Optim™

Data Privacy...The Internal Threat of Which You May Not be Aware

Eric Offenberg, CIPP, MBA

Business Development Manager

IBM Software Group

Agenda

- The Latest on Data Privacy
- Understanding Data Governance
- The Easiest Way to Expose Private Data
- Understanding the Insider Threat
- Success Stories

The Latest on Data Privacy

- **2007 statistics**
  - **$197**
    - Cost to companies per compromised record
  - **$6.3 Million**
    - Average cost per data breach “incident”
  - **40%**
    - % of breaches where the responsibility was with Outsourcers, contractors, consultants and business partners
  - **235 Million**
    - TOTAL number of records containing sensitive personal information involved in security breaches in the U.S. since 2005

* Sources”: Ponemon Institute, Privacy Rights Clearinghouse, 2007

Did You Hear?

- •Hannaford Supermarket chain (165 stores in New York and New England) recently confirmed a data intrusion of 4.2 million credit/debit cards
- •Included were Sweetbay stores in Florida (106 stores)
- • 1800 reported cases of fraud thus far
- • This merchant claimed PCI compliance!

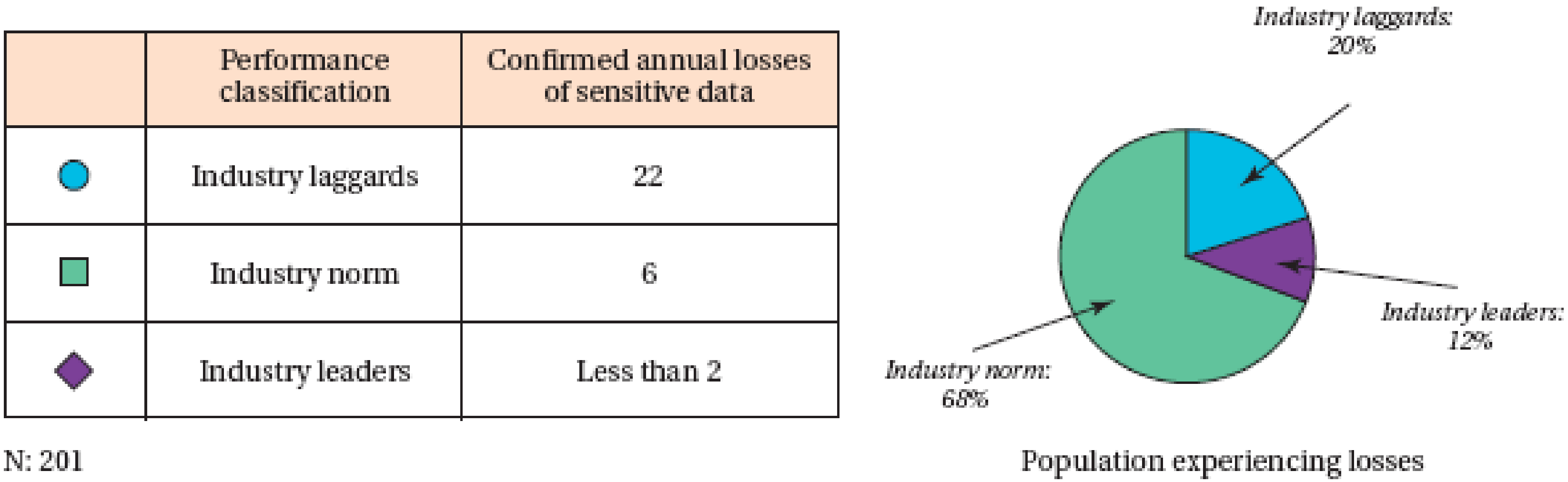
How much is personal data worth?

- **Credit Card Number With PIN - $500**
- **Drivers License - $150**
- **Birth Certificate - $150**
- **Social Security Card - $100**
- **Credit Card Number with Security Code and Expiration Date - $7-$25**
- **Paypal account Log-on and Password - $7**

Representative asking prices found recently on cybercrime forums.

Source: USA TODAY research 10/06

Where do F1000 Corporations Stand today?



	Performance classification	Confirmed annual losses of sensitive data
●	Industry laggards	22
🟩	Industry norm	6
◆	Industry leaders	Less than 2

N: 201

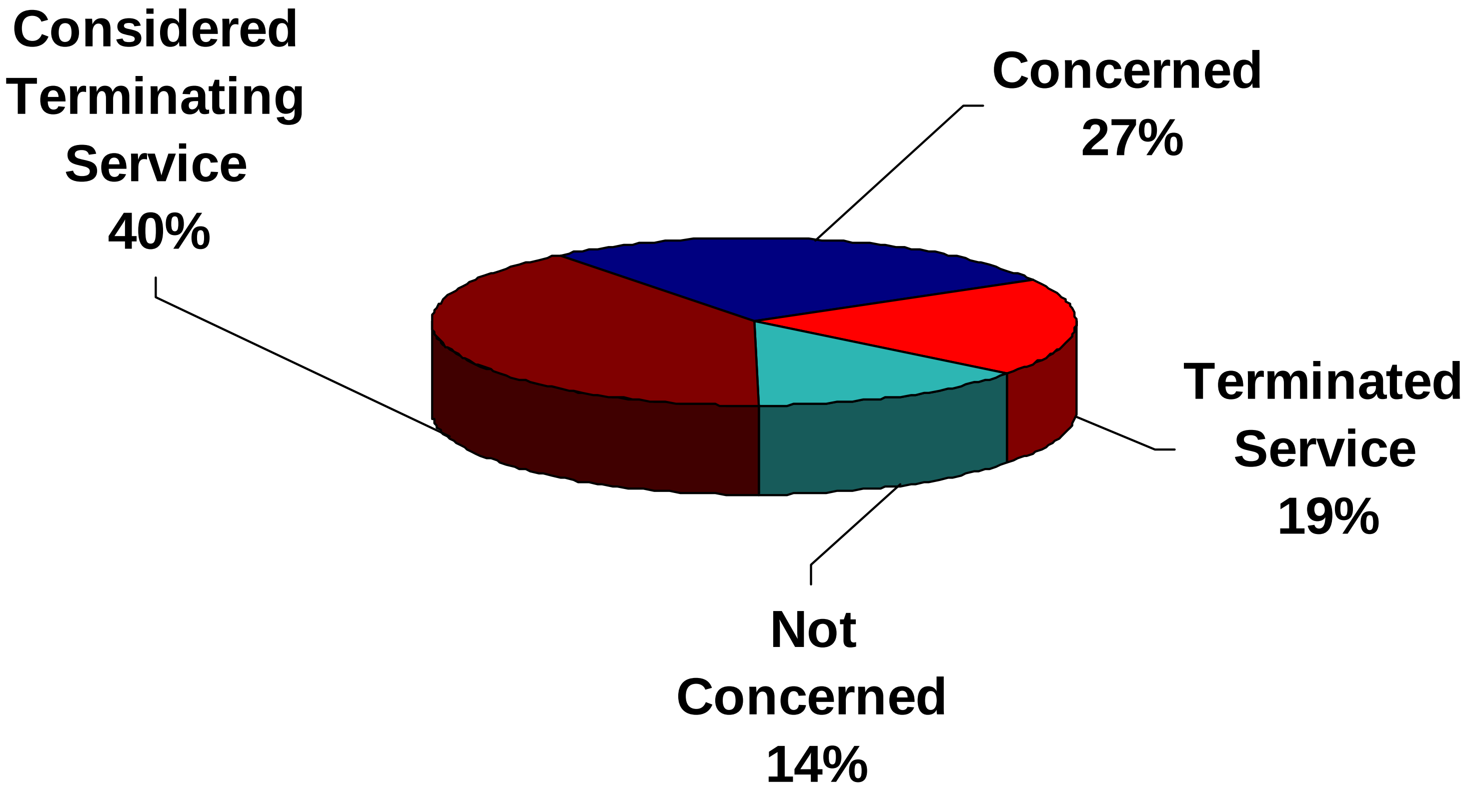
Population experiencing losses

Figure 1: Sensitive data loss results

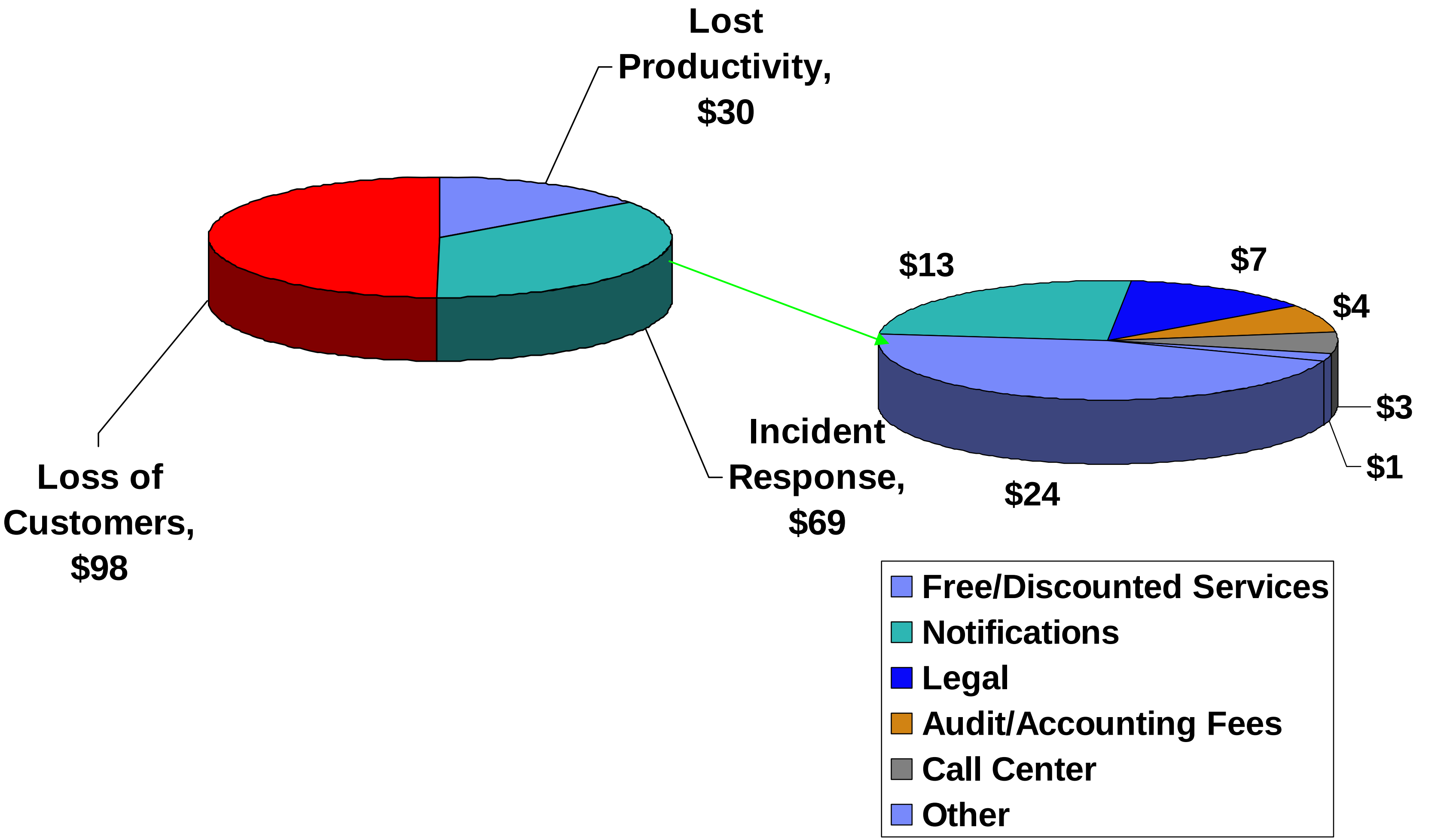
Source: IT Policy Compliance Group, 2007

Consumer Reaction

Banking Customer Survey (Ponemon Institute)



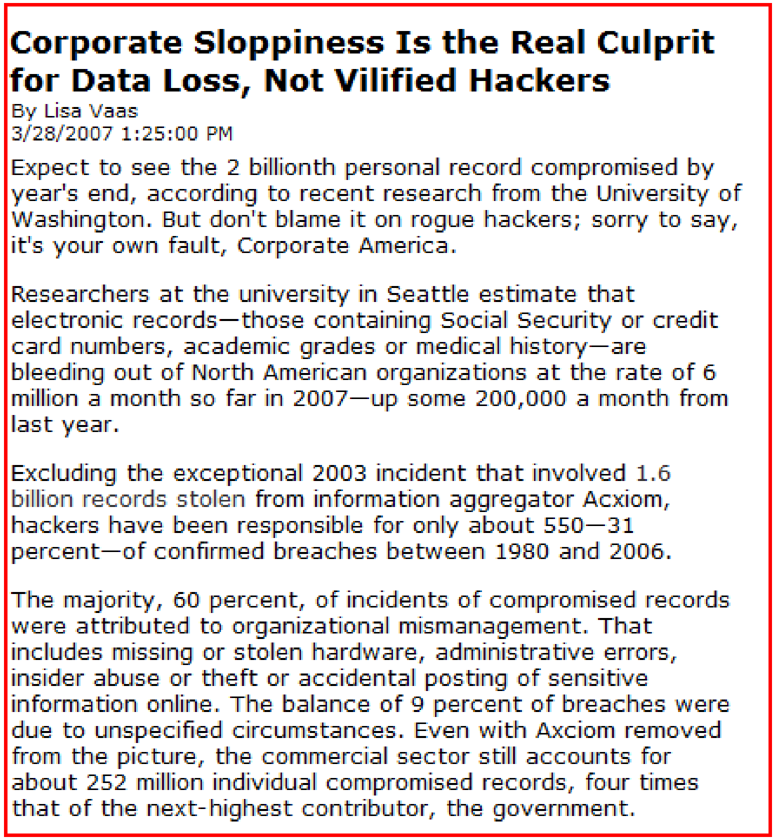
Cost to Company per Missing Record: $197



Source: Ponemon Institute

Without Data Governance…

- **People make mistakes…**
- **Those mistakes more commonly result in losses than hackers…**
- **Those losses effect every aspect of IT and business**
- **But data is still an abstract concept and governance needs technology to be improved…**



Corporate Sloppiness Is the Real Culprit for Data Loss, Not Vilified Hackers

By Lisa Vaas
3/28/2007 1:25:00 PM

Expect to see the 2 billionth personal record compromised by year's end, according to recent research from the University of Washington. But don't blame it on rogue hackers; sorry to say, it's your own fault, Corporate America.

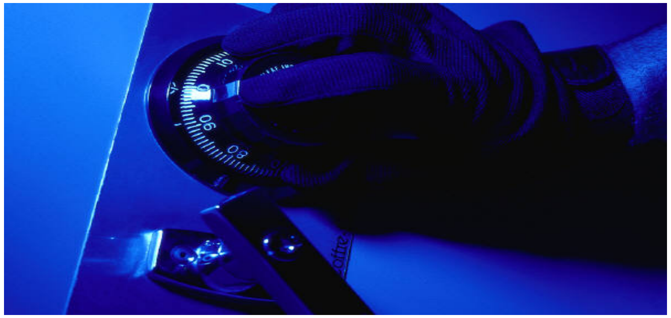
Researchers at the university in Seattle estimate that electronic records—those containing Social Security or credit card numbers, academic grades or medical history—are bleeding out of North American organizations at the rate of 6 million a month so far in 2007—up some 200,000 a month from last year.

Excluding the exceptional 2003 incident that involved 1.6 billion records stolen from information aggregator Acxiom, hackers have been responsible for only about 550—31 percent—of confirmed breaches between 1980 and 2006.

The majority, 60 percent, of incidents of compromised records were attributed to organizational mismanagement. That includes missing or stolen hardware, administrative errors, insider abuse or theft or accidental posting of sensitive information online. The balance of 9 percent of breaches were due to unspecified circumstances. Even with Axciom removed from the picture, the commercial sector still accounts for about 252 million individual compromised records, four times that of the next-highest contributor, the government.

Why the focus on Data Governance?

- Regulatory Compliance
  - Consumer privacy
  - Financial Integrity
- Intellectual Property Theft
  - Confidential manufacturing processes
  - Financial information
  - Customer lists
  - Digital source code
  - Marketing strategies
  - Research data
- Economic Espionage
  - Trade secret



State sues global management consulting company over stolen backup tape. Unencrypted tape contained personal information on 58 taxpayers and nearly 460 state bank accounts.

Over 45 million credit and debit card numbers stolen from large retailer. Estimated costs $1bn over five years (not including lawsuits). $117m costs in 2Q '07 alone.

What is Done to Protect Data Today?

- **Production “Lockdown”**
  - Physical entry access controls
  - Network, application and database-level security
  - Multi-factor authentication schemes (tokens, biometrics)
- **Unique challenges in Development and Test**
  - Replication of production safeguards not sufficient
  - Need “realistic” data to test accurately

The Easiest Way to Expose Private Data … Internally with the Test Environment

- **70% of data breaches occur internally (Gartner)**
- **Test environments use personally identifiable data**
- **Standard Non-Disclosure Agreements may not deter a disgruntled employee**
- **What about test data stored on laptops?**
- **What about test data sent to outsourced/overseas consultants?**
- **How about Healthcare/Marketing Analysis of data?**
- **Payment Card Data Security Industry Reg. 6.3.4 states,** "Production data (real credit card numbers) cannot be used for testing or development"

*** The Solution is Data De-Identification ***

The Latest Research on Test Data Usage

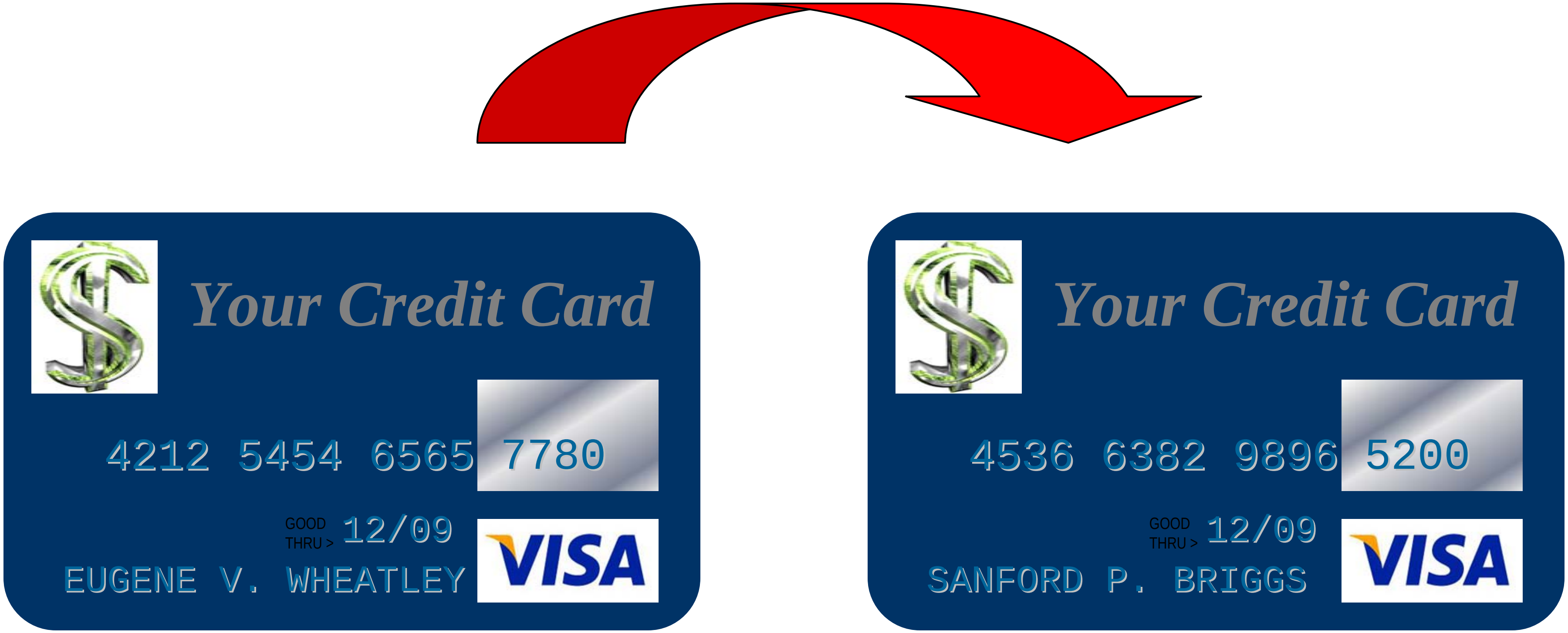
- **Overall application testing/development**
  - 62% of companies surveyed use actual customer data instead of disguised data to test applications during the development process
  - 50% of respondents have no way of knowing if the data used in testing had been compromised.
- **Outsourcing**
  - 52% of respondents outsourced application testing
  - 49% shared live data!!!
- **Responsibility**
  - 26% of respondents said they did not know who was responsible for securing test data

Source: The Ponemon Institute. The Insecurity of Test Data: The Unseen Crisis

What is Data De-Identification?

- **AKA data masking, depersonalization, desensitization, obfuscation or data scrubbing**
- **Technology that helps conceal real data**
- **Scrambles data to create new, legible data**
- **Retains the data's properties, such as its width, type, and format**
- **Common data masking algorithms include random, substring, concatenation, date aging**
- **Used in Non-Production environments as a Best Practice to protect sensitive data**

Masking is transparent to the outside world



Card Holder and Card Number have been masked

Failure Story – A Real Life Insider Threat

- **28 yr. old Software Development Consultant**
- **Employed by a large Insurance Company in Michigan**
- **Needed to pay off Gambling debts**
- **Decided to sell Social Security Numbers and other identity information pilfered from company databases on 110,000 Customers**
- **Attempted to sell data via the Internet**
  - Names/Addresses/SS#s/birth dates
  - 36,000 people for $25,000
- **Flew to Nashville to make the deal with…..**
- **The United States Secret Service (Ooops)**

Results:

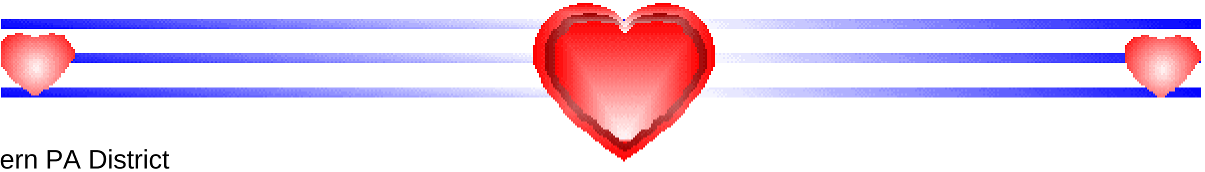
- Sentenced to 5 Years in Jail
- Order to pay company $520,000

The Top 3 Reasons Why Insiders Steal Data

1. **Greed**

2. **Revenge**

3. **Love**



Source: US Attorney General’s Office, Eastern PA District

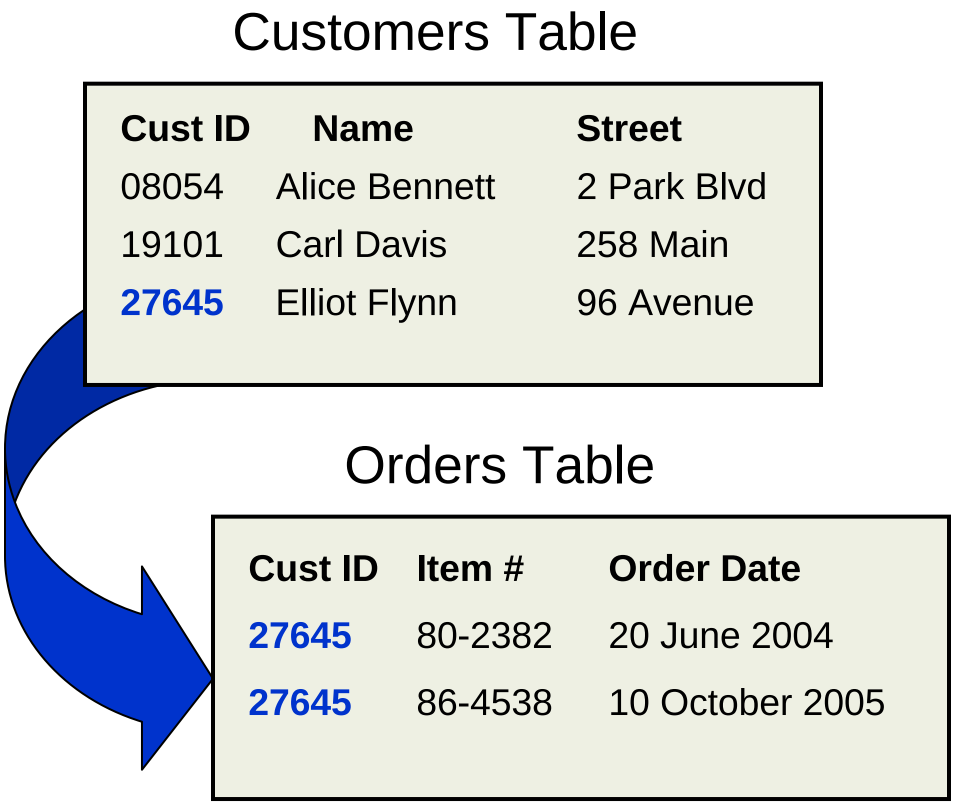
How is Risk of Exposure being Mitigated?

- **No laptops allowed in the building**
- **Development and test devices**
  - Do not have USB
  - No write devices (CD, DVD, etc.)
- **Employees sign documents**
- **Off-shore development does not do the testing**
- **The use of live data is ‘kept quiet’**

Encryption is not Enough

- **DBMS encryption protects DBMS theft and hackers**
- **Data decryption occurs as data is retrieved from the DBMS**
- **Application testing displays data**
  - Web screens under development
  - Reports
  - Date entry/update client/server devices
- **If data can be seen it can be copied**
  - Download
  - Screen captures
  - Simple picture of a screen

Propagating Masked Data



Customers Table

Cust ID	Name	Street
08054	Alice Bennett	2 Park Blvd
19101	Carl Davis	258 Main
27645	Elliot Flynn	96 Avenue

Orders Table

Cust ID	Item #	Order Date
27645	80-2382	20 June 2004
27645	86-4538	10 October 2005

- **Key propagation**
  - Propagate values in the primary key to all related tables
  - Necessary to maintain referential integrity

“We're not going to solve this by making data hard to steal. The way we're going to solve it is by making the data hard to use.”

Bruce Schneier, author of "Beyond Fear: Thinking Sensibly About Security in an Uncertain World"

Thank
You