Extending Your Mainframe for More Business Value

Extend Data Security on the Mainframe

Security and Compliance Issues

- Most Critical Security Issues for the Next Two Years:

  - ▶ Data protection

  - ▶ Identity theft and leakage of private information

  - ▶ Policy and regulatory compliance

  Source: CSI/FBI Survey 2006

  Deloitte 2007 Global Security Survey-- shows that 81% of respondents feel that the issue of security has risen to the level of the C-suite or board as an issue of critical concern.

Protect Customer Data

Our customers are very concerned about the privacy of their data

No problem! You already have many of the required capabilities installed. We can also help you extend your security capabilities.

Service Oriented Finance CEO

IBM

Mainframe Extension Solution – Data Security

- **Start with a secure foundation**
  - ▶ System z platform with RACF

- **Protect customer data end-to-end**
  - ▶ Protect data on platform, off platform, and in transit

- **Block unauthorized network access**
  - ▶ Prevent intrusions

- **Establish and monitor security compliance policies**
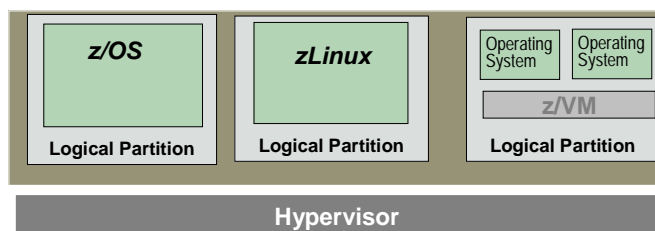 - ▶ Detect any breach of policy

A Secure Foundation Is a Prerequisite to Address Security Issues

- **Workload Isolation**
  - ▶ System z Hypervisor maintains strict isolation between workloads
  - ▶ Hardware coded storage protect keys protects system and user workloads
  - ▶ Architecture design makes typical buffer overflows and virus payloads inoperable
  - ▶ HiperSockets provides secure internal communications

- **Integrated access control throughout the stack**
  - ▶ RACF enforces access control and logs security events

- **Secure cryptographic encoding**
  - ▶ On-chip crypto hardware assist and optional high speed cryptographic processors
    - − Key management facility
  - ▶ **System z10 delivers stronger encryption algorithms with Advanced Encryption Standard (AES) 192 and 256**

A Secure Foundation Requires The Highest Common Criteria Rating for Security

z/OS	zLinux	Operating System / Operating System
		z/VM
Logical Partition	**Logical Partition**	**Logical Partition**

Hypervisor

Partition Manager	Linux	Other OS	VM	DB2
EAL5+	EAL4 for SuSE and Red Hat	z/OS EAL4	zVM EAL3	DB2 for z/OS EAL3

Highest Ratings

- ▶ Common Criteria is an accepted standard for evaluating the security of a computing system

- ▶ IBM System z holds the **highest** commercial operating system Evaluation Assurance Level LPAR ratings at EAL 5+

- ▶ System z prevents unauthorized information flow between logical partitions so that confidential data remains protected

System z Integrated Access Control

- **RACF* provides the basis of security**
  - ▶ Access, Authorization, Auditing and Administration
  - ▶ Authenticates users through passwords or certificates
  - ▶ Unified access control for System z resources

- **Security enforced automatically by internal "router"**
  - ▶ You cannot bypass mainframe security mechanisms

- **A centralized security mechanism is more secure**
  - ▶ RACF security extends across the sysplex
  - ▶ Automatic switch to a backup RACF database when an error is detected on the primary

Resources Protected by RACF

Data	*Media*
▶ DB2	▶ Disk
▶ VSAM	▶ Tape
▶ IMS	▶ Print
▶ Files	▶ Console
	▶ Virtual switches, LANs
Subsystems	*Fine Grained*
▶ CICS	▶ Programs
▶ IMS	▶ Keys
▶ MQ	▶ Ports
▶ WebSphere	▶ Enterprise Java Beans
▶ JES	
▶ TSO	▶ Operator commands

Manage all your resources consistently as you build out new applications

* Resource Access Control Facility

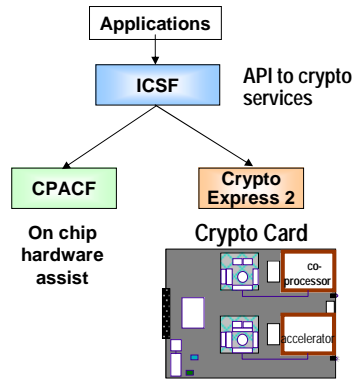# Protect Customer Data End-to-End

- **Access to data is protected by RACF**
  - ▶ RACF gives you the ability to:
    - − Identify and authenticate Users
    - − Log and report unauthorized access attempts
    - − Provides role-based access control

- **Data can be encrypted throughout its lifecycle**
  - ▶ On platform
    - − On System z with or without the use of crypto cards
  - ▶ Off platform
    - − Via tape encryption or network encryption

Built In Encryption on System z Protects Data Privacy

Applications

↓

ICSF — API to crypto services

↓ ↓

CPACF | **Crypto Express 2**

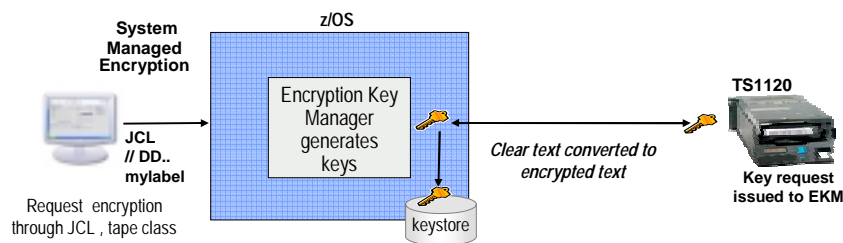**On chip hardware assist** | **Crypto Card**

co-processor

accelerator

- **Central Processor Assist for Cryptographic Function (CPACF)**
  - ▶ A CP Assist for Cryptographic Function (CPACF) is provided free of charge on every chip
  - ▶ Provides clear key encryption
- **Crypto Express2 Card**
  - ▶ High performance cryptography for SSL
    - – 6,000 handshakes per second
  - ▶ Secure key cryptography
  - ▶ Dynamically configurable
    - – Co-processor or Accelerator
  - ▶ FIPS 140-2 Level 4 compliant
  - ▶ Clears out memory if tampered with
- **Trusted Key Entry** (TKE) Workstation
  - ▶ Secured workstation for remote key entry

Prevent Exposure if the Tape Falls Off the Truck!

- **High performance tape encryption**
  - ▶ Protects data on lost tapes
  - ▶ Standard feature on all new TS1120 Tape Drives
  - ▶ Cost effectively encrypts all tape data
  - ▶ Offloads host encryption overhead

- **Leverages System z Key protection**
  - ▶ Create a key and store it securely - same key value can be available 20 years from now!
  - ▶ Policy for encryption specified on DFSMS Data Class
  - ▶ User never sees the key!

System Managed Encryption

z/OS

JCL // DD.. mylabel

Request encryption through JCL , tape class

Encryption Key Manager generates keys

keystore

Clear text converted to encrypted text

TS1120

Key request issued to EKM

System z Encryption Key Management
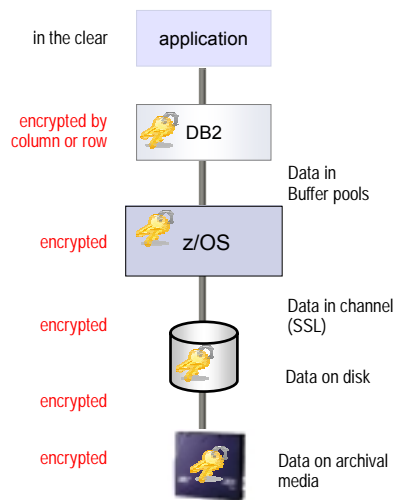
Encryption Key Manager (EKM)

- Java program that transparently generates, serves and maintains encryption keys

- **Provides a single point of control**
  - ▶ Simplified recovery of keys
  - ▶ Auditable through RACF
  - ▶ Over a decade of proven production use
  - ▶ Available at no additional charge

- **Helps protect and manage keys**
  - ▶ Generate and serves keys to tape drives
  - ▶ Uses tamper-resistant crypto cards to store "secure keys"
  - ▶ Can retrieve required keys from protected key stores

- **Options to store the keys**:
  - ▶ RACF protected key stores
  - ▶ Secure hardware
  - ▶ Other protected data sets, files

Protect Data Privacy Using DB2

- DB2 uses either clear key (CPACF) or secure key (Crypto Express2 card) for encryption

- DB2 supports encryption at every level:
  - ▶ In memory, buffers, disk, and archival media
  - ▶ Table, Index, logs, and backup copies
  - ▶ Data sent by remote access (DRDA)

- DB2 provides multiple options for table encryption:
  - ▶ Column level encryption
    - − Enabled by the application
  - ▶ Row level encryption
    - − IBM Encryption Tool for DB2

in the clear — application

encrypted by column or row — DB2

Data in Buffer pools

encrypted — z/OS

encrypted — Data in channel (SSL)

encrypted — Data on disk

encrypted — Data on archival media

Multi-Level Security (MLS) Supports Users with Different Security Clearances

Goals of Multi-Level Security

- Share one data base among organizations with different "need to know"
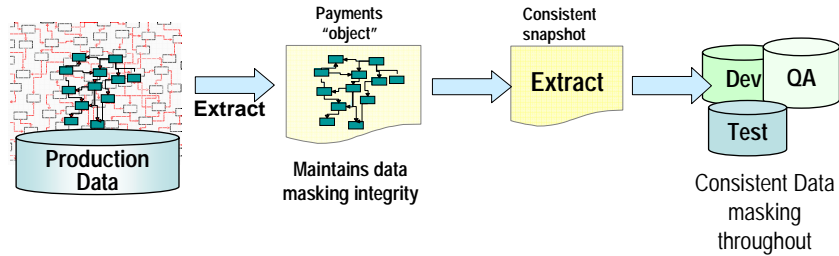- Prevent individuals from accessing information at a higher classification level than what is permitted

DB2 Multi-Level Security

- Restricts row level access to those with appropriate clearance
- Combines both low and high security data in the same database- eliminating redundant infrastructures

Underwriter

Claims Analyst

National Broker

SECURITY Classification	Revenue	Area	Loss
Business Broker	234	USA	50%
Underwriter	198	Ohio	23%
Claims analyst	2	Maine	9%
Underwriter	234	USA	11%
Claims analyst	87	Texas	14%
Affiliate broker	23	NewYork	20%
National broker	223	USA	10%
Affiliate broker	45	Canada	29%

Abraxas Informatik Uses RACF for Secure Outsourcing Services

- Abraxas Informatik AG is one of the largest governmental outsourcers in Switzerland

- Challenges Abraxas faced:
  - High levels of security were needed to handle confidential government information
  - Both CA ACF2 and Top Secret were installed, requiring staff knowledgeable in both
  - Abraxas needed to simplify their security structure, and reduce security expenses

- Solution:
  - Replaced ACF2 and TopSecret with RACF
  - RACF allowed Abraxas to quickly manage resource access and user accountability

- Results:
  - Abraxas now saves 200,000 Swiss francs or $US 180,042 annually
  - Abraxas is now better positioned to offer excellent security services while keeping its fees competitive

abraxas Informatik AG

Don't Forget to Protect Customer Data During Testing of New Releases

Payments "object"

Consistent snapshot

Extract

Extract

Production Data

Maintains data masking integrity
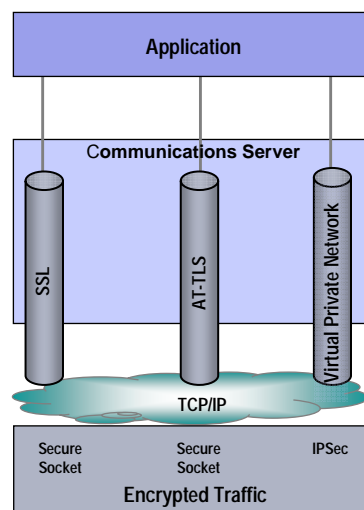
Dev   QA

Test

Consistent Data masking throughout

- Protect customer data throughout testing cycle with Optim
- Customer data can be compromised during testing cycles, especially during audits
- Mask or replace customer data with fictional data in a consistent manner preserving the integrity of data relationships
- Extract a snapshot for testing purposes

Supports many data formats:

DB2, Informix, IMS, VSAM, Oracle, others

Block Unauthorized Network Access

- z/OS Communication Server is the first line of defense against network attacks
  - ▶ Defensive IP filtering (built-in firewall)

- z/OS Communications Server provides multiple styles of encryption for network traffic
  - ▶ Application layer encryption
  - ▶ Network layer encryption
  - ▶ Support for Virtual Private Networks with IPSec

- Application Transparent Transport Level Security (AT-TLS) transparently encrypts application data

- SSL and IPSec processed by crypto processor if available
 - ▶ IPSec can be offloaded to zIIP

Application

Communications Server

SSL

AT-TLS

Virtual Private Network

TCP/IP

Secure Socket

Secure Socket

IPSec

Encrypted Traffic

*AT-TLS= application transparent transport level security

System z Communication Server Encrypts Network Data End-to-End

- Critical for companies that outsource their network yet want greater control over confidential data
- Other router based encryption alternatives expose data in the clear and lack the intrusion detection capabilities of the mainframe.

System z - End-to-end encryption

Encryption with routers can leave gaps
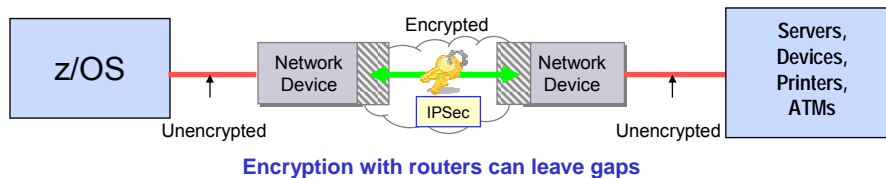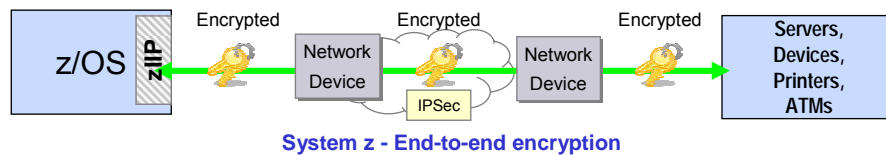
RACF Security Event Logging

- RACF helps you to audit access control and accountability:
  - ▶ Started during IPL to prevent vulnerabilities from being introduced
  - ▶ Audit control functions specify the information RACF should log
  - ▶ SMF log datasets themselves are protected
  - ▶ RACF SMF data unload utility converts SMF records into formats used by other tools

- RACF logs many events:
  - ▶ All accesses to specific data sets, general resources
  - ▶ All accesses to a specified class of resources at a specified access level
  - ▶ All attempts to access a resource with a security level of confidential
  - ▶ RACF-related activities of specific users
  - ▶ Unauthorized attempts to use RACF commands
  - ▶ All RACF commands issued by users who have SPECIAL authority
 - ▶ Changes to any RACF profiles

# Common Logging Simplifies Security Compliance Monitoring

- The mainframe offers comprehensive auditing capabilities for all its subsystems
  - Unified access control with RACF
  - Common logging of RACF security events

- Enables the monitoring of users and their activities

- System z's common logging avoids integration and compliance challenges posed by multiple inconsistent and incompatible log formats

With other systems, customers have to manually make sense out of all these different log formats

---
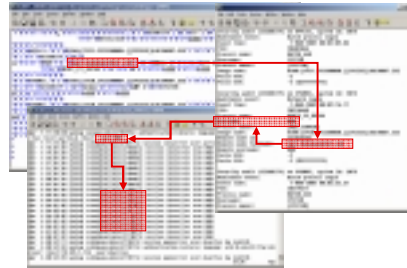
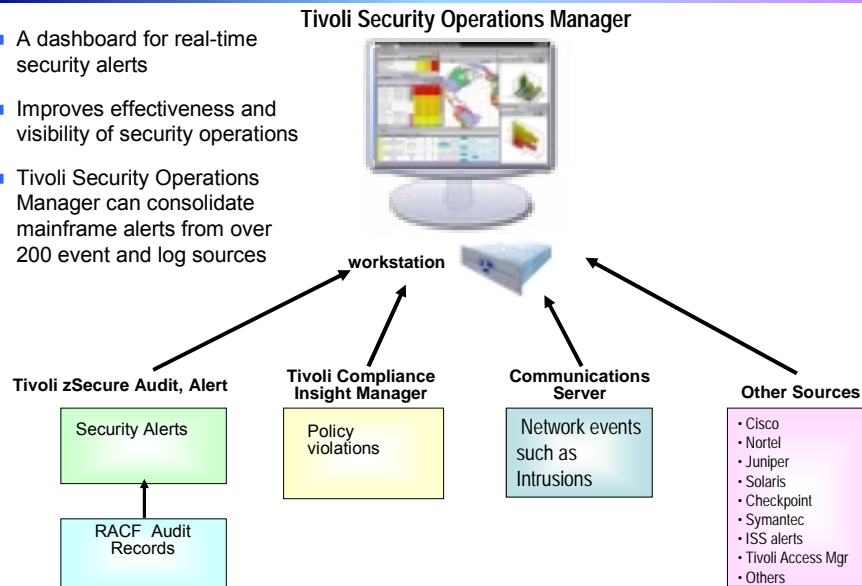# Tivoli zSecure Suite Extends System z Security management

- Tivoli zSecure Alert
  - Can issue alerts when conditions occur
  - Provides real-time threat monitoring for z/OS and RACF
  - Can take action to stop security breaches
  - New RACF offline option simulates impact of RACF changes

- Tivoli zSecure Audit
  - Provides real-time exception alerts
  - An audit and reporting tool for the mainframe
  - Built-in knowledge base identifies exposures
  - Can check integrity of sequential log data residing on tape or disk

- Tivoli zSecure Command Verifier
  - Prevent erroneous RACF commands from executing
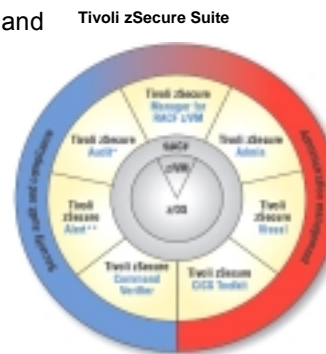
Tivoli zSecure Suite

Tivoli Security Operations Manager (TSOM)

Tivoli Security Operations Manager

- A dashboard for real-time security alerts

- Improves effectiveness and visibility of security operations

- Tivoli Security Operations Manager can consolidate mainframe alerts from over 200 event and log sources
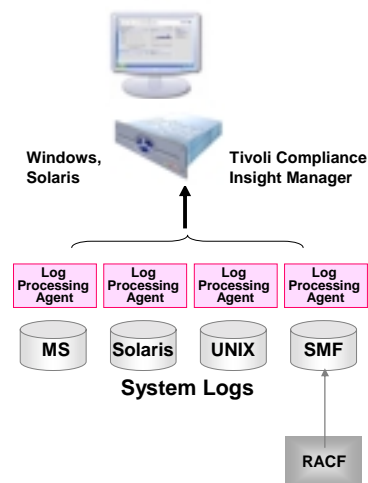
workstation

Tivoli zSecure Audit, Alert

Security Alerts

RACF Audit Records

Tivoli Compliance Insight Manager

Policy violations

Communications Server

Network events such as Intrusions

Other Sources

- Cisco
- Nortel
- Juniper
- Solaris
- Checkpoint
- Symantec
- ISS alerts
- Tivoli Access Mgr
- Others

06 - Extend Data Security on the Mainframe v5.1.ppt

22

Tivoli Compliance Insight Manager Provides System Wide Security Management

- Captures log data on security events from multiple systems

- Correlates data to identify audit risks
  - Unique "W7" format: *w*ho, *w*hat, on *w*hat, *w*here, *w*hen, from *w*here, to *w*here
  - Makes log data easy to understand

- Analysis engine provides a deeper, intelligent analysis of collected data
  - Trace last person to touch a particular resource
  - Link access to resources by users

Windows, Solaris

Tivoli Compliance Insight Manager

Log Processing Agent | Log Processing Agent | Log Processing Agent | Log Processing Agent

MS | **Solaris** | **UNIX** | **SMF**
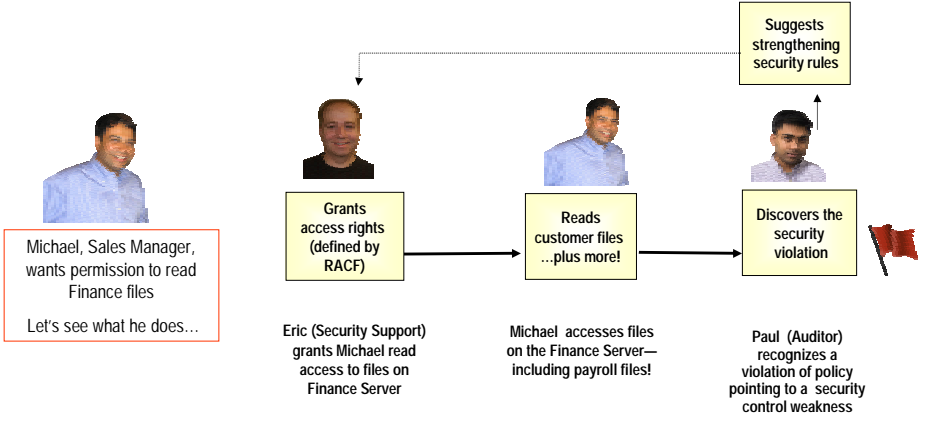
System Logs

RACF

06 - Extend Data Security on the Mainframe v5.1.ppt

23

DEMO: Tivoli Compliance Insight Manager

- Broad file access permission is often granted to privileged users
- But through fraud or accident, privileges may be abused
- Suspicious activity and policy violations are detected by TCIM
- These activities may uncover weak security controls
- Regulatory impact too; Sarbanes-Oxley requires strong security controls

Suggests strengthening security rules

Grants access rights (defined by RACF)

Reads customer files ...plus more!

Discovers the security violation

Michael, Sales Manager, wants permission to read Finance files

Let's see what he does...

Eric (Security Support) grants Michael read access to files on Finance Server

Michael accesses files on the Finance Server— including payroll files!

Paul (Auditor) recognizes a violation of policy pointing to a security control weakness

06 - Extend Data Security on the Mainframe v5.1.ppt   24

Mainframe Extension Solution – Data Security
Make the Most of What You Already Have!

System z	System z trusted base	Workload isolation and storage protection, common criteria evaluation
	z/OS	Avoid need for extra virus control mechanisms or firewalls with System z architecture
	SMF, RACF	Built in logging with SMF records in a consistent format, turn on logging, use RACF to log events
Data Security	RACF	MLS capabilities of RACF, DB2 provide granular security to support different classification schemes
	CPACF	Entitled clear key cryptography
	EKM	Provides the ability to issue, maintain and retrieve cryptographic keys
Communications	z/OS Communications Server	Provides intrusion defense , policy management as well as secured communications
	AT –TLS	Communications Server of System z provides easily accessible encrypted communications for applications

Further extend security

Encryption	TS 1120 tape drive and C06 CU	Secured tape drive with encryption capabilities built in
	2 Crypto Express2 Cards	Buy crypto cards for acceleration and co-processing
	zIIPs (Comm Server + zIIP)	Leverage zIIPs for IPSec
Compliance And Testing	zSecure	Simplifies administration and provides auditing analysis tools
	TSOM	Tivoli Security Operations Manager provides advanced network and systems security event management
	TCIM	Tivoli Compliance Insight Manager provides auditing and compliance reporting
	Optim	Optim provides testing while protecting data confidentiality

06 - Extend Data Security on the Mainframe v5.1.ppt   25

The Cost of a Data Security Breach

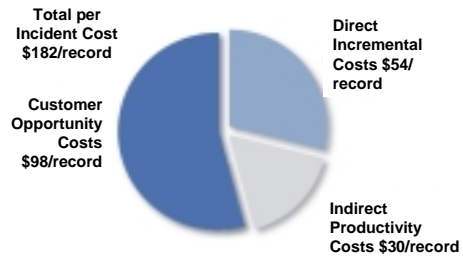- **Total per-incident costs** including average direct, indirect, and opportunity costs:
  - ▶ $182 per record, or $4.8 million per company

- Range of surveyed breach costs:
  - ▶ $226,000 to $22 million per incident

- Each incident resulted in an average 2 percent loss of existing customers
  - ▶ Worst case was 7 percent

Total per Incident Cost $182/record

Customer Opportunity Costs $98/record

Direct Incremental Costs $54/ record

Indirect Productivity Costs $30/record

Ponemon Study: 2006 Survey Cost of a Data Breach

Case Study: Mainframe Extension Solution – Deploy New Security Capabilities

Existing Mainframe

Add mainframe compliance & management products

Prod

3 year cost of acquisition $3.83M

Existing z10:
6 GP 4,000 MIPS
1 zIIP
Tape CU
DB2 workload
z/OS, RACF
Communications Server
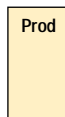
Incremental:
1 zIIP for IPSec
2 TS1120 tape drives
2 Crypto Express2 cards
2 Intel servers
zSecure
TSOM/ TCIM bundle
Optim

According to the Ponemon Study: 2006 Survey Cost of a Data Breach, the average incident costs $4.8M

Service Oriented Finance
CEO