IBM Systems and Technology Group

The Enduring Value of zSeries

Strategic Directions for z/OS, zVM and Linux for zSeries

From a Security Perspective

Jim Porell
IBM Distinguished Engineer
jporell@us.ibm.com

New York RACF Users Group

@server Customer Briefing

© 2005 IBM Corporation

What is Security from a customer view?

- Policy
- Corporate Directive
- Regulatory Compliance (e.g. HIPAA, Sarbanes-Oxley)
- Technology (e.g. RACF, ACF2, Tivoli Access Manager)
- Infrastructure (e.g. Tivoli, Vanguard, Consul, Beta)
- Components (e.g. firewalls)
- Preventative (e.g. anti-virus, intrusion defense)
- Business workflow (e.g. Analytics, audit)
- Physical (e.g. Badge Access, Biometrics)
- Multi-media (e.g. Video cameras, voice analysis)
- Executive Position (e.g. CISO, CPO)
- Skill specialty (e.g. CISSP)
- Department (e.g. Info Assurance, IT Security)

- Redundant
- Bureaucratic
- Too Sensitive
- Expensive
- Unresponsive
- Big Brother

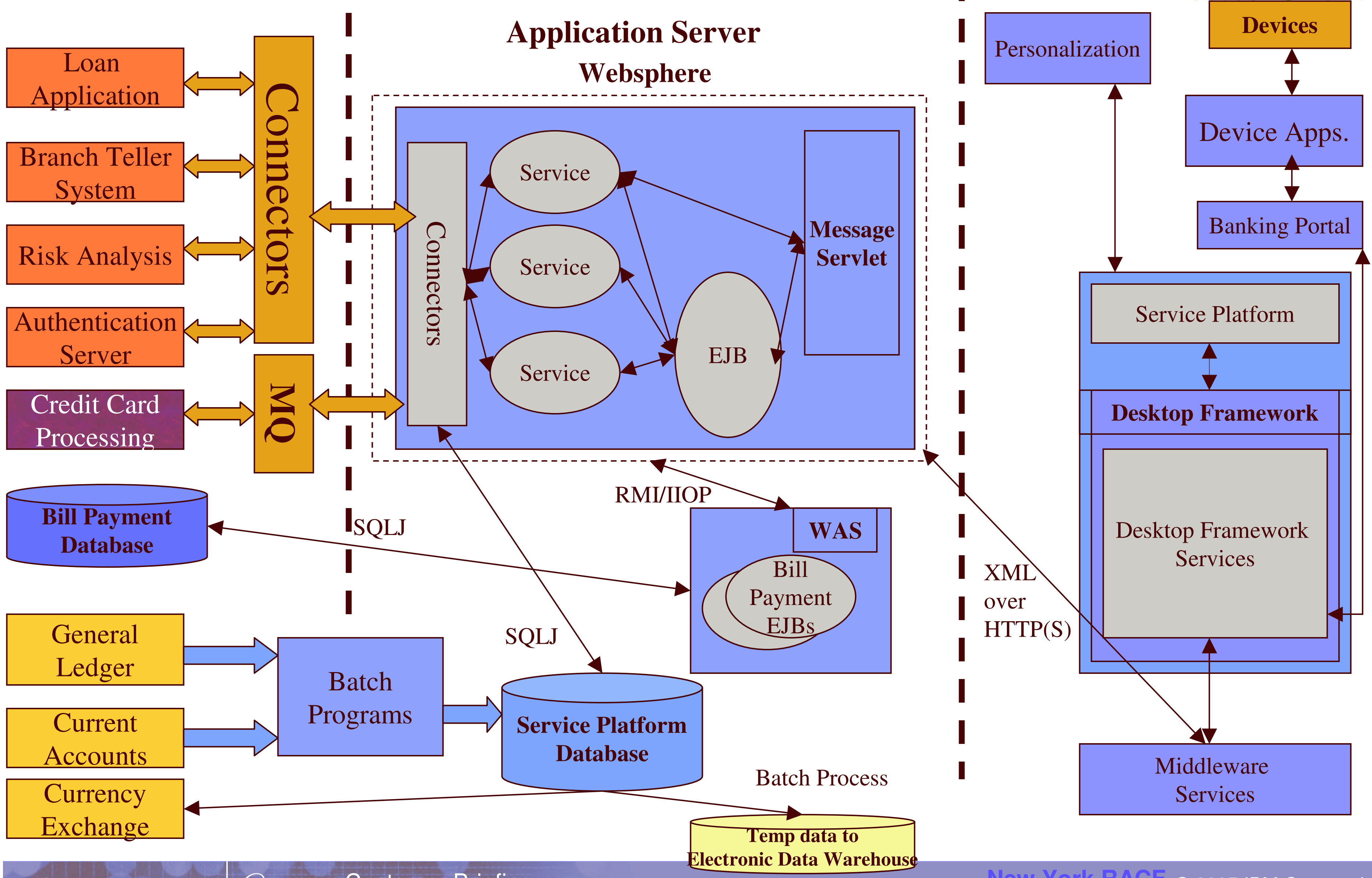
- Typically, it’s not → a Solution
  - Leverage Security to make solutions better
  - But there are new “offerings” evolving that look like solutions
    - e.g. DB2 Entity Analytics Solution

© 2005 IBM Corporation

A large bank – their key components

Service Systems & Databases

End User – Hosted Client



Application Server

Websphere

Loan Application

Branch Teller System

Risk Analysis

Authentication Server

Credit Card Processing

Connectors

MQ

Bill Payment Database

General Ledger

Current Accounts

Currency Exchange

Batch Programs

Service Platform Database

Temp data to Electronic Data Warehouse

Batch Process

SQLJ

SQLJ

RMI/IIOP

Connectors

Service

Service

Service

EJB

Message Servlet

WAS

Bill Payment EJBs

XML over HTTP(S)

Personalization

Devices

Device Apps.

Banking Portal

Service Platform

Desktop Framework

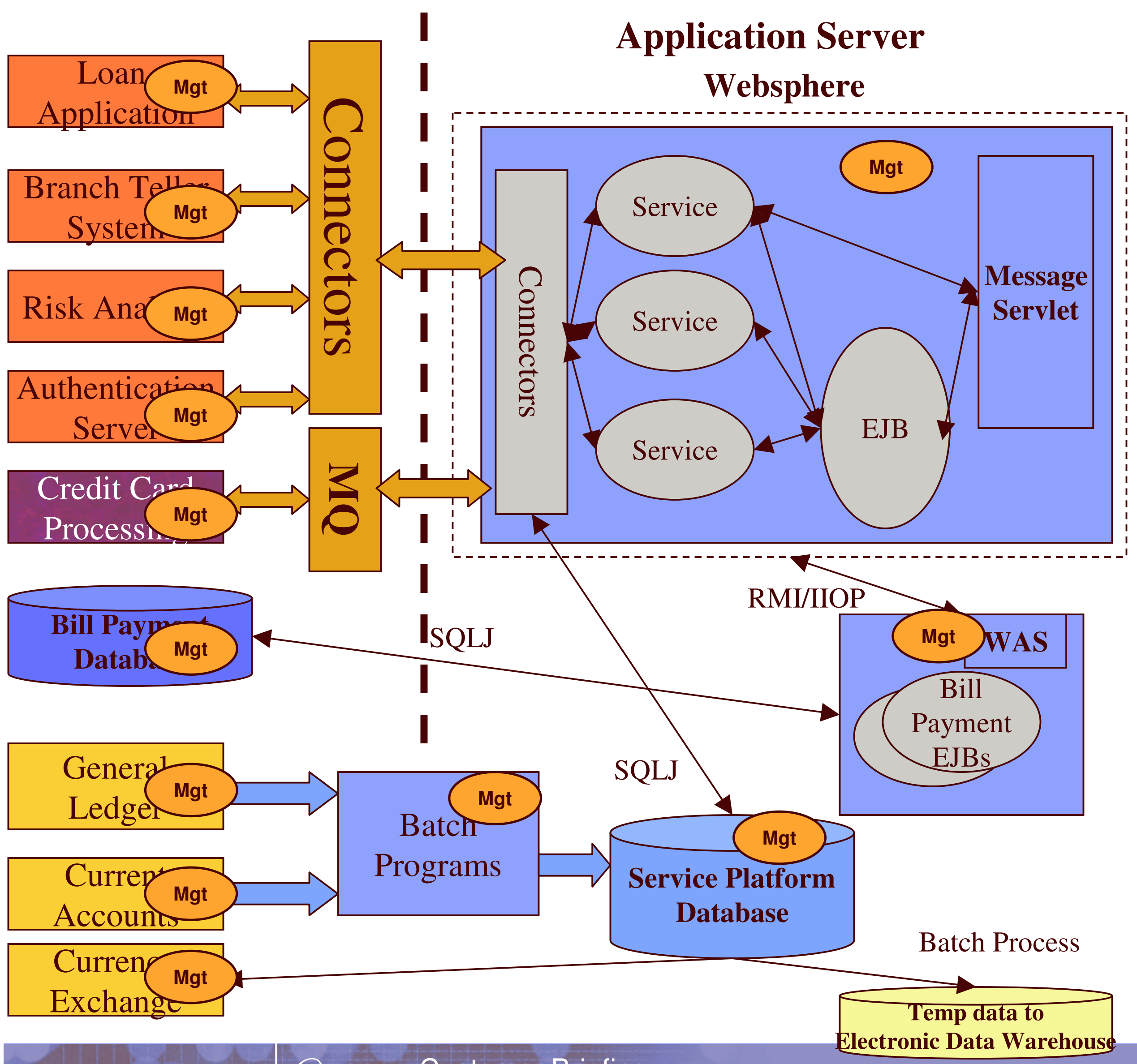
Desktop Framework Services

Middleware Services

© 2005 IBM Corporation

Do they Scale Out?

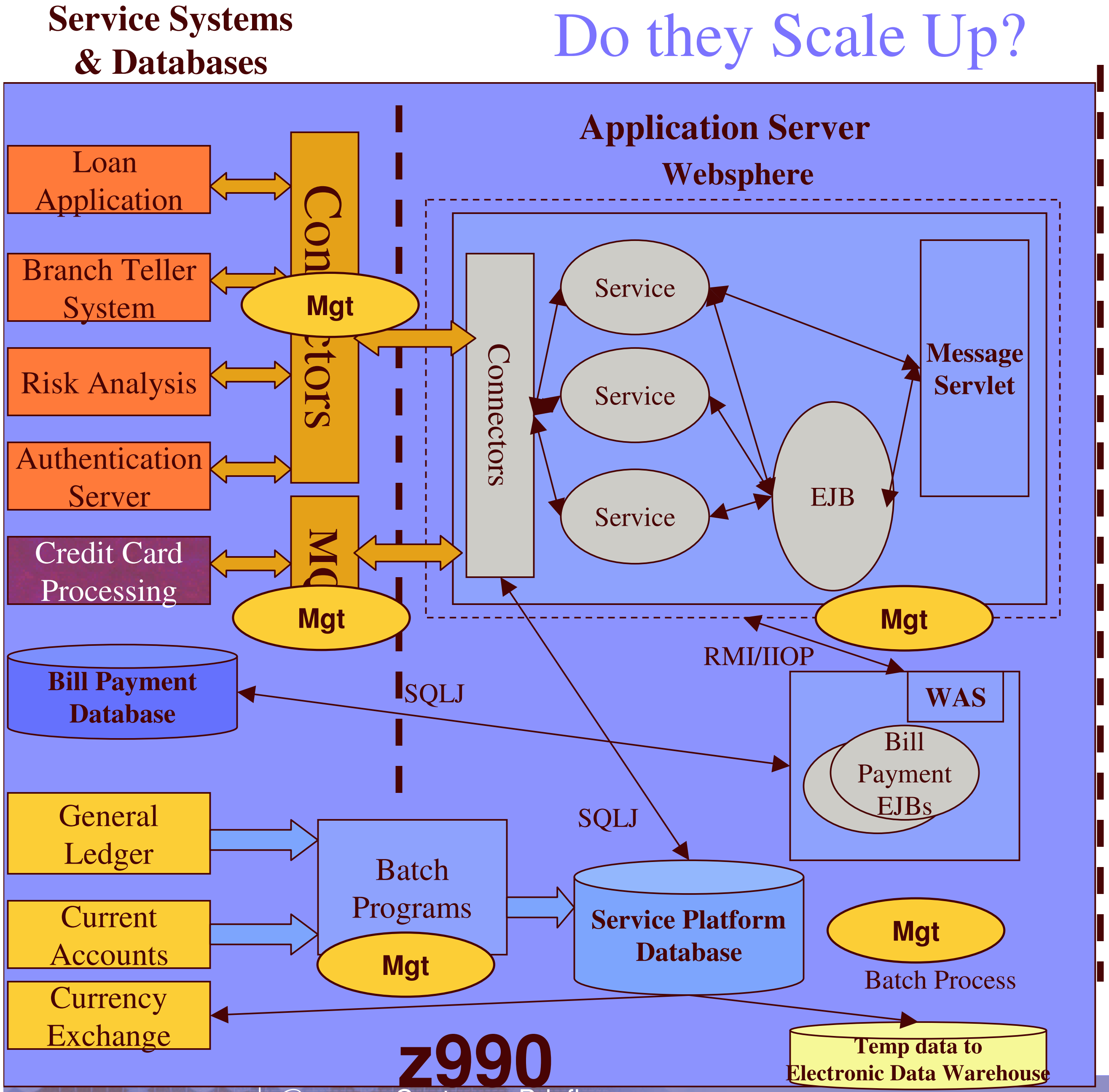
Service Systems & Databases



Mgt

- Authentication
- Alert processing
- Firewalls
- Virtual Private Networks
- Network Bandwidth
- Encryption of data
- Audit Records/Reports
- Provisioning Users/Work
- Disaster Recovery plans
- Storage Management
- Data Transformations
- Application Deployment

Do they Scale Up?



Mgt

Authentication

Alert processing

Firewalls

Virtual Private Networks

Network Bandwidth

Encryption of data

Audit Records/Reports

Provisioning Users/Work

Disaster Recovery plans

Storage Management

Data Transformations

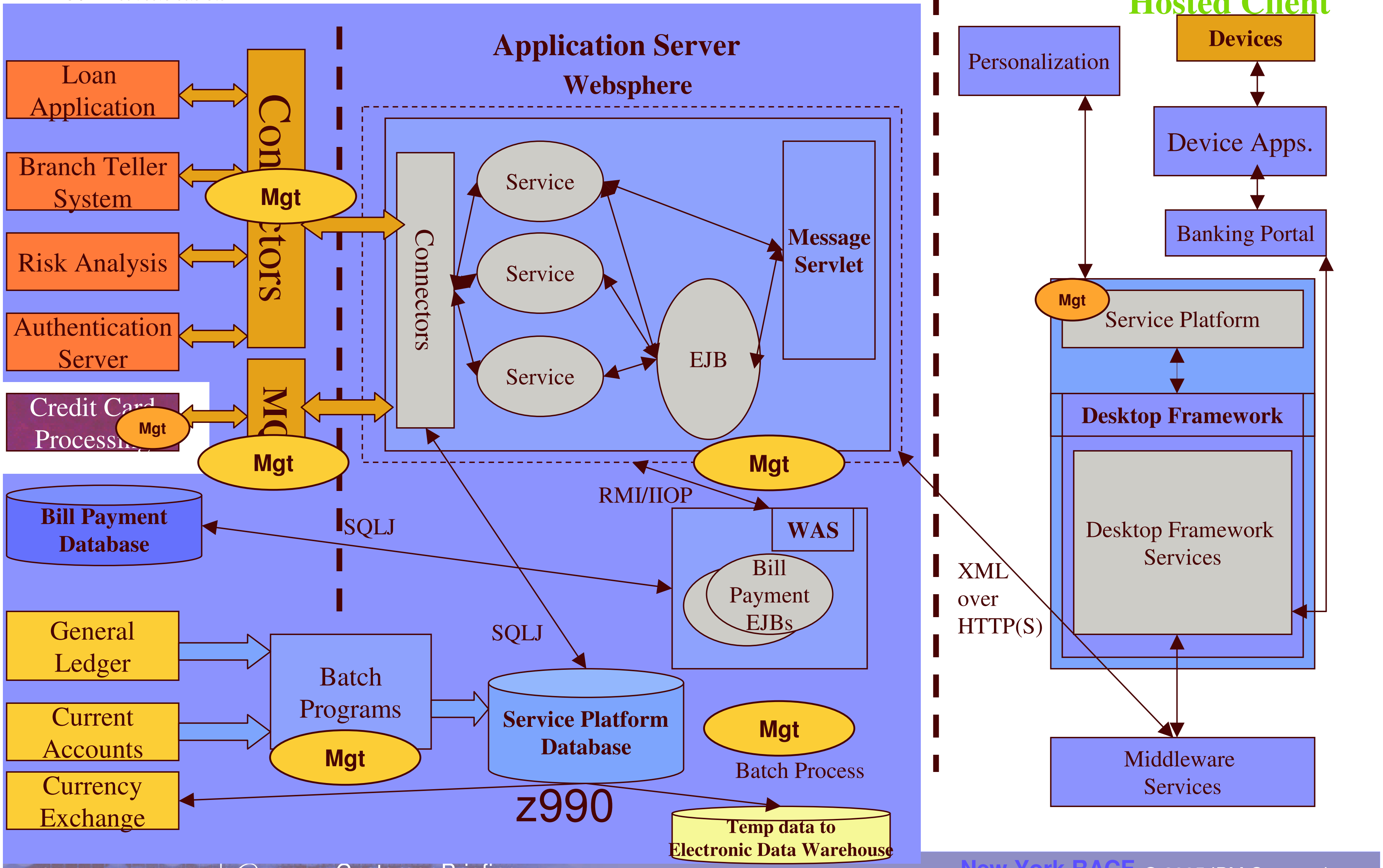
Application Deployment

© 2005 IBM Corporation

Or Both?

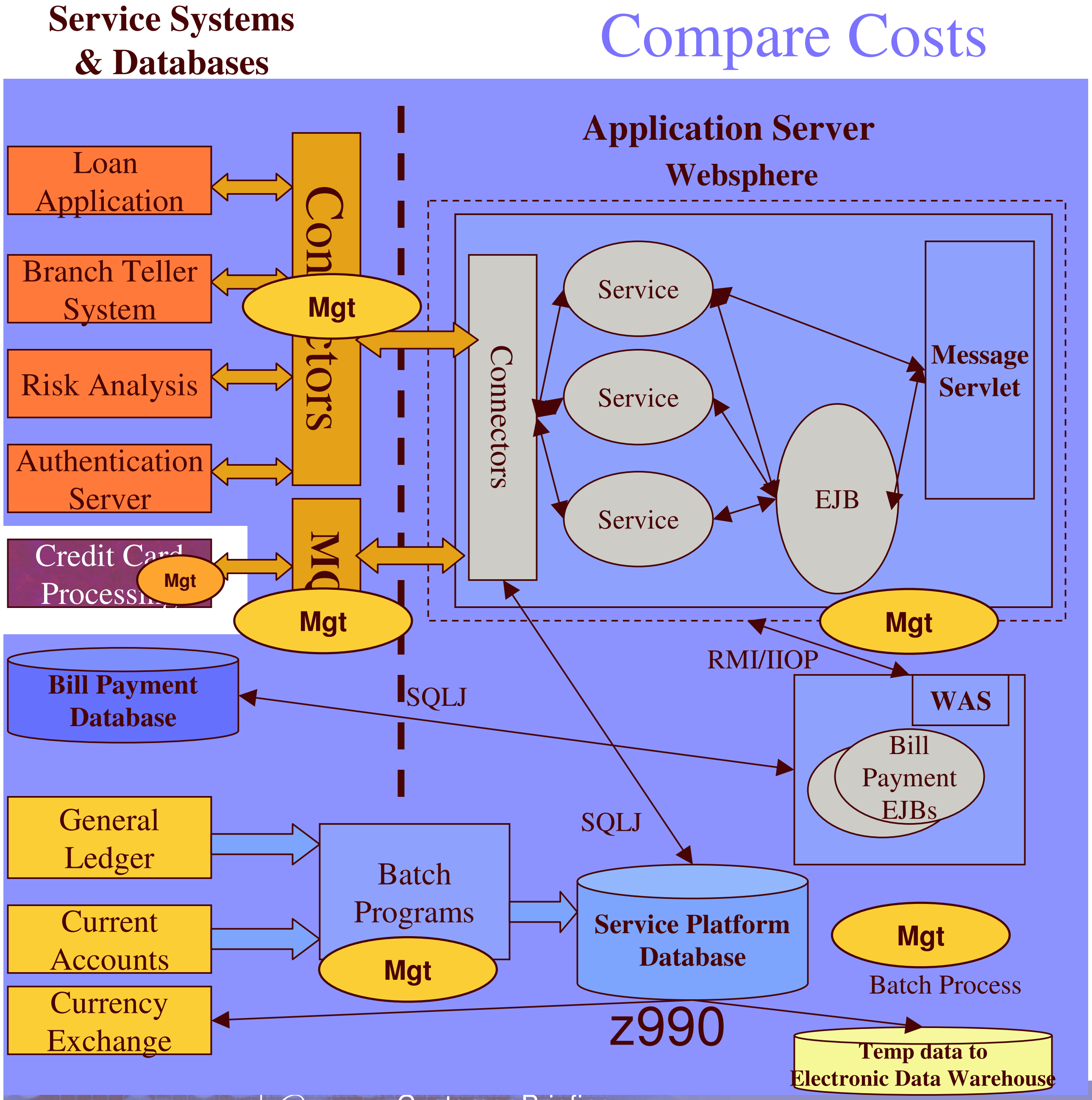
Service Systems & Databases

End User – Hosted Client



© 2005 IBM Corporation

Compare Costs



Compare:

- ✓Scale
- ✓Resilience
- ✓Speed
- ✓Operations
- ✓Control Points
- ✓Complexity
- ✓Batch
- ✓Security
- ✓Compliance/Audit
- ✓Environmentals
- ✓People
- ✘Proof of concept

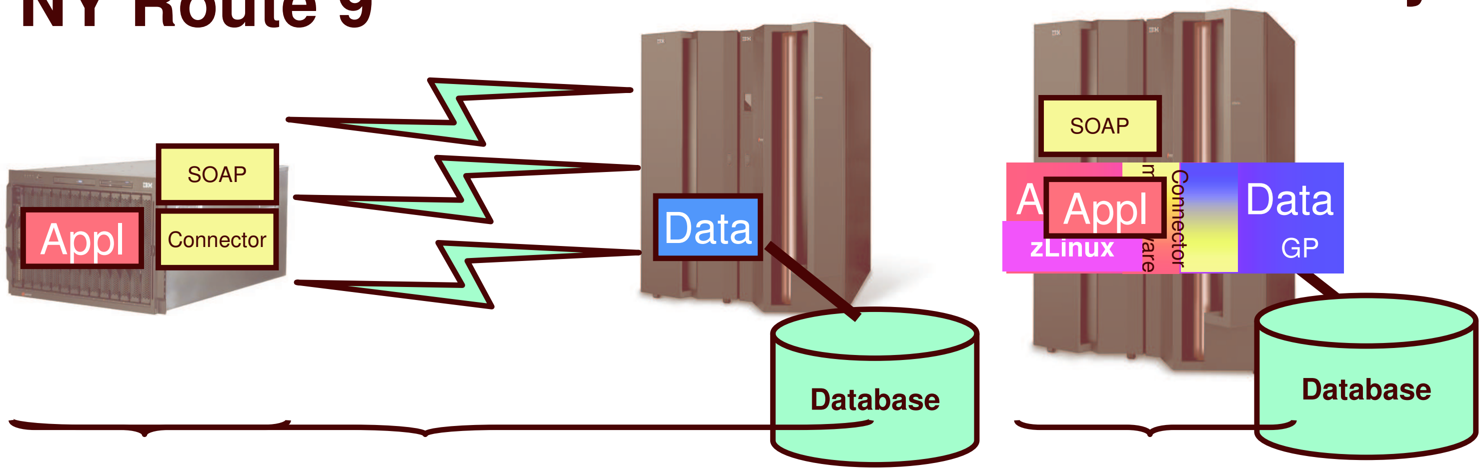
✘Don’t base the production decision on the proof of concept of one part

© 2005 IBM Corporation

Integration of Applications and Data

NY Route 9

NYS Thruway



Compare:

- ✓Scale
- ✓Resilience
- ✓Speed
- ✓Operations
- ✓Complexity
- ✓Environmentals

zSeries: Benchmark Loser ?

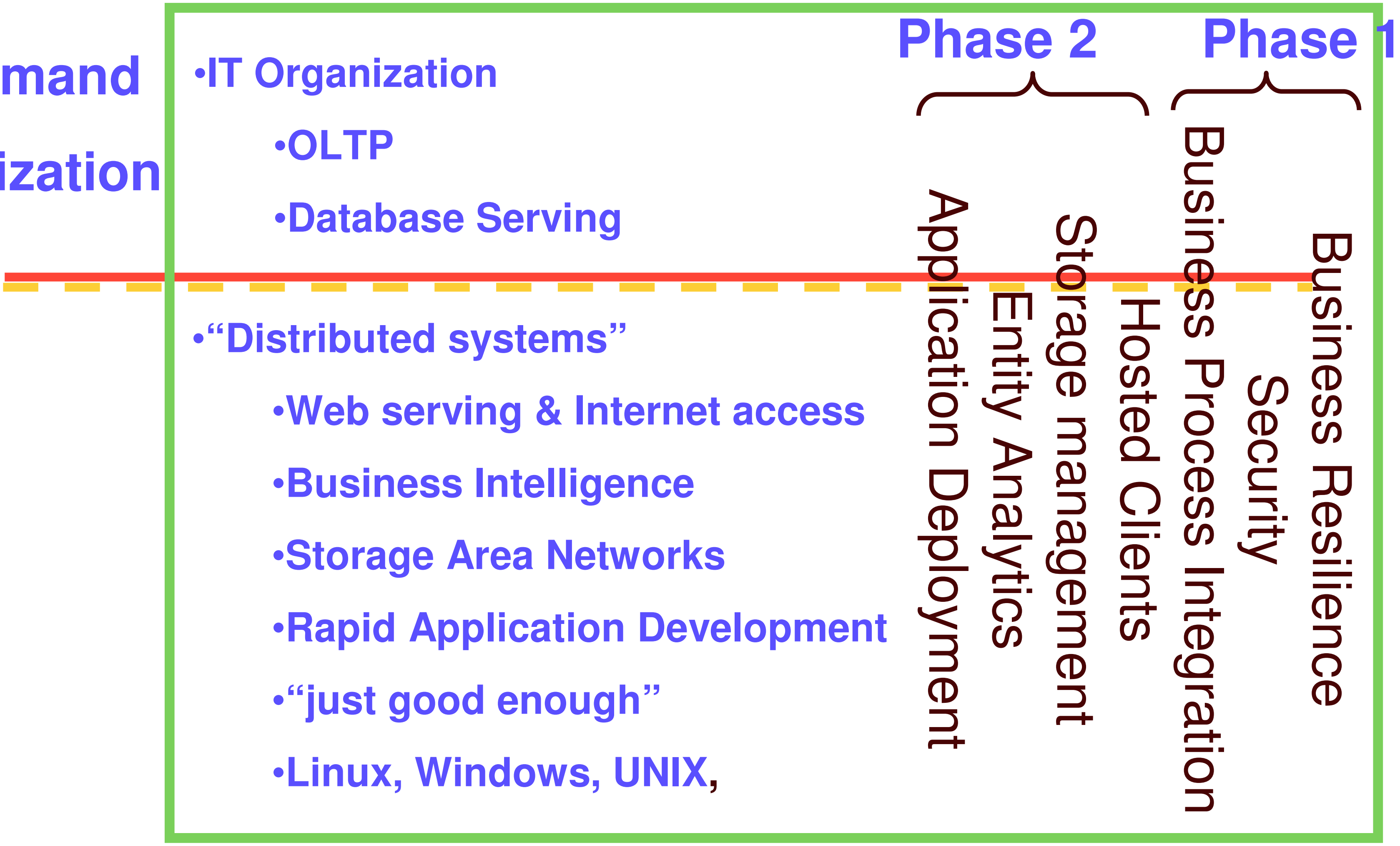
With zLinux (Saw Mill Parkway)

- •Marshall Parameters
- •Cross network hardware
- •Establish security mapping
- •Longer response time
- •Additional capacity and operations
- •Provide data conversion
- •Distributed commit scope
- •Multiple points of failure
- •Fewer points of failure
- •Security intrusion possibilities

- •Intra-process memory calls
- •Internal communications
- •Inherit security credentials
- •Less end to end pathlength
- •Workload managed and balanced
- •Leverage existing data format
- •RRS managed 2 phased commit
- •Fewest points of failure
- •Less opportunity for intrusion

We need to break down the political barriers

OnDemand Organization



- •IT Organization
  - •OLTP
  - •Database Serving
- •“Distributed systems”
  - •Web serving & Internet access
  - •Business Intelligence
  - •Storage Area Networks
  - •Rapid Application Development
  - •“just good enough”
  - •Linux, Windows, UNIX,

Phase 2

Application Deployment

Entity Analytics

Storage management

Hosted Clients

Phase 1

Business Process Integration

Security

Business Resilience

© 2005 IBM Corporation

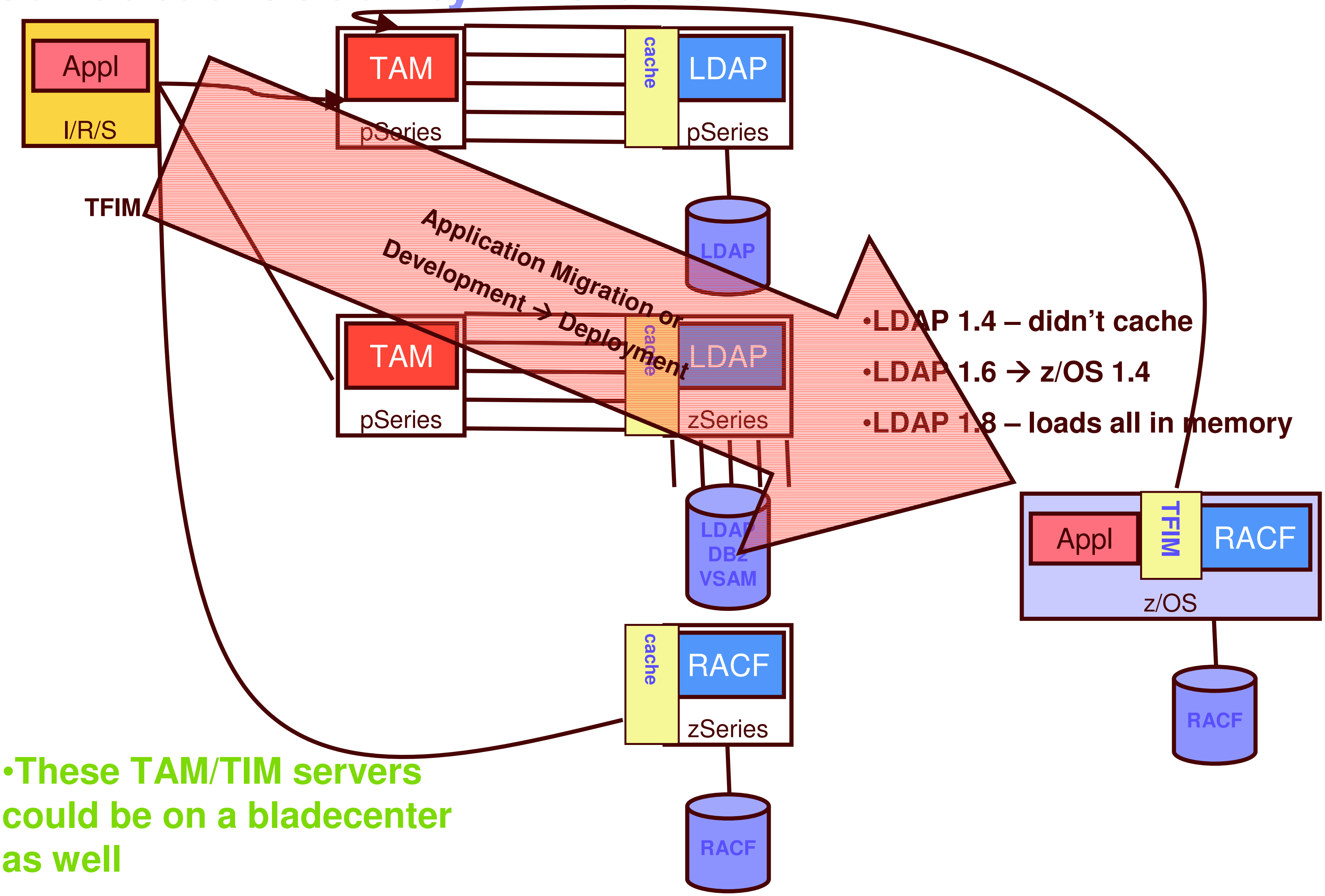
Tivoli and RACF Integration

Enabling Websphere production & development
Simplifying enterprise administration
Improving Corporate Governance

New York RACF
Users Group

© 2005 IBM Corporation

Distributed Security Evolution



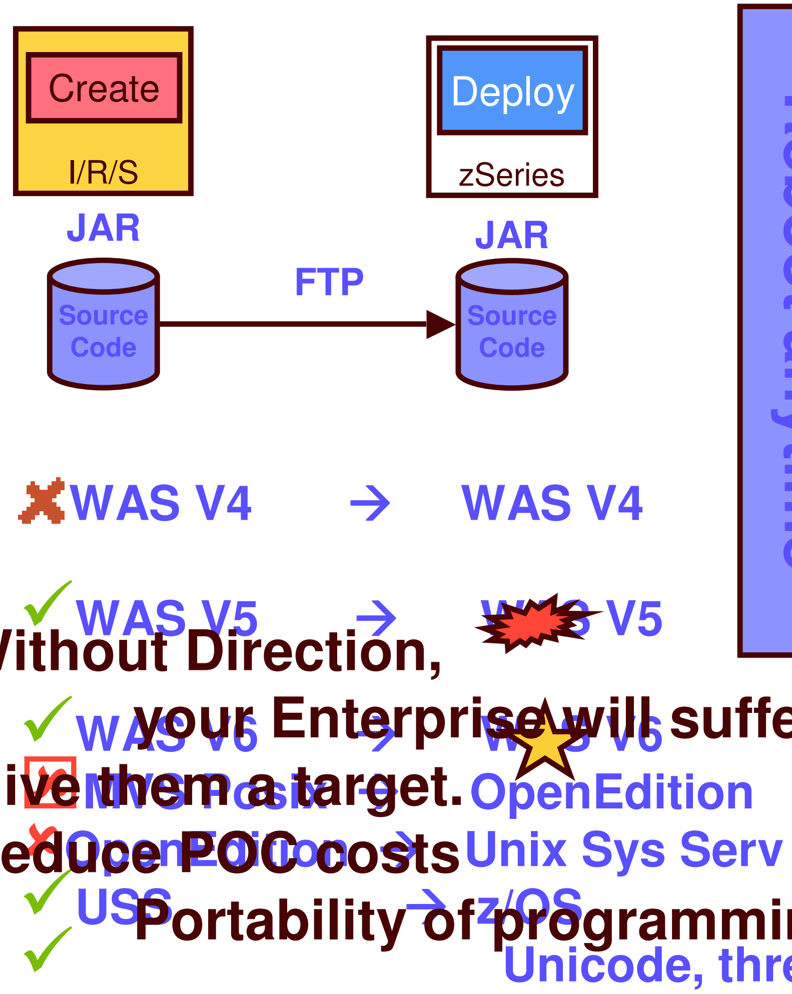
- LDAP 1.4 – didn't cache
- LDAP 1.6 → z/OS 1.4
- LDAP 1.8 – loads all in memory

- These TAM/TIM servers could be on a bladecenter as well

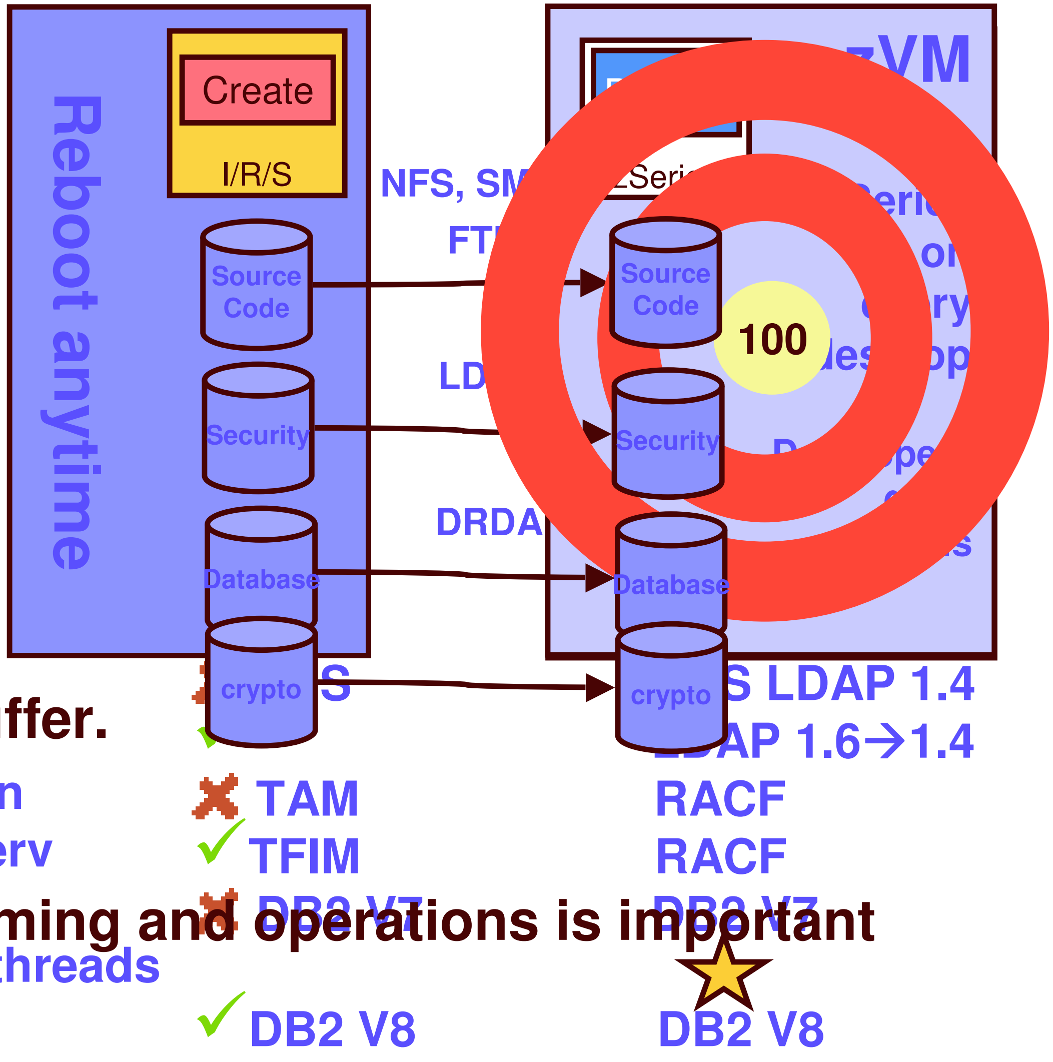
© 2005 IBM Corporation

Application Deployment and Migration Experiences

Application Migration



Operations Migration



Without Direction,
your Enterprise will suffer.

Give them a target.

Reduce POC costs

Portability of programming and operations is important

http://www.ibm.com/university/zseries

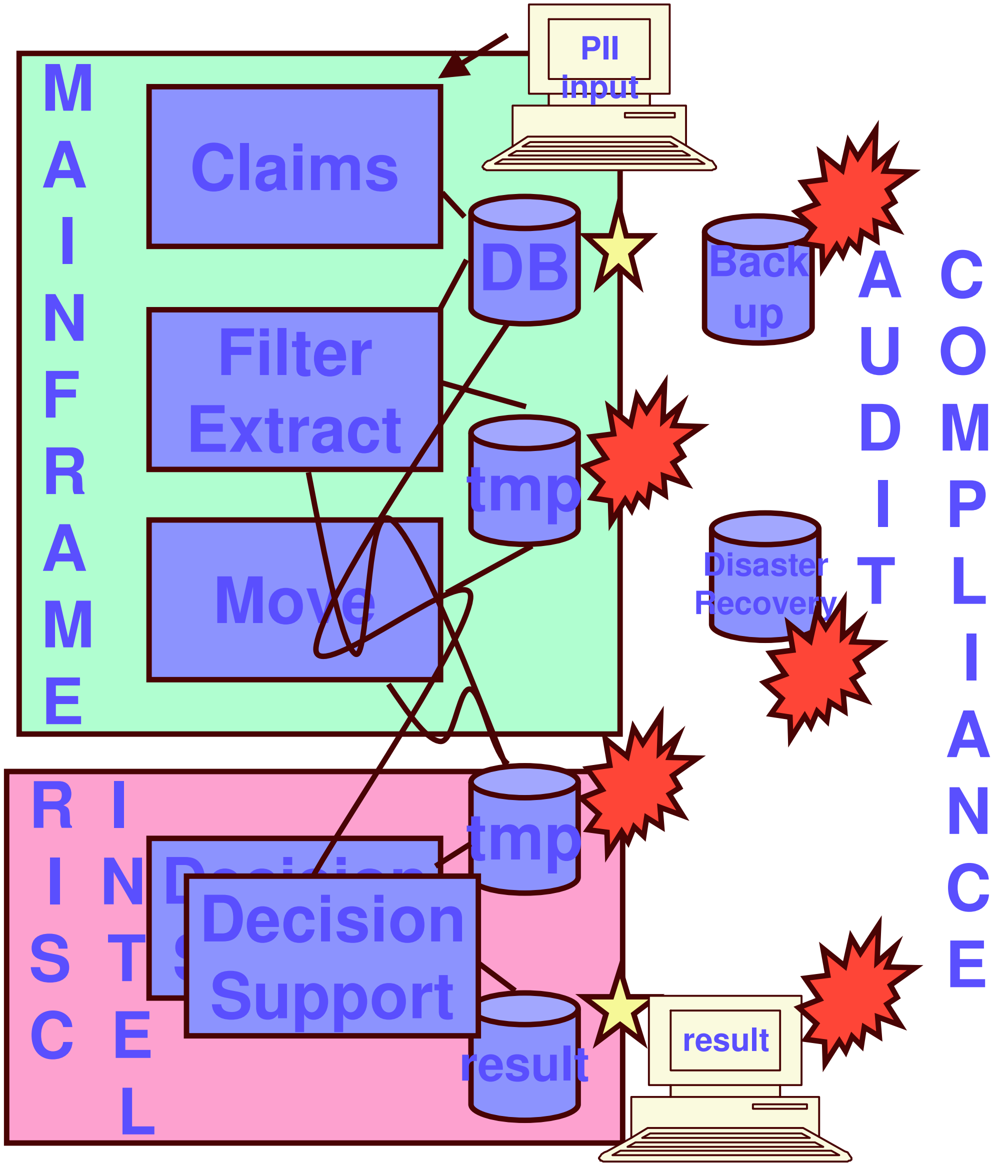
© 2005 IBM Corporation

Tying it all Together

New York RACF Users Group

© 2005 IBM Corporation

Why does Infrastructure simplification matter? HIPAA, Sarbanes-Oxley



Typical Business Workflow

- Do you audit all places with Personally Identifiable Information?
  - Is the process automated?
- Data is easy to replicate
- policies are not.
  - Reducing the copies will reduce compliance efforts and increase resiliency
    - Leverage a file server to delete copies and reduce data movement
    - Application data proximity
      - Move the applications back to the data source, where practical
      - Plus can use WebSphere SOA access facilities, where practical

zSeries: The Data Vault

© 2005 IBM Corporation

IBM Systems and Technology Group

DB2 Entity Analytic Solutions Overview

Answering the Question “Who is Who?” and “Who Knows Who?” to resolve Financial Sanctions and Terrorist Financing Issues

New York RACF
Users Group

© 2005 IBM Corporation

DB2 Identity Resolution Determines “Who is Who?”

DB2 Identity Resolution software helps organizations recognize the single identity who is using multiple identities. So not just “Matching” but beyond “Matching” to finding individuals who are hiding and fraudulent.

Mrs. Kate Greene
1 Bourne St
Clinton MA 01510
Tel#978-365-5312
EIN#097376156
DOB 07/08/64
PPN# 068588345
LIC#1702188364

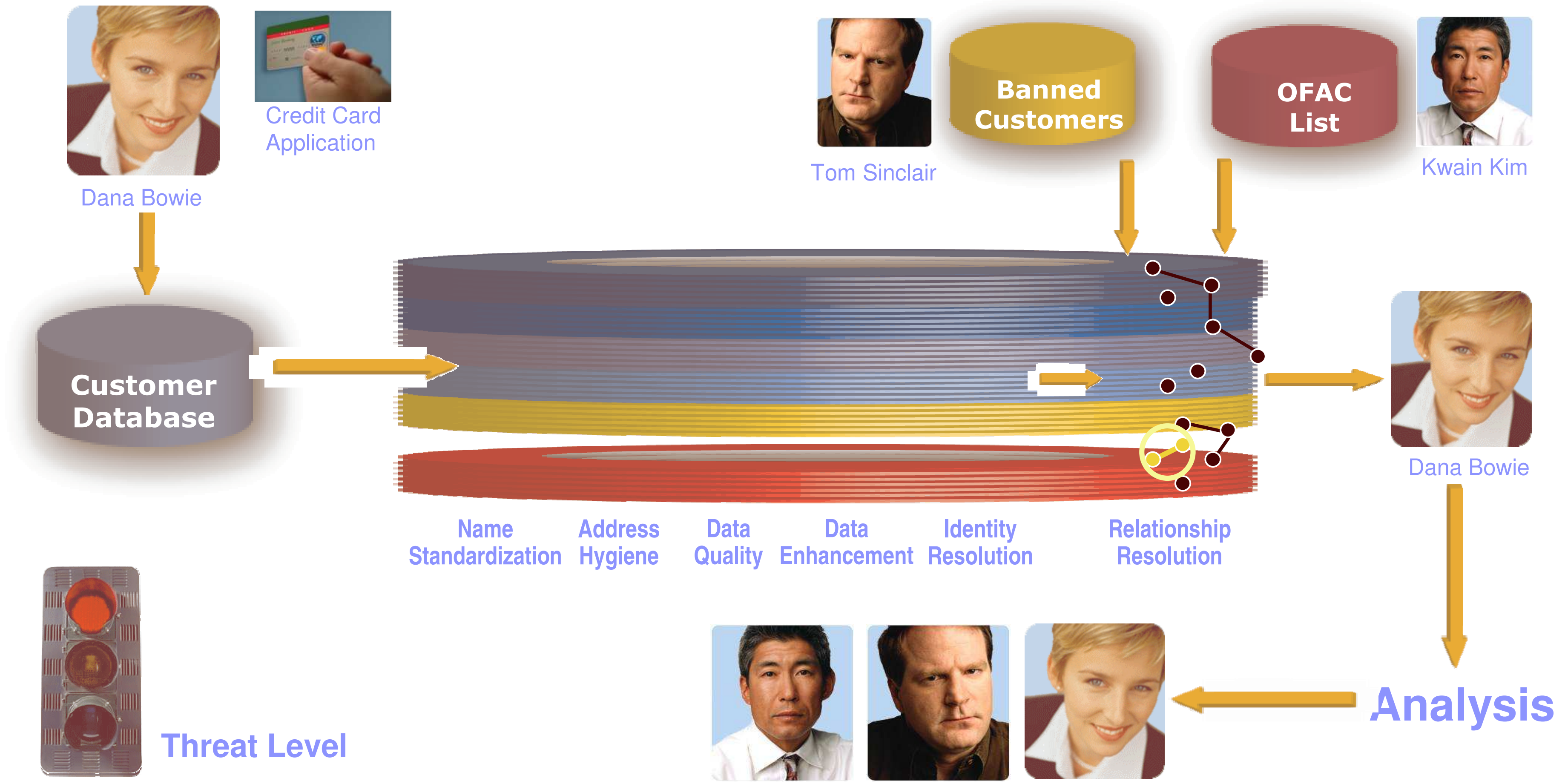
Mrs. Kathy Green
10 Bouren St
Clifton MA 01510
Tel#978-365-5312
LIC#1702188364
PPN# 086588345

Ms. Katherine Green
1 Bourne St
Clinton MA 01510
TEL#978-365-**6631**
LIC#1702188364
DOB 07/**09/66**
EIN#097376156

Mrs. Kate Jones
APT 4909
Bethesda, MD 20814
Tel#301-654-5404
LIC#1702188364
DOB 07/08/64

© 2005 IBM Corporation

DB2 Entity Analytics
Operational Risk Customer Scenario



Dana Bowie

Credit Card Application

Tom Sinclair

Banned Customers

OFAC List

Kwain Kim

Customer Database

Name Standardization

Address Hygiene

Data Quality

Data Enhancement

Identity Resolution

Relationship Resolution

Dana Bowie

Analysis

Threat Level

© 2005 IBM Corporation

How might you quantify value of security?

- Take all your SMF records on z/OS
  - Determine number of I/O's done on the system for a month
  - Count the number of Access failures
    - Remove duplicate failures
      - Create list of unique databases/files with failed attempts
    - Failure to Success ratio is probably: .0000xxx
- Recognize that a successful attempt to access that data may have been to:
  - Corrupt the data (e.g. destroy or modify)
  - Publish personally identifiable data (spam, embarrass, threaten)
  - Identity theft (steal)
- Determine costs to recover from a problem
  - Time, business disruption, lost business, people, backup/archive….
- Project similar costs for each subsequent copy of the data within the enterprise
  - Are similar policies in place with each additional instance to protect?

Net: You are doing a great job managing security!