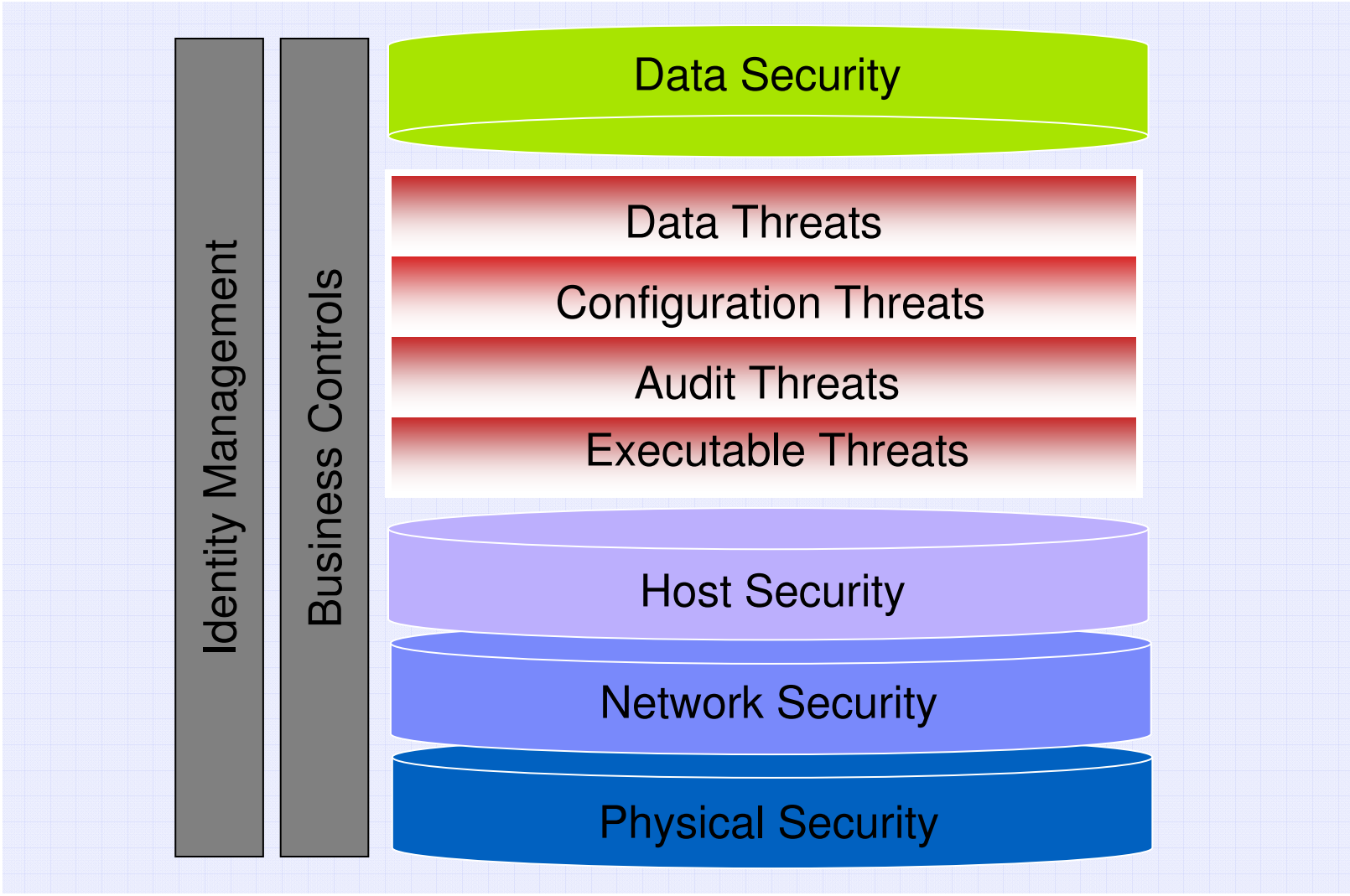
IBM Data Server Security Blueprint

- **A Blueprint for effective data security**
- **Version 1.0.0 released March 2008**
- **Easy to use, single page**
- **DB2 for LUW, DB2 for z/OS and IDS**
- **Accompanying whitepaper**



Threat	Countermeasure	Products Recommended
Data threats		
Data.1.Connection	• Use authentication and authorization best practices following the principle of least privilege	DB2 or IDS
Data.2.BaseTables	• Classify data and set privileges based on the principle of least privilege • Assign privileges via roles and not directly to the users • Ensure sensitive objects owned by roles • Limit all access of these roles to users connecting via trusted contexts • Audit all access to important tables • Do not grant access to PUBLIC • Use LBAC or MLS on sensitive tables in classified government environments	DB2 or IDS IBM AME z/OS RACF
Data.3.OtherTables	• Protect violation, exception and staging tables the same as base tables • Do not grant direct access to MQTs	DB2 or IDS
Data.4.CommonUserID	• Use the Trusted Context feature in any N-tier environment	DB2
Data.5.DBAAccess	• **Monitor:** Audit all actions requiring DBA authority • **Restrict access to DBA Authority:** Make DBA authority available only via a role and control access to this role using trusted context • **Prevent DBA from accessing data:** Protect the data with LBAC or MLS	DB2 or IDS IBM AME
Data.6.OSAdminAccess	• Encrypt data at rest (AES recommended) • Use extended operating system access control	IBM DEE z/OS Encryption z/OS RACF
Data.7.InTransit	• Encrypt data in motion (SSL recommended)	DB2 or IDS z/OS AT-TLS
Data.8.Backups	• Encrypt all backup images and archive images on any media type • Implement access control and full auditing for any attempt to access the backup encryption keys	IBM DEE IBM Optim Archive z/OS Tape Drive
Data.9.TxnLogs	• Use extended operating system access control	IBM DEE z/OS RACF
Data.10.ArchiveLogs	• Encrypt data at rest (AES recommended)	IBM DEE z/OS Tape Drive
Data.11.Diagnostics	• Use extended operating system access control • Audit any access to these files	IBM DEE z/OS RACF
Data.12.Extract	1. **Test:** • Use Optim TDM's data privacy capabilities to mask out all sensitive information 2. **Distribution:** • Encrypt data at rest (AES recommended) • Audit all access to the extract file	IBM Optim TDM IBM DEE z/OS Encryption
Threat	**Countermeasure**	**Products Recommended**
Configuration threats		
Config.1.Files	• Use extended operating system access control	DB2 or IDS IBM DEE z/OS RACF
Config.2.DBCreate	• Revoke this privilege except for authorized DBA • Audit all create database attempts	DB2 or IDS
Threat	**Countermeasure**	**Products Recommended**
Audit threats		
Audit.1.Config	• Use extended operating system access control	DB2 or IDS IBM DEE z/OS RACF
Audit.2.Logs	• Use a secure centralized audit repository • Encrypt data at rest (AES recommended)	DB2 or IDS IBM AME IBM DEE
Threat	**Countermeasure**	**Products Recommended**
Executable threats		
Executable.1.Files	• Use executable security, such as the "operational controls"	IBM DEE z/OS RACF
Executable.2.Dirs	• Use extended operating system access control on directories	IBM DEE z/OS RACF

IBM Data Server Security Blueprint



What the Security Blueprint Is NOT

- **The IBM Data Server Security Blueprint is not :**
  - An implementation guide
  - A replacement for a data server security policy
  - Concerned with physical, host, network or application security layers
  - Does not discuss the reasoning and tradeoffs for each recommended countermeasure

Threats

Data Threats

- **Threats whereby data can be accessed by unauthorized users**
- **The largest # of distinct threats (12)**

Threat	Threat Description
Data.1.Connection	Exploiting poor database connection authentication and authorization
Data.2.BaseTables	Exploiting poor authorization on base tables
Data.3.OtherTables	Exploiting poor authorization on other tables (replicated tables, MQTs, exception tables etc.)
Data.4.CommonUserID	Loss of identity of connected users in N-tier architectures due to common user ID
Data.5.DBAAccess	Abusing database administrator privileges

Data Threats (Con't)

Threat	Threat Description
Data.6.OSAdminAccess	Abusing operating system administrator privileges
Data.7.InTransit	Sniffing data in transit on the network
Data.8.Backups	Exploiting poor security on backups and archives
Data.9.TxnLogs	Exploiting poor security on transaction logs
Data.10.ArchiveLogs	Exploiting poor security on archived transaction logs
Data.11.Diagnostics	Exploiting poor security on trace files, dump files, and output of monitoring and diagnostics
Data.12.Extract	Exploiting extracted data that has been moved from its secure home

Configuration Threats

- **Threats against configuration mechanisms of data server**
- **Control critical aspects of data server security**

Threat	Threat Description
Config.1.Files	Exploiting poor security on database configuration files
Config.2.DBCreate	Exploiting lack of authorization on who can create databases

Audit Threats

- **Threats against audit facility itself**
- **Tampering to hide one tracks**

Threat	Threat Description
Audit.1.Config	Exploiting poor security on audit configuration files
Audit.2.Logs	Exploiting poor security on audit log files

Executable Threats

- **Threats against DBMS executable files**
- **Unauthorized executable modification for denial of service, Trojan horse attacks etc.**

Threat	Threat Description
Executable.1.Files	Maliciously modifying data server executable files
Executable.2.Dirs	Exploiting poor security on directories containing executables or data

Countermeasures

Countermeasures : Data Server Security Features

- Authentication
- Authorization
- Database Roles
- Trusted Contexts
- Label-Based Access Control
- Auditing
- Encryption
- Static SQL / pureQuery

Countermeasures : Data Server Governance Tools

- **IBM Optim**
  - IBM Optim Test Data Manager
  - IBM Optim Data Privacy
  - IBM Optim Data Growth
- **IBM DB2 Audit Management Expert**
  - z/OS and LUW versions
- **IBM Database Encryption Expert**
- **z/OS Security Server (RACF)**

Data.1.Connection

- **Use Authorization and Authentication best practices**
  - Use Server, LDAP or Kerberos authentication
    - Never use CLIENT authentication!
  - Grant CONNECT privilege to only those who have a business need to connect to the database
    - Never grant CONNECT privilege to PUBLIC!
  - Create new databases with the RESTRICT option

Data.2.BaseTables

- **All Objects**
  - Classify sensitive and non-sensitive data
  - Validate database privileges based on the principle of least privilege
  - REVOKE all privileges from those who do not absolutely need them
  - Access to objects should not be granted to PUBLIC
  - Assign privileges to roles and not directly to specific users
  - Have sensitive objects owned by roles (where applicable)
  - Limit all access of these roles to users connecting from trusted contexts.

- **BASE or SYSTEM CATALOG TABLES**
  - Audit all access to sensitive tables
  - Access to the system catalogs should not be granted to PUBLIC
  - Use Label-Based Access Control (LBAC) or z/OS MLS on sensitive tables in highly sensitive and regulated environments.

Data.3.OtherTables

- **Don't forget the other tables in your database**
  - SQL Replicated tables
  - Materialized Query Tables (MQTs)
  - Exception tables
  - Staging tables
  - OLAP Cubes
  - Clone Tables
  - ….
- **Treat them like base tables for the purposes of security.**
- **MQTs**
  - MQTs should be internal tables, with no direct user access
  - If direct access is required, turn on fine-grained auditing of all SQL access

Data.4.CommonUserID

- **Use the Trusted Context feature in any N-tier environment**
- **Trusted contexts allow the middle-tier to assert the identity of the end user accessing say “to” instead of accessing the database**
- **The end user's database identity and database privileges are then used for any database requests by that end user**

Data.5.DBAAccess

- **Monitor**
  - Audit all actions requiring DBA authority.
- **Restrict access to DBA Authority**
  - Assign DBA authority only through a role and control access to this role using trusted contexts.
- **Prevent DBA from accessing data**
  - Protect the data with LBAC or z/OS MLS features.

Data.6.OSAdminAccess

- **Prevent the data from being copied or read directly from the file system by using data-at-rest encryption.**
  - AES encryption is recommended

- **Prevent sensitive files (eg. table space files), from being modified directly by the OS administrator.**
  - This requires extended OS access control functionality, such as that provided by IBM DEE and z/OS RACF

Data.7.InTransit

- **Always encrypt the data before it is transferred on the wire**
- **Use SSL encryption**
- **Note that turning on network encryption will cause any data sniffing applications to no longer function**

Data.8.Backups

- **Encrypt *all* backup images and archive images on *any* media type**
  - Disk
  - Tape
  - Optical Disk
  - Etc.

- **Restoration of the backup image**
  - Must require controlled access to the encryption key
  - Must be audited

Data.9 to Data.11

- **Data.9.TxnLogs**
  - Prevent files from being modified directly by the OS admin or any other privileged user using extended OS access control
- **Data.10.ArchiveLogs**
  - Prevent the logs from being copied or read directly from the file system by using data-at-rest encryption
- **Data.11.Diagnostics**
  - Prevent files from being modified directly by the OS admin or any other privileged user using extended OS access control.
  - Audit any direct file system access to these files.

Data.12.Extract

- **Countermeasure depends on purpose of data extract**
  - **Test**
    - Use IBM Optim Data Privacy capabilities to automatically mask out all sensitive information from the data during extraction to your test environment
  - **Distribution**
    - Prevent extract file from being read or modified by using disk encryption
    - Audit all access to the extract file

Countermeasures for Configuration Threats

- **Config.1.Files**
  - Prevent files from being modified directly by the OS admin or any other user using extended OS access control.

- **Config.2.DBCreate (IDS Only)**
  - Revoke this privilege except for authorized DBA.
  - Audit all create database attempts.

Countermeasures for Audit Threats

- **Audit.1.Config**
  - Prevent files from being modified directly by the OS admin or any other privileged user using extended OS access control.

- **Audit.2.Logs**
  - Use a secure centralized audit repository such as IBM Audit Management Expert
  - Use extended OS access control to prevent files from being modified directly on file system by the OS admin or any other privileged user
  - Encrypt the audit logs records on disk

Countermeasures for Executable Threats

- **Executable.1.Files**
  - Use executable security feature, such as the “operational controls” functionality in IBM DEE or z/OS RACF, to prevent executable modification

- **Executable.2.Dirs (DB2 for LUW & IDS Only)**
  - Use extended OS access control to prevent directories from being modified by unauthorized users

Summary

Summary

- **Data security has become critical due to increase of severe data breaches and regulatory compliance requirements**
- **Effective security is multi-layered and challenging**
  - Physical Security
  - Network Security
  - Host Security
  - Data Security
  - Business Controls + Identity Management
- **Data security requires understanding your data, the threats, and effective countermeasures**

Summary

- **The IBM Data Server Security Blueprint get you started and helps simplify task**
  - Includes the current recommendations of data server security team
  - Simple and easy to use
- **Version 1.0.0 was released on March 2008**
  - Contains 18 threats, broken into 4 categories
- **The IBM Data Security Blueprint and accompanying whitepaper can be downloaded from :**

http://www.ibm.com/software/db2/.....