



# Interfaces Between Disparate Databases

Auditing and Controls

David Litton - VCU

Phil Napier - VCU

# Disparate Databases

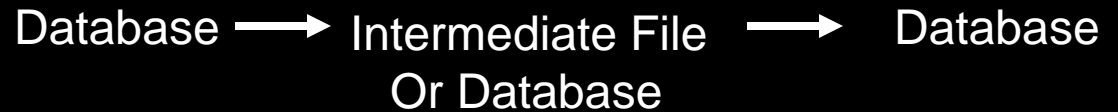
- Definition
  - Databases supporting independent operations, functions, or applications requiring integration.
- Examples
  - Oracle server supporting Human Resources
  - SQL Server supporting Identity Management
  - Databases “external” to a ERP or other systems where some level of integration is desired

# Database Interface Classification

- Batch



- Interface Engine



- Direct



# Database Interfaces

- Batch – Traditional Batch Processing
  - DMZ “Drop” Server
  - “Hub Server” to Process Transaction Updates
  - Traditional ACH transfers
  - HL7 Interfaces

# Database Interfaces

- Interface Engines (can be real time)
  - eGate
  - Eclipsys eLink
  - Oracle SOA Suite
  - Orion Health Rhapsody
  - Siemens OPENLink
  - HL7 Interfaces
- Transaction Queue Monitoring

# Database Interfaces

- Direct Interfaces (Database to Database)
  - OLE DB (Object Linking and Embedding, Database)
  - ODBC (Open Database Connectivity)
  - JDBC (Java Database Connectivity)
  - .NET flavors for OLE and ODBC

# Same as it Ever Was.....

And you may ask yourself

How do I work this?

And you may ask yourself

Where is that large automobile?

And you may tell yourself

This is not my beautiful house!

And you may tell yourself

This is not my beautiful wife!

David Byrne and Bryan Eno - 1980

Mainframes

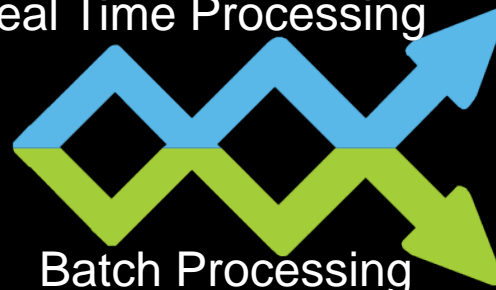
Handhelds  
And the Web



Mini Computers  
Application Centric

Micro Computers  
Client Server Applications

Real Time Processing



Batch Processing

# Why Care?

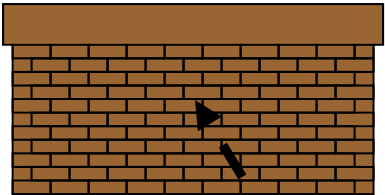
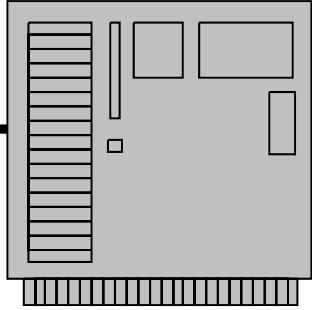
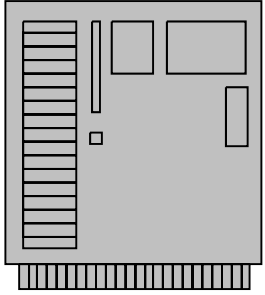
- Sensitive Data
- High Transaction Volume
- High Dollars
- Processing Patient Data via HL7
- Processing Financial Data via ACH
  
- New System Deployment encourages / requires more Interfaces

# Batch Processing or Interface Engine Server

Interface Server

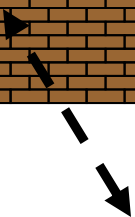
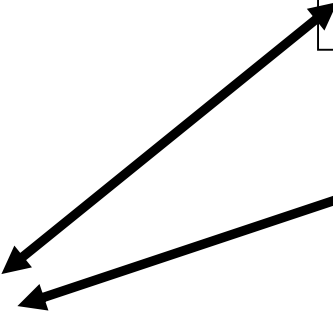
Initiating System

Receiving System



Initiating User

Receiving User or System



# Risks

- Processing Risks
  - Duplicate Records in Receiving System
  - Failed Transmissions / Lost Records
  - Delayed Updates
  - Process Crash / Incomplete Batch / FTP Timeouts
  - Downstream processes receiving incorrect data with no further edit checks
    - Internal Systems or External Organizations

# Risks

- Security Risks
  - External Theft of Information
  - Internal Viewing or Access to Sensitive Data
  - Fraud Risk (changes to data at interim processing step)

# Risk Mitigation Strategies

- Policy
  - Requirements
  - Define Authority
- Standards
  - Identify who is responsible
- Procedures
  - Minimum Requirements
  - Non Compliance

# Risk Mitigation Strategies

- Interface Discovery
- Identification of Key Stakeholders
  - Application
    - System Owner
    - Power Users
  - Technical Staff
    - Application Programming Staff
    - Database Administrators
    - Operating System Administrators
    - Network Staff

# Risk Mitigation Strategies

- Design Procedures that meet policy requirements
- Documentation
  - File Layouts
  - Transmission Timing / Frequency
  - Contacts
  - Workstation Security Controls (if appropriate)
  - Retransmit Procedures
  - Reconciliation/Verification Procedures
  - Test Results

# Application Interface Controls

- Service Agreements
- System to System Transfer verification reports or automated emails
- Control Totals (Batch Totals) and Verification on update
- Periodic Out of Band Reconciliations
- Analytics (period to period comparisons)
  - Are periods within expected “norms”
- Receiving System edit checks
- Error Handling Procedures

# Application Interface Controls

- Unique Filenames
  - Generational, Include time/date in name if possible
- Restrictions on personal database downloads (exports, ODBC connections)
- Transmission or Update Logs
- Automate Purging of Aged Transmissions
- Resist Automating Repairs
- Timing of Repairs (avoid weekends)

# Operating System Controls

- Encryption
- Unique Logins and Directories for users or groups
- Operating System/Access Logs
  - Directory or File Access
- System Hardening
- Directory / Folder permissions
  - Access Restrictions to appropriate users
  - Sending user or System has “write-only” privileges
  - Receiving user has “read-only” privileges

# Questions / Discussion

- David Litton [dmlitton@vcu.edu](mailto:dmlitton@vcu.edu)
- Phil Napier [pnapier@vcu.edu](mailto:pnapier@vcu.edu)