




 What makes you special?

# Security and Compliance Management: From IT Burden to Business Enabler

**Marc van Zadelhoff**  
*Program Director, Business Development*  
IBM



IBM Governance and Risk Management   
Business alignment, visibility and control



# Agenda

- Security Shifts...
- ... Regulators Awaken ...
- ... Can I Get a Pay Raise?! (e.g., PCI's a lotta work!)
- IBM Customers' Stories
- Questions and Answers



# Remember the Good Old Days?

Unknown people...

... doing bad things ...

... Intentionally

# The most publicized threat



## The *Unknown People* Threat: Examples of old...



**Chen-Ing Hau**  
**CIH Virus**



**Joseph McElroy**  
**Hacked US Dept  
of Energy**



**Jeffrey Lee  
Parson**  
**Blaster-B  
copycat**

## The *Unknown People* Threat: ... newer examples



**Jeremy  
Jaynes**  
**\$24M SPAM  
KING**



**Jay Echouafni**  
**Competitive  
DDoS**



**Andrew  
Schwarmkoff**  
**Russian Mob  
Phisher**

Photos from colleagues at F-Secure



## And it gets worse



### T.J. Maxx Parent Company Data Theft Is The Worst Ever

The intrusion hands the retailer the dubious honor of surpassing the 40 million stolen customers record mark, something that only CardSystems had been able to achieve.

By Larry Greenemeier, InformationWeek [InformationWeek](#)  
March 29, 2007

TJX Co., the parent company of T.J. Maxx and other retailers, on Wednesday dropped a bombshell in its ongoing investigation of a customer data breach by announcing in a security and exchanges commission filing that more than 45 million credit and debit card numbers have been stolen from its IT systems. Information contained in the filing reveals a company that had taken some measures over the past few years to protect customer data through obfuscation and encryption. But TJX didn't apply these policies uniformly across its IT systems and as a result still has no idea of the extent of the damage caused by the data breach.

As a result, TJX is a company under siege. The company recorded a fourth-quarter charge of about \$5 million to cover the costs of containing and investigating the breach, as well as improving the security of its IT systems, communicating with customers, and paying legal fee. The U.S. Federal Trade Commission has launched an investigation of TJX. While the FTC wouldn't reveal the nature of the investigation or when it began, it's likely the result of the data breach. And lawsuits have begun to fly, including one by the Arkansas Carpenters Pension Fund, which owns 4,500 shares of TJX stock.

The intrusion into TJX's IT systems also hands the retailer the dubious honor of surpassing the 40 million stolen customers record mark, something that only CardSystems had been able to achieve. And it puts to shame the Veterans Affairs Department, which last year briefly lost track of more than 26 million records thanks to a stolen employee laptop.



... but if that looks scary...

... What about this?





## Massive Insider Breach at DuPont

**February 15, 2007 – A research chemist who worked for DuPont for 10 years before accepting a job with a competitor downloaded 22,000 sensitive documents and viewed 16,706 more ...**

“The best way to guard against insider breaches is for companies to **monitor database and network access for unusual activity** and set thresholds that represent acceptable use for different users.”

### What occurred:

- Employee leaving for competitor
- Accessed database
- Transferred 180 documents to new laptop

### Carnegie Mellon CERT Comments:

- “75% of ... confidential information thefts studied ... were committed by current employees”
- “45% had already accepted a job offer with another company”

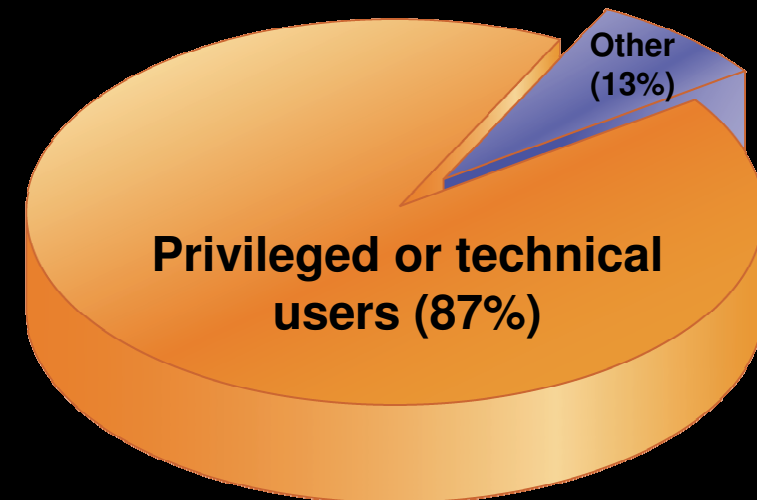
### CIA Comments:

- “...designers and scientists tend to view their company's intellectual property as their own... and something they want to take with them”

## Known People (un) Intentionally Do Great Harm

- **87% of insider incidents are caused by privileged or technical users**
- **Many are inadvertent violations of:**
  - Change management process
  - Acceptable use policy
- **Others are deliberate, due to:**
  - Revenge (84%)
  - “Negative events” (92%)
- **Regardless, too costly to ignore:**
  - Internal attacks cost 6% of gross annual revenue
  - Costing \$400 billion in the US alone

### Who Causes Internal Incidents?





# Agenda

- Security Shifts...
- ... Regulators Awaken ...
- ... Can I Get a Pay Raise? (e.g., PCI's a lotta work!)
- IBM Customers' Stories
- Questions and Answers



## What is Compliance?

- Compliance
  - Acting according to certain accepted standards
    - Princeton University WordNet
      - <http://wordnet.princeton.edu/perl/webwn?s=compliance>
  
- Regulatory Compliance
  - The combined set of organizational capabilities, processes, supporting infrastructure and tools, data and information, and operational and financial controls required to satisfy the requirements set forth by all applicable regulatory agencies

# Key Regulations Affecting IT and Compliance

## Privacy Regulations

1999 Gramm-Leach-Bliley Act (GLBA) US	2000 PIPEDA Canada	2000 COPPA and CIPA US	2003 California Individual Privacy (SB1386) California	<b>2006 PCI DSS v1.1 Industry</b>
1987 Computer Security Act US	1995 EU Data Protection Directive EU	1996 HIPAA US	1997 Personal Health Information Act Canada	1998 Data Protection Act UK

## Financial Integrity and Solvency Regulations

2005 8th Company Law Directive (Euro SOX) EU	2006 Financial Instruments and Exchange Law (J-SOX) Japan	2012 Solvency II EU
2002 Sarbanes-Oxley Act US	2002 Corporate Law Economic Reform Program Australia	2003 Basel II EU

## Other Regulations

2006 Federal Rules of Evidence US
2001 USA PATRIOT Act US



## Common Denominator: Risk Management

- Regulatory compliance initiatives involve reducing the risk of adverse events
  - Sarbanes Oxley compliance initiatives require reducing the risk that the financial reporting processes, systems and data lack integrity and accuracy
  - PCI Data Security Standard compliance initiatives require reducing the risk that cardholder data will be subject to inappropriate access or theft
- Common Steps for Risk Management Crosses Many Regulations
  - Evaluation of control environment
  - Risk assessment
  - Control testing
  - Remediation
  - Ongoing Monitoring



## Compliance Mandates Dictate Protecting Narrow Classes of Assets

Asset Class	Systems	Transaction	Process	Information
<b>Compliance Mandate</b>	<ul style="list-style-type: none"> <li>▪ FISMA</li> <li>▪ DCID</li> <li>▪ NISPOM</li> </ul>	<ul style="list-style-type: none"> <li>▪ FISMA</li> <li>▪ DCID</li> <li>▪ NISPOM</li> </ul>	<ul style="list-style-type: none"> <li>▪ SOX</li> <li>▪ Basel II</li> </ul>	<ul style="list-style-type: none"> <li>▪ HIPAA</li> <li>▪ GLBA</li> <li>▪ PCI</li> </ul>
<b>Basic Requirement</b>	<ul style="list-style-type: none"> <li>▪ Assure the availability and integrity of critical infrastructure assets for the purpose of ensuring the public good</li> </ul>	<ul style="list-style-type: none"> <li>▪ Assure the availability and integrity of critical infrastructure assets for the purpose of ensuring the public good</li> </ul>	<ul style="list-style-type: none"> <li>▪ SOX: Assure the integrity and availability of the financial reporting process in order to protect the individual shareholder</li> <li>▪ BASEL II: For the good of the shareholder, ensure the integrity and availability of the IT domain through effective IT governance</li> </ul>	<ul style="list-style-type: none"> <li>▪ Assure the confidentiality, integrity, and availability of select data sets collected from private citizens.</li> </ul>
<b>Buzzwords</b>	<ul style="list-style-type: none"> <li>▪ Hackers</li> <li>▪ Crackers</li> <li>▪ Trojans</li> <li>▪ DOS</li> </ul>	<ul style="list-style-type: none"> <li>▪ Hackers</li> <li>▪ Crackers</li> <li>▪ Trojans</li> <li>▪ DOS</li> </ul>	<ul style="list-style-type: none"> <li>▪ IT Governance</li> </ul>	<ul style="list-style-type: none"> <li>▪ Acceptable Use of Information</li> </ul>
<b>Concern owner</b>	<ul style="list-style-type: none"> <li>▪ IT</li> <li>▪ IS</li> </ul>	<ul style="list-style-type: none"> <li>▪ IT</li> <li>▪ IS</li> </ul>	<ul style="list-style-type: none"> <li>▪ CXO</li> </ul>	<ul style="list-style-type: none"> <li>▪ CISO</li> <li>▪ Privacy Officer</li> <li>▪ Internal Audit</li> </ul>



## Compliance Challenges

**Companies face increased pressure to achieve and maintain compliance – all with limited resources, time and budget.**

- “Through 2010, public companies that do not adopt a compliance management architecture will spend 50 percent more annually than their peers to achieve Sarbanes-Oxley compliance.”  
– Gartner Group
- “As companies look to make SOX compliance more efficient and repeatable and improve controls reliability, technology is becoming a key enabler of these efforts...Corporate governance, including Sarbanes-Oxley, remains one of the top five priorities for North American IT organizations in 2006.”  
– Forrester Research



- **43% of CFOs think that improving governance, controls and risk management is their top challenge.**

64% of CIOs feel that the most significant challenges facing IT organizations are security, compliance and data protection

*CFO Survey: Current state & future direction, IBM Business Consulting Services*

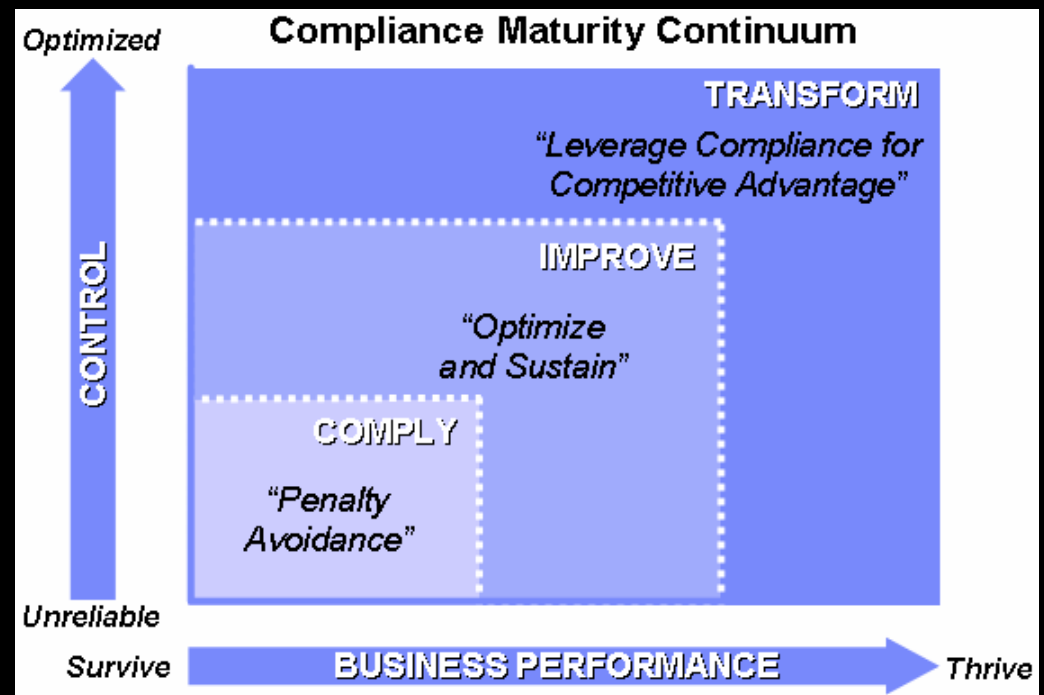
*IBM Service Management Market Needs Study, March 2006*



# Compliance Requirement... and opportunity?

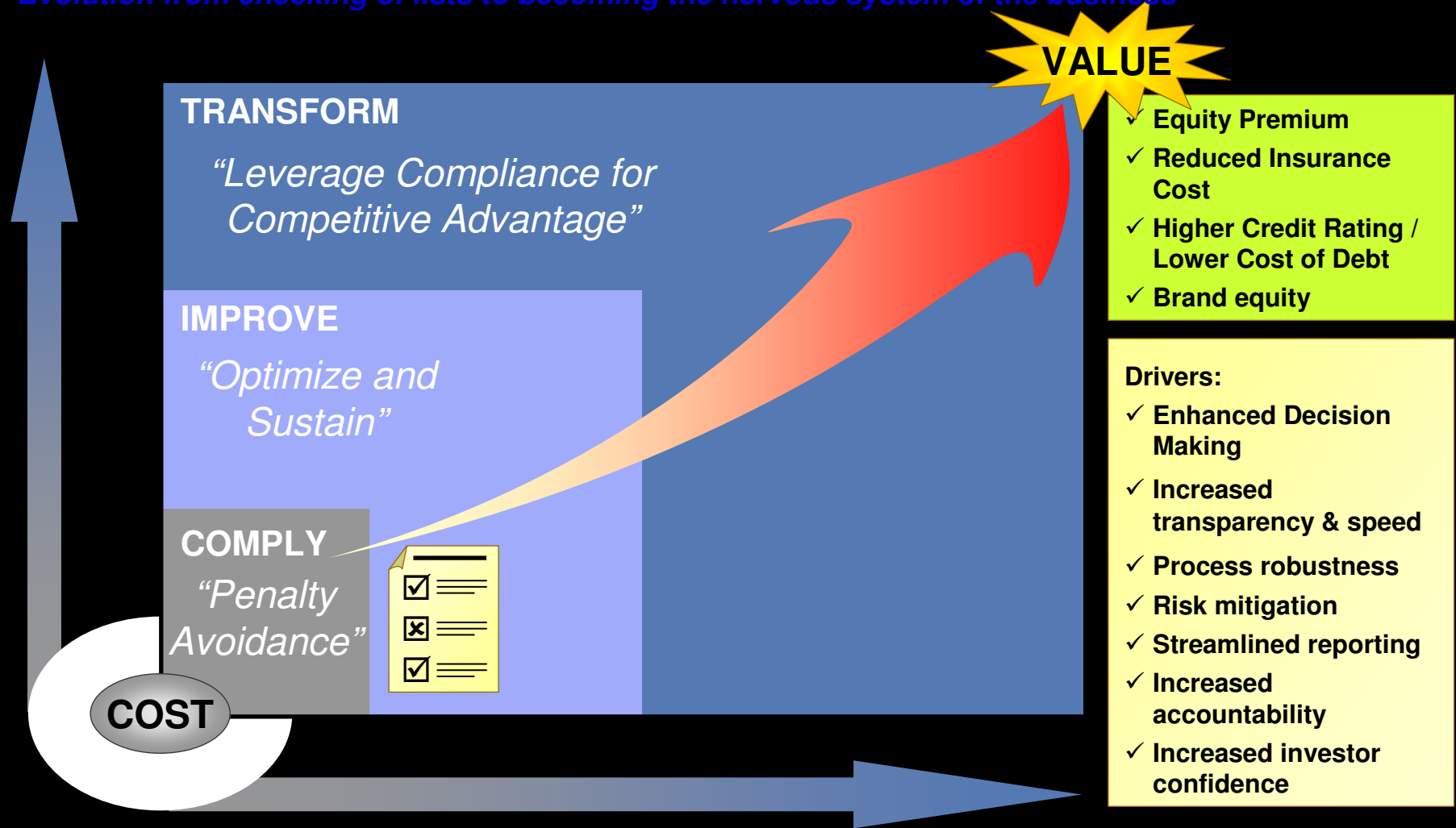
***“If companies view the new laws as opportunities – opportunities to improve internal controls, improve the performance of the board, and improve their public reporting – they will ultimately be better run, more transparent, and therefore more attractive to investors.”<sup>1</sup>***

*William Donaldson  
former SEC Chairman*



# Key Stages in Maturation along the Risk & Compliance Management Continuum

*Evolution from checking of lists to becoming the nervous system of the business*



# CIOs with effective IT governance and risk management ...

## Enhance business performance

- *Maintain visibility of end to end service to help ensure service quality*
- *Improve time to value and manage costs of strategic initiatives*

## Improve business resilience

- *Reduce risks and protect confidential intellectual property*
- *Minimize and control impact of planned and unplanned disruptions*

## Achieve compliance

- *Create alignment with internal and external policies and regulations*
- *Effectively prioritize and get more value from IT investments*



The screenshot shows the Washington section of The New York Times website. The main article is titled "In Turnaround, Industries Seek U.S. Regulations" by Eric Lipton and Gardiner Harris, published on September 16, 2007. The article discusses how industries are pushing for federal regulations after years of favoring the hands-off doctrine of the Bush administration. A multimedia section includes a graphic titled "Push for Regulations from Unlikely Sources" and a sponsored article titled "once in Theatres Now".



# Agenda

- Security Shifts...
- ... Regulators Awaken ...
- ... Can I Get a Pay Raise? (e.g., PCI's a lotta work!)
- IBM Customers' Stories
- Questions and Answers

# Skipping compliance: *The short path from breach to extinction*



## Lawsuit filed over CardSystems data breach

Class action suit says company was negligent in maintaining consumer credit data

By Robert McMillan, IDG News Service  
June 28, 2005

SAN FRANCISCO - A class action lawsuit has been filed in California over the CardSystems Solutions security breach, which reportedly exposed as many as 40 million credit-card numbers to fraud.

The New York Times

## 68,000 MasterCard Accounts Are at High Risk in Breach

By ERIC DASH (NYT) 489 words  
Late Edition - Final, Section 1, Page 22, Column 1

The New York Times

## CardSystems Sets Plan to Comply With Security Standards

By ERIC DASH (NYT) 537 words  
Late Edition - Final, Section C, Page 4, Column 3



## Visa cuts CardSystems over security breach

By John Leyden (john.leyden@theregister.co.uk)  
Published Tuesday 19th July 2005 16:33 GMT

Visa USA has dumped a card processing firm blamed for a security breach affecting anything up to 40m credit card numbers from MasterCard, Visa and card issuers.



## CardSystems says it faces 'imminent extinction'

Published: July 22, 2005, 5:44 AM PDT

U.S. payment-processing company CardSystems Solutions said Thursday it faces "imminent extinction" after revealing last month a massive credit card data security breach.

# PCI DSS Requirements “The Digital Dozen”

## Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

## Protect Cardholder Data

3. Protect stored cardholder data
4. Encrypt transmission of cardholder data sent across open, public networks

## Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications

## Implement Strong Access Control Measures

7. Restrict access to cardholder data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data

## Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes

## Maintain an Information Security Policy

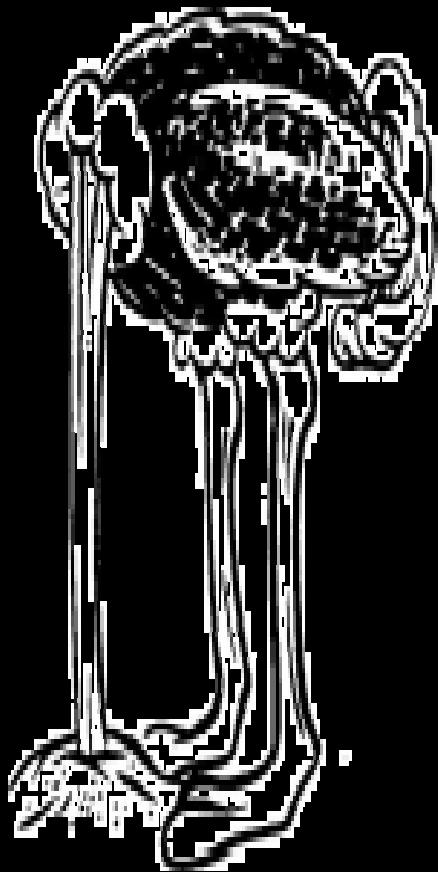
12. Maintain a policy that addresses information security – Connected Entities and Contracts

## Incentives (Visa Compliance Acceleration Program)

- In January 2007, Visa USA announced a \$20M incentive fund payable to acquiring financial institutions.
- Acquiring banks of Level 1 and 2 merchants who have validated full compliance with the PCI Data Security Standard by March 31, 2007 will be eligible to receive a one-time payment for each qualifying merchant.
  - Note: This incentive only applies to merchants that have not been previously been compromised.



# The Cost of Non-Compliance





# Consequences for lack of compliance

## ■ Financial Risk

- Merchant banks may pass on substantial fines
- Up to \$500,000 per incident from Visa alone
- Civil liability and cost of providing ID theft protection



## ■ Compliance Risk

- Exposure to Level 1 validation requirements

## ■ Operational Risk

- Visa-imposed operational restrictions
- Potential loss of card processing privileges



## Recent Gartner Findings on PCI Compliance

- Cost comparison
  - Data Breaches ~ \$300/user
  - Data Protection ~ \$16/user
  - It's cheaper to do the right thing!
  
- Encryption is key but if you can't encrypt data at rest, consider the following compensatory controls:
  - Narrow segmentation of cardholder data surrounded by strong access controls
    - Identity and Access Management
  - Database activity monitoring
    - Security Information and Event Management
  - Outsourcing
    - Managed Security Services

Source: "Data Breaches and PCI Compliance — Which Costs More?" Gartner Compliance & Risk Management Summit, Avivah Litan, May 2007



## Common Problem Areas

- Lack of encryption for emails and messaging
- Lack of encryption for data at rest
- Lack of knowledge where all the data is at rest
- Lack of segregation of duties
- Lack of adequate access controls (generic, default and shared IDs)
- Lack of network segregation
- Back end operation networks often break the isolation of PCI networks
- Too many firewall rules with no business justification
- Insufficient documented policies and procedures
- Un-patched systems
- Storing sensitive magnetic stripe data

# Where Organizations Fail Audits

PCI Requirement	% Failure
<b>Requirement 3: Protect stored data.</b>	79%
<b>Requirement 11: Regularly test security systems and processes.</b>	74%
<b>Requirement 8: Assign a unique ID to each person with computer access.</b>	71%
<b>Requirement 10: Track and monitor all access to network resources and cardholder data.</b>	71%
<b>Requirement 1: Install and maintain a firewall configuration to protect data.</b>	66%
<b>Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.</b>	62%
<b>Requirement 12: Maintain a policy that addresses information security.</b>	60%
<b>Requirement 9: Restrict physical access to cardholder data.</b>	59%
<b>Requirement 6: Develop and maintain secure systems and applications.</b>	56%
<b>Requirement 4: Encrypt transmission of cardholder data and sensitive information across public networks.</b>	45%

Source: VeriSign sample of 112 assessments, where 30 ultimately passed and 82 did not

## Card Systems Solutions

- May 2005
- 40 Million Account Numbers Accessed
  - Card Systems was a third-party processor of payment data
  - Its primary customers were Card Associations and FIs



- Routinely handled account and transaction data
- The network in the Tuscon, AZ office was hacked
- FBI notified
- Consumers subsequently notified according to state data breach notification laws



## What Happened ??

- Common vulnerability exploited
  - A hacker accessed a central database
    - Installed a script that captured transaction data
  - According to MasterCard:
    - MC fraud monitoring systems detected a large amount of fraudulent activity for a number of card holders
    - Working with a member bank, began forensic investigation
    - The trail led directly to Card Systems
  - According to Card Systems:
    - CS IDS system detected an intruder on May 22
    - On May 23, CS contacted the FBI
    - With the approval of law enforcement, VISA, MasterCard, and other organizations were subsequently notified
  - Data Exposed
    - 20 million VISA-branded cards
    - 13.9 million MasterCard-branded cards
    - American Express, Discover, JBC, etc. affected
    - Major financial institutions issuing branded cards impacted



## What does PCI say?

- In General: **Build and Maintain a Secure Network, Protect Cardholder Data and ...**
- Requirement 3: Protect stored cardholder data
  - ... methods for minimizing risk include not **storing cardholder data unless absolutely necessary** ...
  - 3.1 Keep cardholder **data storage to a minimum**. Develop a data retention and disposal policy. Limit storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy.
  - 3.2 Do not store sensitive authentication data subsequent to authorization (even if encrypted).
  - 3.2.1 Do not store the full contents of any track from the magnetic stripe (that is on the back of a card, in a chip or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic stripe data. In the normal course of business, the following data elements from the magnetic stripe may need to be retained: the accountholder's name, primary account number (PAN), expiration date, and service code. To minimize risk, store only those data elements needed for business. NEVER store the card verification code or value or PIN verification value data elements.
- Requirement 6: Develop and maintain secure systems and applications
  - Unscrupulous individuals use security **vulnerabilities** to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches. All systems must have the most recently released, appropriate software patches to protect against exploitation by employees, external hackers, and viruses.
  - 6.2 Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet). Update standards to address new vulnerability issues.
  - 6.3 Develop software applications based on industry best practices and incorporate information security throughout the software development life cycle.



## What Did Gartner Say About Common Problems??

- Lack of encryption for emails and messaging
- **Lack of encryption for data at rest**
- **Lack of knowledge where all the data is at rest**
- Lack of segregation of duties
- Lack of adequate access controls (generic, default and shared IDs)
- Lack of network segregation
- **Back end operation networks often break the isolation of PCI networks**
- Too many firewall rules with no business justification
- Insufficient documented policies and procedures
- **Un-patched systems**
- Storing sensitive magnetic stripe data





## One other example: Chipotle Mexican Grill

- August 2004
  - Theft of patrons' credit card numbers added up to 2000+ incidents of fraud
  - Chipotle was liable for \$1.4 million
  - Discovered that software was retaining Track 2 data, and Internet gateways were not secured
  - To correct situation
    - Fixed software problems
    - Set aside \$4 million to cover liabilities
      - Fraudulent charges
      - Card replacement
      - Monitoring expenses
      - Card association fines



## What Did Gartner Say About Common Problems??

- **Lack of encryption for emails and messaging**
- Lack of encryption for data at rest
- Lack of knowledge where all the data is at rest
- Lack of segregation of duties
- **Lack of adequate access controls (generic, default and shared IDs)**
- Lack of network segregation
- Back end operation networks often break the isolation of PCI networks
- Too many firewall rules with no business justification
- Insufficient documented policies and procedures
- **Un-patched systems**
- **Storing sensitive magnetic stripe data**



# Agenda

- Security Shifts...
- ... Regulators Awaken ...
- ... Can I Get a Pay Raise? (e.g., PCI's a lotta work!)
- IBM Customers' Stories
- Questions and Answers

## Philips International BV

### *Securing company assets and strengthening compliance*

#### Challenge:

- Ensure total control of global funds network
- Comply with regulations such as Sarbanes Oxley and Tabaksblat, the corporate governance code for Netherlands

#### Solution:

- Implemented IBM Tivoli Compliance Insight Manager to protect company assets and comply with regulations

#### Benefits:

- Total control of all data activities and traffic
- Constant control and evidence of commercial payment processes
- Established complete protection against manipulation of information



*“Thanks to IBM Tivoli Compliance Insight Manager, we can now validate all the treasury data published in our annual report with greater confidence than ever before.”*

**Gabriel van de Luitgaarden**  
*Senior Vice President*



# Bancaja

## Client requirements

- Minimize the risk of customer dissatisfaction and regulatory fines by managing the impact of unplanned system outages
- Reduce IT costs and improve security across the bank's two data centers

## Solution

- Engage IBM Global Technology Services to provide business resilience services and two IBM eServer™ zSeries® servers in an IBM Geographically Dispersed Parallel Sysplex™ (GDPS) configuration
- Provide automated transaction monitoring with IBM Tivoli® NetView® software, and automated failover support with IBM TotalStorage® Enterprise Storage Server hardware

## Benefits

- Reduced from several days to an hour and a half the time required to initiate backup support due to CPU problems
- Established automatic system recovery in the event of a disk failure
- Reduced the risk of lost revenue and regulations costs, and eliminated risk of Basel II penalties



# Pay by Touch

*Building a retail payment system that provides total security*

## Value Drivers

Pay By Touch had put together two existing capabilities—biometric recognition and electronic financial transactions—to create a groundbreaking new retail payment service. The company needed a highly scalable, secure and easy-to-integrate platform to support its rapidly growing operations.

## Solution

A service-oriented architecture (SOA) approach that provides the ability to integrate IT assets and capabilities while remaining rapidly scalable as well as secure. The underlying platform is built on WebSphere and Tivoli software for process choreography, integration and high availability.

## Value Realization

- 25 percent reduction cost of integrating acquired companies
- 30 percent increase in the productivity of IT staff
- 15 percent reduction in total cost of ownership
- Provides secure, positive identification of shoppers
- Eliminates the possibility of credit/debit card fraud due to theft



*"For customers, it [Pay by Touch] offers ease and security that just doesn't exist elsewhere—they don't have to carry cash or even a card that could be stolen. Literally, they can walk into a store empty-handed and make a purchase."*

*— Ryan Ross  
Vice President, Business  
Development  
Pay By Touch*

## Swiss Reinsurance Company

*Implements comprehensive IT governance framework*

### Challenge:

- Link IT processes and data to business strategies
- Optimize IT processes, including planning, implementing and delivering IT systems
- Optimize IT resources to capitalize on business opportunities and gain competitive advantage

### Solution:

- Developed IT governance framework to establish governance processes and steps to monitor regulatory compliance
- Created a process maturity model for IT governance processes

### Benefits:

- Better able to manage risks
- Increase in investor and shareholder confidence
- Corporate wide standardization of all IT-related risks

Swiss Re



***SwissRe increases stakeholder confidence and ensures compliance by reducing IT-related risks.***



# Consumer Bank

## Challenge

- Organization had grown through acquisitions, with no centralized governance over IT assets
- Failed external regulatory audit
- Reasons for audit failure:
  - Inadequate security and business controls over software lifecycle
  - Poor governance over software development environment

## Solution

- Bank-wide configuration and change management for IT systems
- Implemented Rational ClearCase Multisite, Rational ClearQuest, Tivoli Configuration Manager

## Benefits

- Passed audit
- Compliance infrastructure well positioned the bank for Sarbanes-Oxley compliance
- Enhanced software team productivity
- Improved governance over software assets





*Thank You*