Security in a Distributed Environment
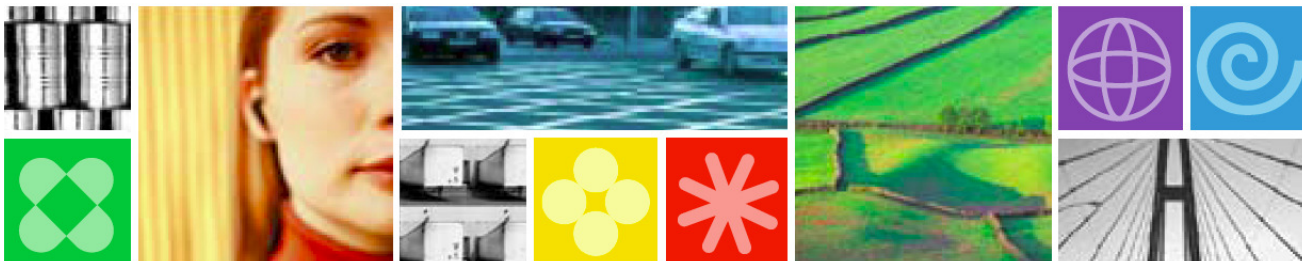
The role of the Mainframe

Jim Porell
IBM Distinguished Engineer
IBM System z Business Development

Cross Domain Risks

- **LAN and Network Security**

- **Secure Sign in**

- **Cross Domain Authentication**

- **Self Signed Certificates**

- **Certificate Management**

- **Data privacy**
  - Developers
  - PII data

- **Abhorrent behavior**

- **Insider Theft**

- **Forensics**

- **Prevention**

❑ **Transaction processing**
  - Point of sale
  - Claims processing
  - Credit/Debit/Transfer
  - Working off an operational data store (ODS)

❑ **Data Mining/Data warehouse**
  - Batch operations – many times not on the operational data store
  - Looking for new business opportunities

❑ **Operational Risk (OR)**
  - Leverages the data base
  - Originally, it was also using a copy of the ODS for detection purposes
    - After 9/11, this proved to be inefficient. Fraud occurs during the batch window
  - Now OR is more preventative, so it must work off of real time data
    - Additions to any OR database must also be considered in real time vs batch

Security on System z: Reducing risk for the Enterprise
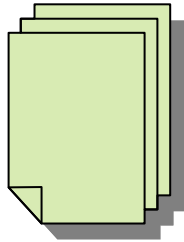
| Basic Insurance Policy | Basic Security: System z |
| $100,000 Liability | RACF |

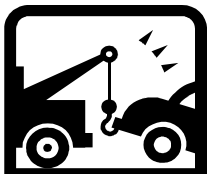| Rider: Excess replacement for valuable items | Data Encryption services Enterprise Key mgt |

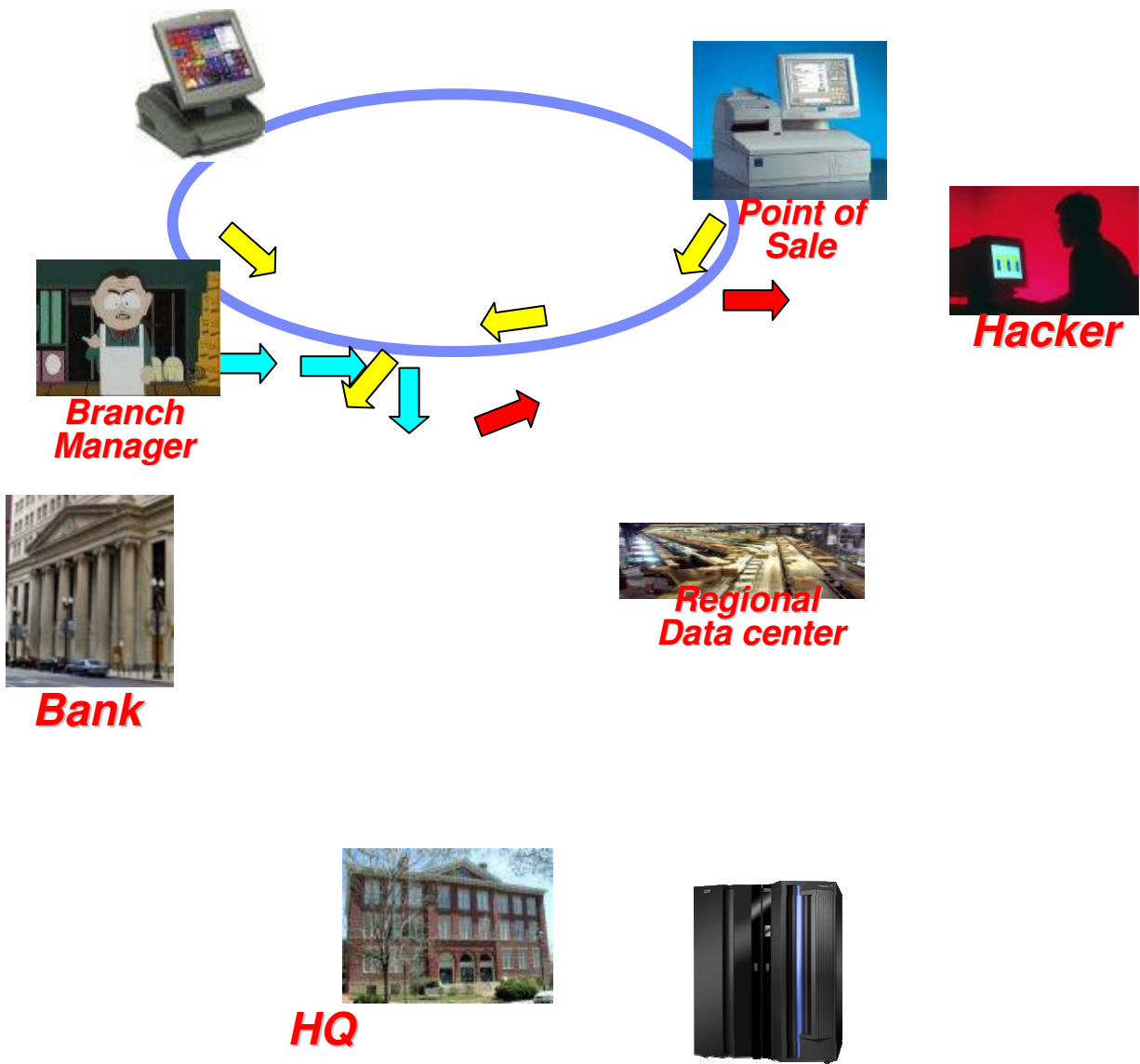| Rider: Excess medical coverage | Identity Management |

| Rider: Unlimited vehicle towing | Compliance Reporting |

| Rider: Excess liability insurance $3,000,000 | Fraud Prevention, Forensics and Analytics |

Point of Sale

Hacker

Branch Manager

Bank

Regional Data center

HQ

```
ERROR: stackunderflow
OFFENDING COMMAND: ~

STACK:
```