



**IBM Software Universe**  
Smarter Businesses, Smarter Industries.

8th March 2011, Pan Pacific, Dhaka.



# **Security, Risk and Compliance management for the Financial Market**

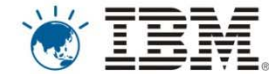
**Pawan Chopra**

*Business Manager : Software Security*

*IBM India*



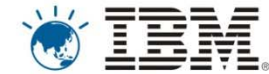
# A Smarter BFSI focus on three key imperatives....



- IBM BFSI Industry Solutions - Enabling speed, flexibility & choice in solution deployment
- Banking Performance Management
- **Managing Security, Risk & Compliance in BFSI**
- Securing Enterprise Data for Banks
- Managing Quality & Security of Banking Applications
- Unified Business Process Management for Collaborative Process Improvement
- Payment Systems: Evolution and Framework
- Better Customer Service Through Exceptional Web Experiences

Smarter Businesses, Smarter Industries.

# Paradigm change in Banking in Last 10 Years



Hobby Hackers

External Threat

Security a technology  
issue

Simpler Infrastructure

Perimeter Security



Professional Hacking

Internal Threats

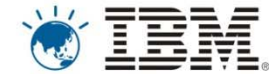
Security a BUSINESS issue

Complex , heterogeneous

Not plugability , compliance,  
operational efficiency the bigger

Smarter Businesses, Smarter Industries.

# Welcome to the Smart planet... and a Smarter infrastructure



**One Click Banking: Core Banking**

**Billions of mobile devices accessing the Web: Net Banking, Phone Banking**

**Access to streams of information in the Real Time**

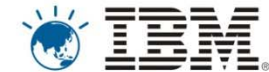


**New possibilities.**  
**New complexities.**  
**New risks.**

**Integrated Heterogeneous Infrastructure**

Smarter Businesses, Smarter Industries.

# On Contrary: State Of Security In Enterprise



- **Incomplete**

- Multiple point solutions from many vendors
- Disparate technologies that don't work together

- **Complex**


- Repeated point-to-point integrations
- Mostly manual operations

- **'Non-compliant'**

- Difficult to enforce consistent set of policies
- Difficult to measure compliance with those policies



**Loss of customer data at BNY Mellon much bigger than first thought.** Bank confirms tape with info on 12 million customers of its shareholder service unit is unaccounted for



**Societe Generale loses \$7.2 billion in trading fraud.** Lack of privileged password management and insufficient IT security controls

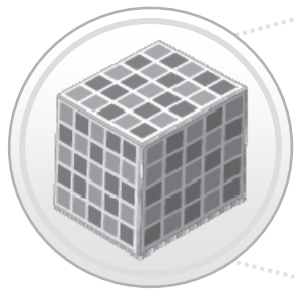
- **70% attacks originate inside the firewall**
- **90% attacks perpetrated by employees with privileged access**
- Security breaches cost \$90 to \$305 per lost record



Source: IBM Global CIO Study, The New Voice of the CIO, 10 September 2009



**Built in. Not bolted on.**  
Smarter security solutions from IBM



Information



Infrastructure



Databases



Applications

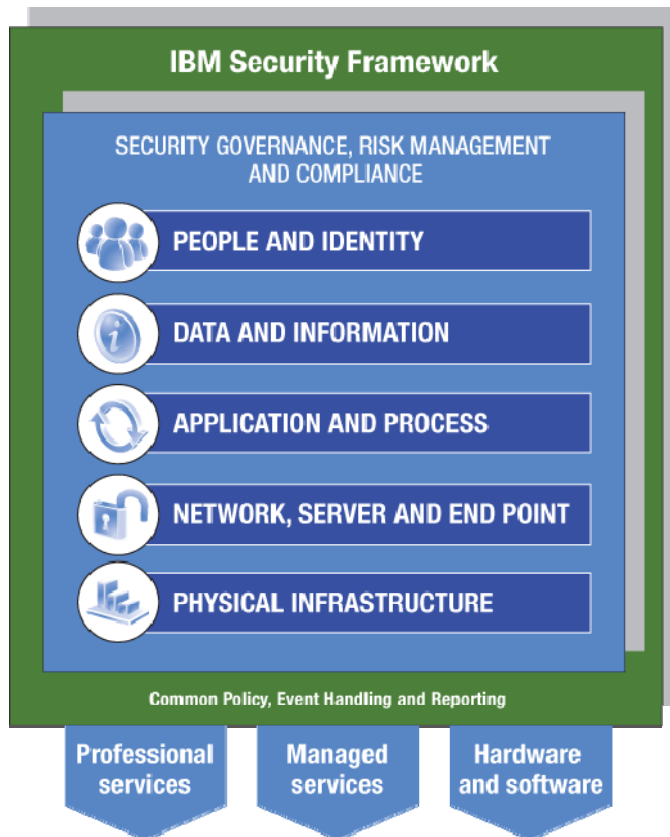
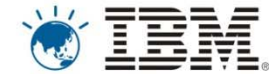


Content

Smarter Businesses, Smarter Industries.

© 2011 IBM Corporation. All rights reserved. IBM, the IBM logo, and "Smarter Business" are trademarks of International Business Machines Corporation. "Smarter Industries" is a trademark of International Business Machines Corporation.

# IBM delivers a new approach to Security



## Designed to....

- Enable innovation through secured infrastructure and platforms
- Reduce number and complexity of required security controls
- Reduce redundant security expenses
- Improve organizational and operational agility and resiliency
- Deliver needed visibility, control and automation

- ✓ **Only security vendor** in the market with ***end-to-end coverage of the security foundation***
- ✓ **15,000** researchers, developers and SMEs on security initiatives
- ✓ **3,000+** security & risk management patents
- ✓ **200+** security customer references and **50+** published case studies
- ✓ **40+** years of proven success securing the mainframe environment
- ✓ **\$1.5 Billion** security spend in 2008

Smarter Businesses, Smarter Industries.

# IBM's unparalleled breadth across domains



Each domain has a distinct security lifecycle. IBM uniquely secures assets across their lifecycle in all IT domains that impact business processes.



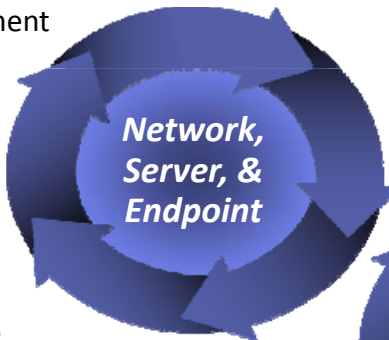
## End to End Business Process & Dependencies

- Identity & Access Mgt
- Federated Identity Mgt.
- Trusted Identity
- Identity Provisioning
- Identity Proofing



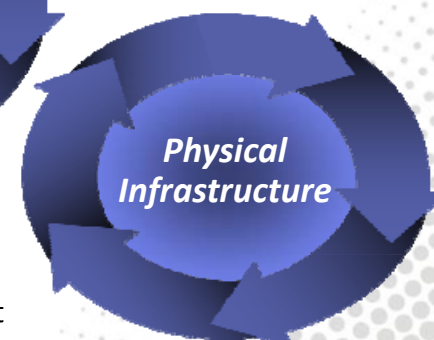
- Database/Content Mgt
- Content Monitoring
- Data Governance
- Data Encryption Solns.
- Storage Management

- Secure Development Tools
- Security Method Enforcement
- Web Application Scanning
- Application Firewall
- SOA & XML Security



- Intrusion Detection
- Vulnerability Mgt.
- Event Correlation
- Change & Config. Mgt
- Security Compliance Scan

- Digital Video Surveillance
- Smart Surveillance Solns.
- RFID solutions
- Enterprise Asset Mgt.
- Physical Security



Smarter Businesses, Smarter Industries.



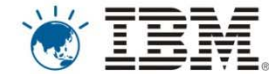
# IBM Global Security Reach



**IBM has the unmatched global and local expertise to deliver complete solutions – and manage the cost and complexity of security**

Smarter Businesses, Smarter Industries.

# Client Experiences



## Hudson's Bay Company

- Anticipates, tracks and mitigates security threats before they cause harm to data or the IT infrastructure.
- Provides professional management of network devices.

*"IBM provided us with more than just compliance. Sensitive data is secure, systems are monitored closely for performance issues, and our IT staff can focus more mission-critical activities."*



## DTCC

- Security features are designed and built into more than 225 new applications per year.
- Help improved developer productivity.
- Reduced time to market for each new service.

*"IBM helped us have the education in place and can implement security early in the application development lifecycle, so that we have less overall vulnerabilities to manage."*



## Community Medical Centers

- Reduced costs with fewer password resets and simplified administration.
- Enhanced security through HIPAA support.
- Improved staff productivity with single sign-on support.

*"IBM provided our users with one secure password to our applications and flexibility to manage how users access applications, something other vendors have not easily been able to provide."*

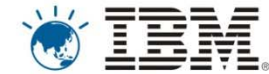


## Allianz Seguros

- Applied proven data masking techniques to protect privacy and support compliance with country regulations.

*"IBM provided the capabilities we needed to improve application development and testing processes and protect privacy,"*

# More Success Stories



**enresa**  
Empresa Nacional de Residuos Radiactivos, S. A.

**Borregaard**

**NAYANA**  
COMMUNICATION

**Washington Trust Bank**

**DukeMedicine**

**GODIVA**  
Chocolatier

**Australian Open**

**cmc**  
community medical care

**CONVERGENCE CT**

**GLOBAL DATA VAULTING**

**arek**

**HUGHES**

**AGENTRICS**

**Mercantil**

**Mn Services**

**BAYLOR**  
UNIVERSITY

**bp**

**IBM**

**Trillium**  
HEALTH CENTRE

**STADTWERKE ILMENAU GMBH**  
STROM • ERDGAS

**AVIYA**  
Clinical Research and Development

**POLICE DEPARTMENT WEST AVE**  
CONNECTICUT

**DTCC**

**WestLB**

**THE INTERNATIONAL BANK OF MIAMI, N.A.**

**P&G**

**NORTHWEST HOSPITAL & MEDICAL CENTER**

**ZOO ATLANTA**

**hbc**

**IBM Security Framework**

SECURITY GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE

- PEOPLE AND IDENTITY
- DATA AND INFORMATION
- APPLICATION AND PROCESS
- NETWORK, SERVER AND END POINT
- PHYSICAL INFRASTRUCTURE

Common Policy, Event Handling and Reporting

- Professional services
- Managed services
- Hardware and software

Smarter Businesses, Smarter Industries.



IBM Software Universe  
Smarter Businesses, Smarter Industries.

8th March 2011, Pan Pacific, Dhaka.

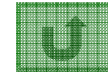


Risks Details

# RISK DETAILS

(Slide 5 includes links to the slides in this section)

# Risk: New technology introduces new security challenges



Technology innovations, like [virtualization & cloud computing models](#), used to enable the globally integrated enterprise increase infrastructure complexity

- Lack of skills, best practices, industry expertise compounds the security challenge

[Web 2.0 and SOA](#) style composite applications introduce a new level of complexity

- 54% of all vulnerabilities disclosed in 2008 were web-based<sup>1</sup>
- 80% of development costs are spent identifying and correcting defects, costing \$25 during coding phase vs. \$16,000 in post-production<sup>2</sup>
- View into application and information level entitlements is needed for regulatory compliance

Web Application Vulnerabilities

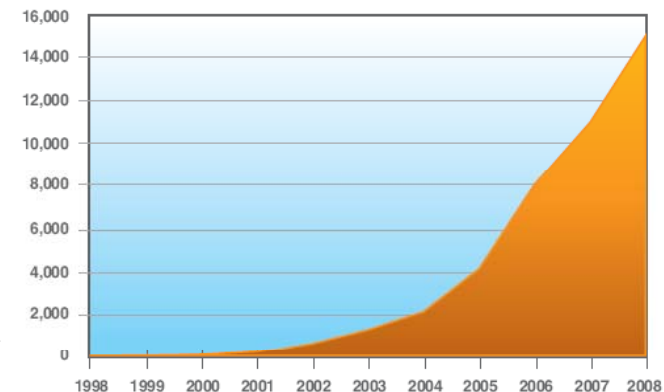


Figure 16: Cumulative Count of Web Application Vulnerabilities, 1998 – 2008

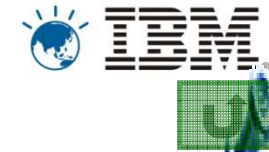
<sup>1</sup>IBM Internet Security Systems: X-Force®

2008 Trend & Risk Report, Jan 2009

<sup>2</sup>Applied Software Measurement, Caper Jones, 1996

***To what extent has introduction of new technologies, like virtualization, changed your approach to security and compliance management?***

# Risk: Volume of data is exploding



## What's driving this tremendous growth?

- Records retention for regulatory and industry compliance
- Data Backup and a Disaster Recovery environment that mirror production data for business resiliency
- Development and test requirements
- Mergers and acquisitions that lead to redundant systems, data centers, applications, etc.
- Technology innovation that makes it possible to access more data, more quickly than ever before

- ⓘ Data volumes double every 18 months<sup>1</sup>
- ⓘ 37% of data is expired or inactive<sup>2</sup>
- ⓘ Information created, captured, or replicated exceeded available storage for the 1st time in 2007<sup>3</sup>
- ⓘ 70% of the digital universe is created by individuals<sup>3</sup>...
  - ⓘ Enterprises are responsible for the security, privacy, reliability & compliance of 85%<sup>3</sup>
  - ⓘ Data breach costs \$6.6 million on average and more than \$200 per compromised record<sup>4</sup>
- ⓘ Average US legal discovery request can cost organizations from \$150K to \$250K<sup>5</sup>

How have you addressed the information explosion?

Smarter Businesses, Smarter Industries.

<sup>1</sup> "Changing Enterprise Data Profile", IDC, December 2007

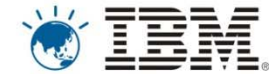
<sup>2</sup> "The Costs of Enterprise Downtime: NA Vertical Markets 2005" International Research; IBM Market Intelligence

<sup>3</sup> "The Diverse and Exploding Digital Universe, IDC, March 2008

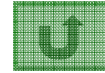
<sup>4</sup> Ponemon Institute, February 2009

<sup>5</sup> CIO Magazine, Survey 2007

# Risk: Barbarians are everywhere



Wireless devices empower individuals to more effectively participate in the global economy



- Able to send and receive information (audio and video)
- Authentication tool for secure transactions
- Security technology is many years behind the security used to protect PCs

Green initiatives lead to increased adoption of telecommuting strategies

- New breed of security threat: Those that know no geographical boundaries



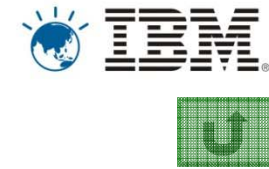
Persistent security threat

- Privileged users with limited skills, following manual process definition, with high levels of physical and logical access

**Have you considered how security can enable a 'teleworking' strategy?**

Smarter Businesses, Smarter Industries.

# **Risk:** The supply chain is only as strong as the weakest link

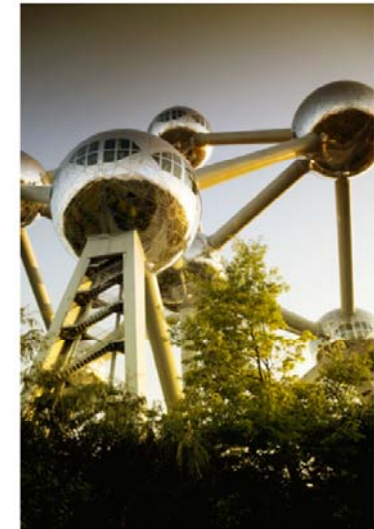


In an increasingly networked world, enterprises must shore-up their weakest supply chain partners

Need to collaborate in monitoring end-to-end security and respond to threats time

- More evenly distributed security responsibilities
- Increased transparency from start to finish
- Eased burden of customer-facing unit

Growing number of compliance requirements and industry standards, like the Payment Card Industries Data Security Standard (PCI-DSS), require partners to certain minimum requirements



**How does your organization ensure each link in the supply chain shoulders their fair share of the load for compliance and the responsibility for failure?**



# Risk: Expectation of privacy



Consumer expectation is that security should be built in to services themselves

- 50% of consumers still avoid online purchases due to fear of financial information being stolen<sup>1</sup>

Expectation drives regulation

Vendors, like automakers, are expected to take a greater share of responsibility



- **Critical to assess trade-offs consumers are willing to make against convenience or cost**
- **Risk of so much security that functionality is lost:**  
*careful not to destroy that which you are trying to protect!*

<sup>1</sup>Cyber Security Industry Alliance (CSIA) survey, May 2005

To what extent is privacy driving security spend?

Smarter Businesses, Smarter Industries.

# Risk: Compliance fatigue



Complexity and confusion keep customers from acting strategically

- Extended relationships create a tangle of potential legal liability
- Compliance requirements are inconsistent within and across geographies
- Confusion as to where to start

Pressure to simply “check the box” has resulted in creation of silos

- Silos lead to duplicative efforts and redundant spending as well as reduced visibility

The CSO struggles to become a consultant to the business

- Nearly impossible without a central, risk based view

October 17, 2007

### Apathy and Alchemy: When Good Enough Security is Good Enough

U.S. Securities and Exchange Commission

#### SEC Charges LPL Financial for Failing to Protect Customer Privacy

FOR IMMEDIATE RELEASE  
2008-10-17

Washington today took action to adopt policy information following a

Additional  
Administration

September 12, 2008 9:30 AM PDT  
Filed by Stephanie Condon

#### Former Intel worker charged in theft of secret files

The FBI has charged an engineer with stealing trade secrets from Intel, his former employer, after taking a position with rival chip maker Advanced Micro Devices. The Division of Cyber Operations

A search of Bloughman Pan's home in Worcester, Mass., on July 1 turned up more than 100 pages of sensitive Intel documents, including 13 "top secret" files with designs for future processor chips, the FBI charged. A criminal complaint against Pan, which was unsealed Tuesday, was filed by the FBI in late August in U.S. District Court in Boston.

Pan turned in his resignation to Intel in May, stating he would continue working there through June 14, according to an affidavit filed with the criminal complaint. However, he began working for AMD on June 2, while he still had access to his Intel laptop and the company's computer network. The affidavit said Pan collected the sensitive information from Intel for its competitive value to his new employer.

Pan admitted to the FBI during a July 23 interview that he obtained the files but only out of curiosity and to aid his wife, also an Intel employee, prepare for a transfer to a new Intel plant.

Intel asked the FBI and the Justice Department to intervene after learning about Pan's job at AMD from another Intel employee. The FBI said there is no evidence that AMD knew of or encouraged Pan's actions or ever received the confidential Intel files. Pan is currently employed by AMD. Intel employees who were

How much security and compliance control is good enough?

Smarter Businesses, Smarter Industries.