IBM Software Group

Tivoli. software

IBM Tivoli z Security Solutions

"Business Impact of a Security Breach"

Joyce F. Ruff, Product Management
jfruff@us.ibm.com, 512-286-2317

Last updated May 15, 2008

IBM Tivoli Security Solutions

- IBM delivers innovative security solutions to help you meet the challenges of staying a step ahead of fast-evolving threats and compliance requirements though smart, strategic solutions that help you to secure your business:
  - Real-time, risk-based insight into the state of your IT security defenses and compliance posture
  - Adaptive solutions that can be seamlessly integrated within the enterprise to meet your evolving needs
  - Confidence that your organization's data, applications and infrastructure are protected and used only by the right people, at the right time, and in the right way

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.**

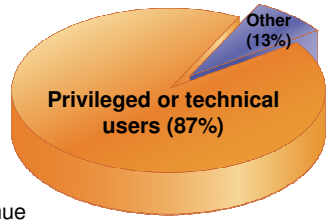
64% of CIOs feel that the most significant challenges facing IT organizations are security, compliance and data protection

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

IBM Service Management Market Needs Study, March 2006

Who Causes Security Breach Incidents?

- Malicious or unintentional insiders
  - 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%)
  - Either way, too costly to ignore:
    - Internal attacks cost 6% of gross annual revenue
    - Costing $400 billion in the US alone



- Sophisticated outsiders
  - Efforts to penetrate corporate defenses through their high-level employees' information are on the rise
  - Phishing, Whaling, etc.

Sources: Forrester research, IdM Trends 2006; USSS/CERT Insider Threat Survey 2005; CSI/FBI Survey, 2005; National Fraud Survey; CERT, various documents.

Security Breach Risks

The problem:

- 3 of the Top 10 Threats to Enterprise Security are insider related:
  - Employee error
  - Data stolen by partner/employee
  - Insider Sabotage
- Insider driven fraud costs US enterprises over $600 Billion annually

How to handle:

- Get better visibility into activity of privileged user accounts and access
- Improve identity controls
- Automate monitoring and audit to more easily flag threats

THE WALL STREET JOURNAL.

PAGE ONE

French Bank Rocked by Rogue Trader

Société Générale Blames $7.2 Billion in Losses On a Quiet 31-Year-Old

By DAVID GAUTHIER-VILLARS, CARRICK MOLLENKAMP and ALISTAIR MACDONALD

PARIS -- The rogues' gallery of banking has a new candidate for membership: 31-year-old trader Jérôme Kerviel.

In one of the banking world's most unsettling recent disclosures, France's Société Générale SA said Mr. Kerviel had cost the bank €4.9 billion, equal to $7.2 billion, by making huge unauthorized trades that he hid for months by hacking into computers. The combined trading positions he built up over recent months, say people close to the situation, totaled some €50 billion, or $73 billion.

The loss -- dwarfing the $1.3 billion Nick Leeson cost British bank Barings in 1995 -- has forced Société Générale to seek a capital infusion. It is expected to try to raise €5.5 billion, chiefly from its existing shareholders.

Results of a Security Breach

InformationWeek
BUSINESS INNOVATION POWERED BY TECHNOLOGY

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 …

InfoWorld HOME NEWS TEST CENTER OPINIONS PRODUCT

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 may have exposed as many as 40 million credit-card numbers to fraud.

InformationWeek
BUSINESS INNOVATION POWERED BY TECHNOLOGY

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.

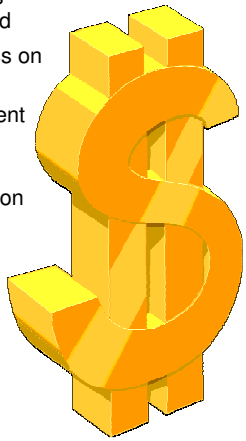
As a result, TJX is a company under siege. The company recorded a fourth-quarter charge of about $5 million to cover the costs of containing and investigating the breach, as well as improving the security of its IT systems, communicating with customers, and paying legal fee. The U.S. Federal Trade Commission 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.

Why Should You Care?

- Your auditors care
  - Industry and government regulations (e.g. PCI, SOX, etc)
  - Fines and penalties for non-compliance
- Your CEO cares
  - Brand and corporate image and integrity
  - Customer retainment / attrition
- Business risks:
  - Intellectual Property
  - Legal and Regulatory Exposures
  - Your Customer Information
  - Customer Confidence
  - Cost of Remediation
  - Business Disruption
  - Your Job

Consequences of a PCI-Related Security Breach

- Financial Risk
  - Average cost of data-loss incident = $197 per record
  - 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

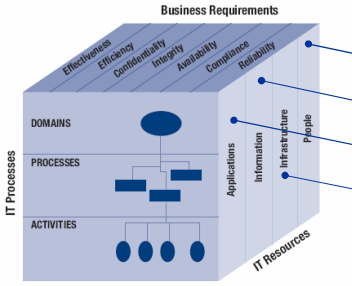


- Compliance Risk
  - Exposure to Level 1 validation requirements
- Operational Risk
  - Visa-imposed operational restrictions
  - Potential loss of card processing privileges

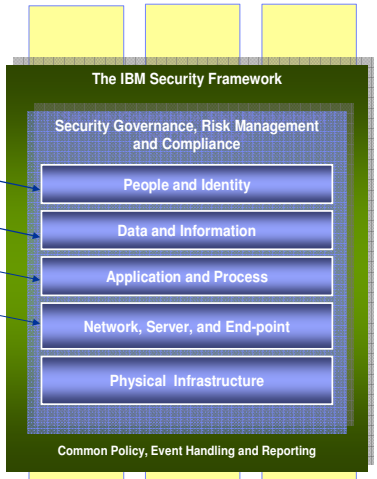
Security Landscape

Control Objectives for Information and related Technology (COBIT)

Figure 15—The COBIT Cube



Source: IT Governance Institute, Control Objectives for Information and related Technology (COBIT) 4.0.

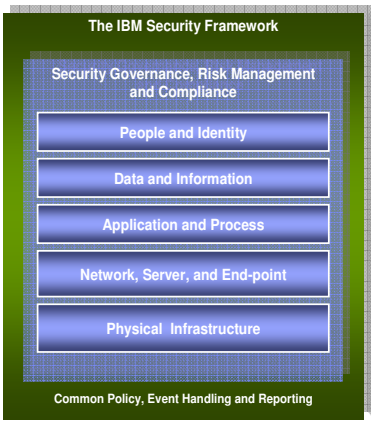


Delivered by… Professional Services | Managed Services | Hardware & Software

The IBM Security Framework

Enabling collaboration while mitigating risk

- IBM delivers:
  - Timely **visibility** into business continuity risks and compliance posture
  - More effective **control** over utilization of sensitive business assets
  - Efficient **automation** of the identification and remediation of vulnerabilities and the addressing of compliance mandates



- **SECURITY COMPLIANCE**
  - Demonstrable policy enforcement aligned to regulations, standards, laws, agreements (PCI, FISMA, etc..)
- **IDENTITY & ACCESS**
  - Enable secure collaboration with internal and external users with controlled and secure access to information, applications and assets
- **DATA SECURITY**
  - Protect and secure your data and information assets
- **APPLICATION SECURITY**
  - Continuously manage, monitor and audit application security
- **INFRASTRUCTURE SECURITY**
  - Comprehensive threat and vulnerability management across networks, servers and end-points

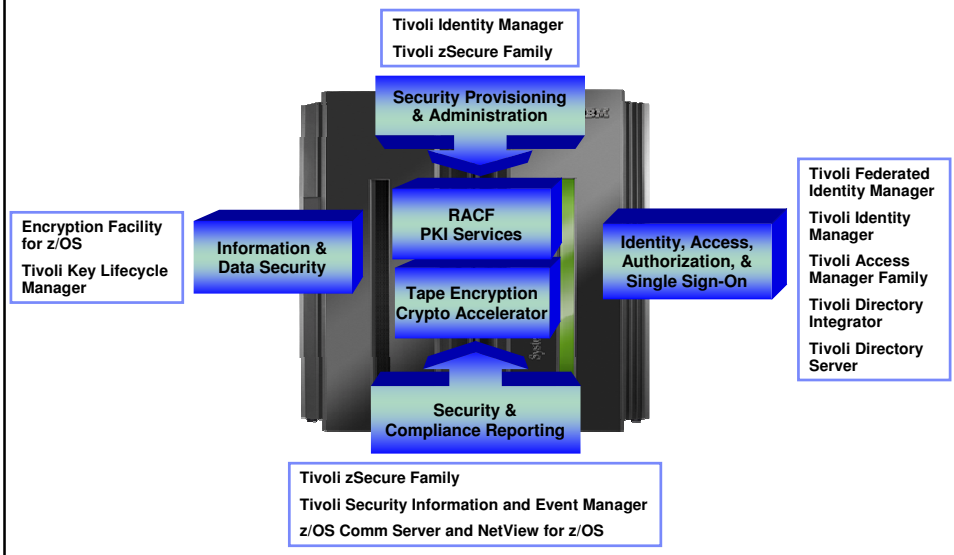
System z as the security hub for the enterprise

Leverage the mainframe security policies and processes that have been developed over many years in your enterprise

- Security-rich holistic design to help protect system from malware, viruses, and insider threats
- Granular access controls integrated across the platform
- Network security features to help address outside threats
- Encryption solutions to help secure data from theft or compromise
- Tivoli tools allowing you to address administration and compliance needs with more confidence

The industry's most securable platform!

Tivoli Enterprise Security Hub Overview



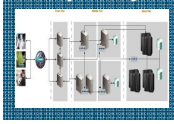
IBM Security Management

From reactive security to risk aware enterprise

CIO's Top Priorities Are to Deliver

Business Agility/Innovation While Retaining a Resilient Business

Complexity

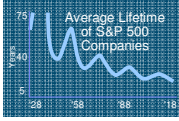


Increased complexity makes change management much harder

Compliance

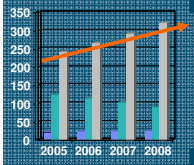
Changing regulatory environment requires security, privacy and ongoing audit capabilities

Change



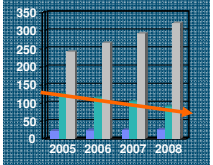
Increased competitive pressure while IT has an increasing role in every business process

Rising Cost of Operations



The cost of operations continues to increase at 10% CAGR … twice the rate of the IT budget

Inability to Innovate

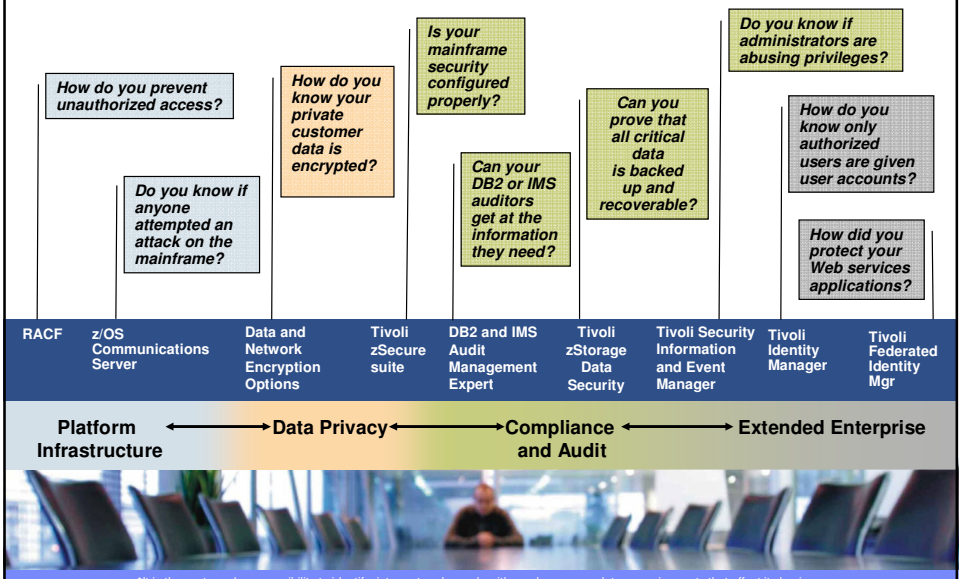


Increased focus on development project spend due to higher % of costs going to keeping the lights on … creates a dual focus of doing the right thing and doing things well

Your Conflict: Regulation versus Reality

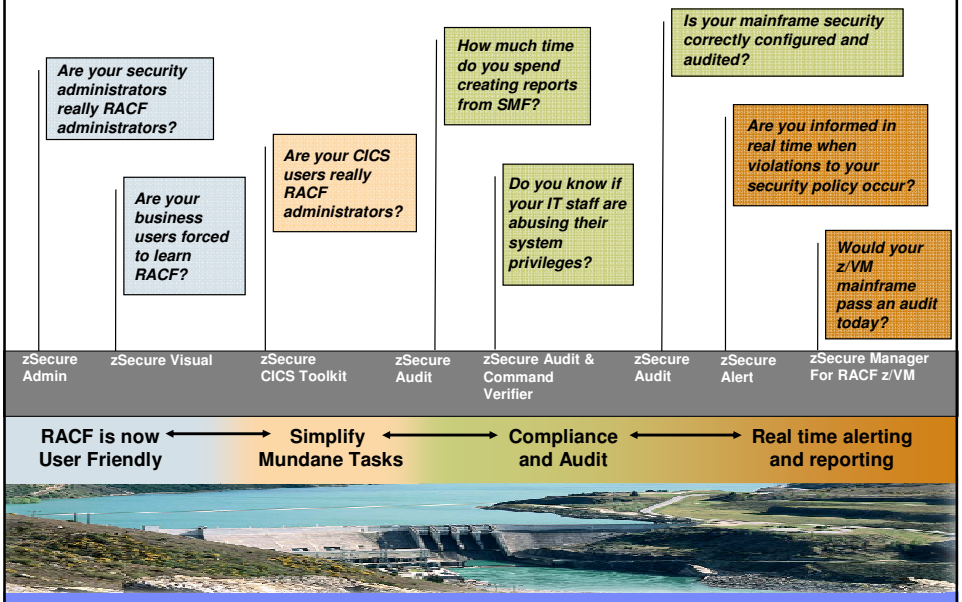
Regulation	Reality
▪ Change management – Clearly defined process with approval and reporting – Ability to identify changes ▪ Security management – Separation of duties – Identification of exposures and mis-configurations – Clear audit trail and accountability ▪ Data security – Data confidentiality and integrity – Prevent improper access to financial, medical or personal data – Monitor access to data by technician, administrator, outsiders	▪ Separation of duty impractical with small teams ▪ Highly authorized ids necessary for final go-to technician ▪ Mainframe installations often rely on "system special" and "uid(0)" ▪ Red-tape bypassed for high-impact problem resolution ▪ Manual monitoring impractical due to volume of data ▪ Human mistakes cause service outages ▪ Cleanup projects are long running and expensive

IBM Solutions Help to Address Potential Audit Concerns



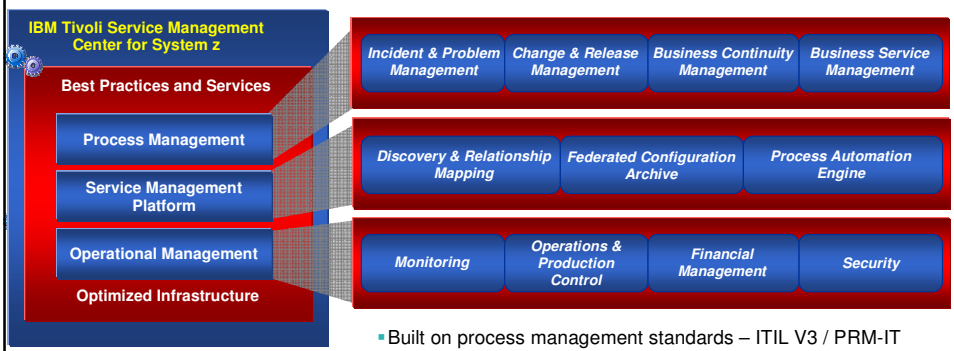
*It is the customer's responsibility to identify, interpret and comply with any laws or regulatory requirements that affect its business. IBM does not represent that its products or services will ensure that the customer is in compliance with the law.

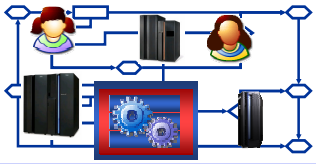
Tivoli zSecure suite addresses today's challenges



IBM Tivoli Service Management Center for System z

Enabling clients to strategically use their System z as an integrated, enterprise-wide, hub for the efficient management of business and IT services



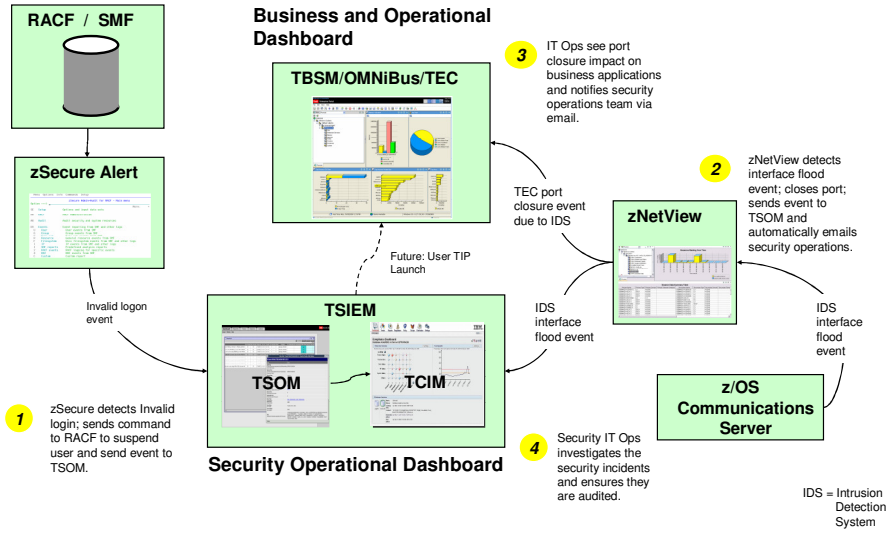


- Built on process management standards – ITIL V3 / PRM-IT
  - Delivers maximum value and flexibility
- Built on SOA foundation
  - Better integration with IBM and non-IBM applications
  - Seamless version to version upgrades of customizations
- ISV product integration support
  - Operational, Service and Process products

End-to-End Solution – Security Management

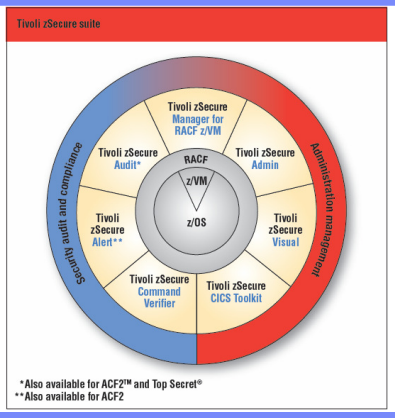
- Business Challenges
  - Accountable for validating and demonstrating audit and compliance capabilities without tools
- IBM Tivoli Service Management Center for System z Solution
  - Comprehensive audit and compliance management
  - Identity and access management
  - Automatic detection, collection, analysis and alerting of security-related events and threats from RACF, applications, data and systems
- Business Benefits
  - Improved security administration and audit compliance
  - Improved overall IT efficiency

Security Management Best Practice Details



IBM Tivoli zSecure Suite

The Tivoli zSecure suite adds a user-friendly layer onto the mainframe that enables superior administration coupled with audit, alert and monitoring capabilities for Resource Access Control Facility (RACF)



Key Features

- The zSecure suite improves the efficiency of mainframe administration and enhances the ability for the mainframe to be the hub of enterprise security.
- Administration and provisioning:
  - zSecure Admin enhances user management
  - zSecure Visual offers a Microsoft® Windows® GUI
  - zSecure CICS Toolkit for simplified RACF security management
  - zSecure Manager for RACF z/VM provides combined audit & admin for VM environment
- Audit, monitoring and compliance:
  - zSecure Audit provides event detection, analysis & reporting and system integrity audit & analysis
  - zSecure Alert provides intrusion detection and alerting
  - zSecure Command Verifier offers automated security monitoring

Benefits Summary

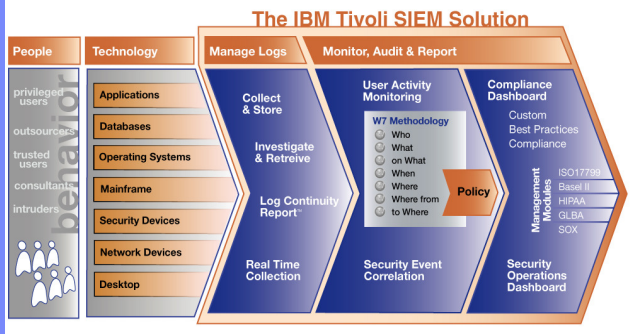
- Administration and provisioning:
  - Reduce administration time, effort and cost
  - Reduce training time needed for new administrators
- Audit, monitoring and compliance:
  - Helps to pass audits more easily
  - Can improve security posture
  - Save time and costs through improved security and incident handling
  - Can increase operational effectiveness

Security Compliance

Aligning IT security to business priorities

Goals

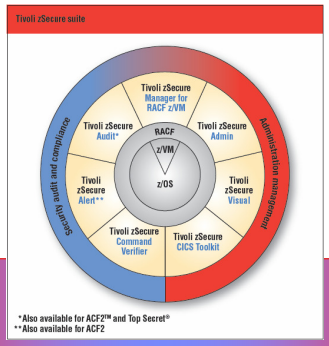
- Proactive real-time monitoring of network & systems for compliance with security policies
- Monitor platforms from mainframe to distributed & devices
- Historical reporting to demonstrate compliance
- Clearly define & communicate potential security incidents so they can be handled correctly
- Ensure that preventive, detective and corrective measures are in place to protect information systems & technology from malware



IBM solutions
- Tivoli Security Information & Event Manager
- Tivoli Compliance Insight Manager
- Tivoli Security Operations Manager
- Tivoli Security Compliance Manager

A Cornerstone for Tivoli's Mainframe Security Strategy

IBM Tivoli zSecure Suite



Enterprise Security Monitoring and Audit Reporting

Enterprise Identity and Access Management

Tivoli Compliance Insight Manager (TCIM)	Tivoli Security Operations Manager (TSOM)	Tivoli Identity Manager (TIM) for z/OS	Tivoli Federated Identity Manager (TFIM) for z/OS	Tivoli Directory Server (TDS) for z/OS	Tivoli Directory Integrator (TDI) for z/OS

* Also available for ACF2 and Top Secret
** Also available for ACF2

Aviva – Norwich Union

Improving mainframe user management in a complex environment

Challenge

- Norwich Union needed to facilitate compliance with identity and access management initiatives by implementing preventative, detective and corrective controls within its IT environment
- With several RACF tools to maintain various RACF databases – most homegrown, Norwich Union needed a strategic, robust solution to keep up with high demand for security and audit reports, and with often-complex security requests

Solution

- IBM Tivoli zSecure Admin, which enables efficient RACF administration with fewer resources
- IBM Tivoli zSecure Audit for RACF and ACF2, which automatically analyses and reports on security events and exposures
- IBM Tivoli zSecure Alert for RACF to enable quick response to RACF and z/OS events through real-time alerting

Benefits

- Simplifies mainframe security administration tasks, improving efficiency and reducing errors
- Enables quick, proactive response to security events
- Supports robust audit and compliance reporting
- Helps maintain high levels of security automation for system security management
- Provides a consistent and uniform approach to security management across the System z environment

"IBM Tivoli zSecure software gives us a simple, powerful way to comply with identity and access management initiatives, and to assure auditors that preventative, detective and corrective controls are installed."

Phil Secker, Security Support Manager, Norwich Union

NORWICH UNION
an AVIVA company

Profile: *Norwich Union is part of the Aviva group, a leading provider of life and pension products in Europe and one of the largest insurance groups in the world.*

ING Group

Challenge

As the number of industry regulations increased and the complexity of its operating environment grew, ING needed to reduce the time and cost of providing its 113,000 employees with secure access to data and services.

Solution

- IBM Tivoli Identity Manager, IBM Tivoli Directory Integrator, IBM Tivoli Access Manager for e-business, IBM WebSphere Application Server, IBM eServer pSeries
- IBM Global Services

Benefits

- Projected savings of total €15 million (US $20 million) a year through process improvements.
- Projected 50% reduction in number of staff needed to manage identities.
- Decrease in turn-on time for new users from one week to less than 24 hours.
- Anticipated 25% savings in help-desk costs through self-service of password resets.
- Reduction in time and cost of regulatory compliance.

ING

"With IBM Tivoli identity management technology, we can transform a convoluted process into a model of efficiency. Once fully implemented, this will save us a total of €15 million a year and help us reduce the number of staff needed to manage employee identities by 50 percent."

— *Dion Kotteman*
Program Manager
Global Information Risk Management, ING

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

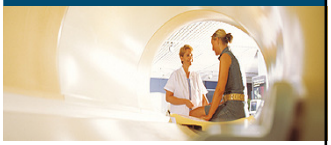
Benefits

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

PHILIPS
sense and simplicity

"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



Pay by Touch

Building a retail payment system that provides total security

Challenge

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.

Benefits

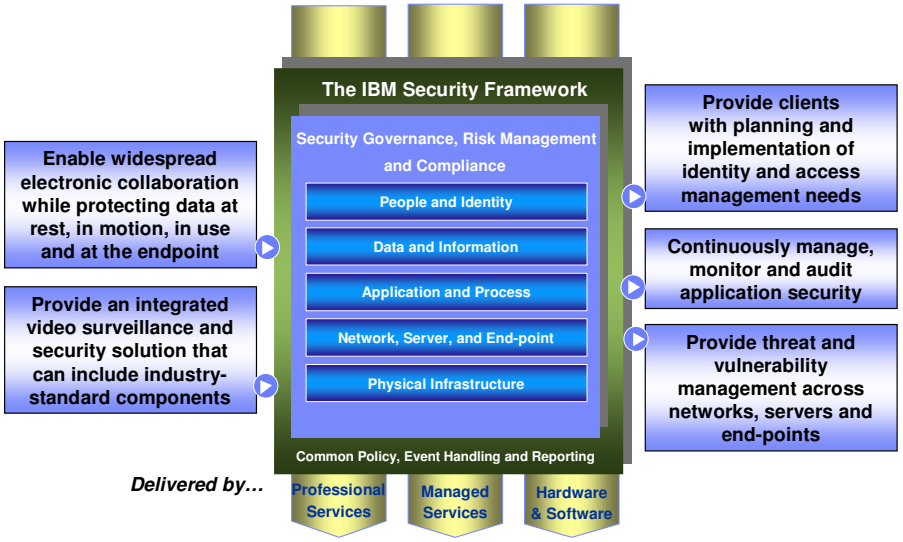
- 25 percent reduction cost of integrating acquired companies
- 30 percent increase in the productivity of IT staff
- 15 percent reduction in total cost of ownership
- Provides secure, positive identification of shoppers
- Eliminates the possibility of credit/debit card fraud due to theft

PAY BY TOUCH™

"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

While many security companies can help you with the crisis of the day, IBM offers security solutions that address the full range of security challenges *from core to perimeter…*

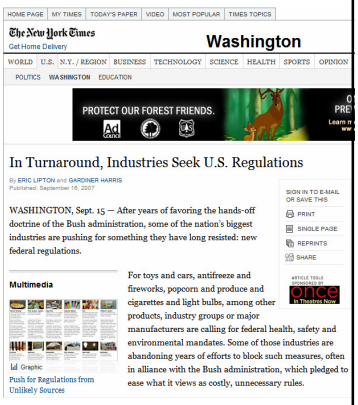


CIOs with effective mainframe security…

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*



In Closing…

- IBM is uniquely positioned to address security and compliance needs
  - ✓on all of your computing systems
  - ✓across security disciplines
  - ✓using a combination of offerings available today
  - ✓with active research and innovation in security
  - ✓across the enterprise

- Tivoli's end-to-end System z security management solution includes:
  - ✓Tivoli zSecure suite
  - ✓Tivoli Security Information and Event Manager
  - ✓Tivoli Identity Manager
  - ✓Tivoli Federated Identity Manager
  - ✓And more!

Thank You!

Trademarks and disclaimers

Learn more about zSecure

- Upcoming webcast:
  - System z security – Educational webinar for state and local government and education
    - Register at: http://www.ibm.com/software/systemz/telecon/31jul
- Links to recent webcasts and teleconferences available for replay
  - The System z Security Hub: RACF Administration – zSecure suite
    - http://www-306.ibm.com/software/os/systemz/telecon/14feb/
  - Enforce Policy Compliance on RACF – zSecure Command Verifier
    - http://www-306.ibm.com/software/os/systemz/telecon/19jun/index.html
  - Optimizing RACF Security for z/VM – zSecure Manager for RACF z/VM
    - http://www-306.ibm.com/software/sw-events/webcast/X659588E45662G80.html
- SHARE, Aug 10-15, 2008
  - Demos at z security pedestal at Expo booth
  - Lunch and Learn session on Tuesday, 8/12 @ 12:15pm
  - Education sessions and hands-on labs for zSecure

Resource Center

zSecure online customer forum
- http://www-128.ibm.com/developerworks/forums/forum.jspa?forumID=1255

CCR2 Newsletter Article
- http://www.ibm.com/software/tivoli/features/ccr2/ccr2-2007-09/innovative-mainframe.html

zSecure data sheets, solution sheets, and white papers
- http://www-306.ibm.com/software/tivoli/products/zsecure/

zSecure Manuals
- http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.zsecure.doc/welcome.htm
- Some manuals are restricted to licensed customers

Redbooks & Redpapers
- http://www.redbooks.ibm.com/

IBM Tivoli Security and System z Redpaper
- http://www.redbooks.ibm.com/redpieces/abstracts/redp4355.html?Open