Ultimate Protection for your business data with IBM System z

***Mark Simmonds** – WW Product Marketing Manager System z*
IBM Information Management Division
***Ernie Mancill** – Executive IT Specialist, IBM Information Management Division*

Feb 23, 2011, Southfield

Information Management software

Agenda for this morning….

- ***7:30** Registration / Continental Breakfast*
- **8:15 Session 1 : "End to end Information Protection – the complete picture"**
- *Break (15 mins)*
- **9:30 Session 2 : "Taking back control through Security, Audit and Encryption"**
- *Break (15 mins)*
- **10:45 Session 3 : "Discovery, Privacy and Archiving as part of your information protection strategy"**
- ***11:45** Close and next steps*
- ***12:00** Lunch*

Agenda

- The need to protect data
- Information Governance and the market place
- Information Protection entry point to Information Governance
- IBM's Information Protection capabilities
- Summary

Data Breaches continuing to increase

- 2008 recent survey reveals :
- 62% of respondents at some time had their data lost of stolen
- 84% of these expressed increased concern or anxiety due to the data loss.
- Breach costs avg of $202 per compromised record - $152 pertains to indirect cost including abnormal turnover or churn of existing and future customers.
- Cost per victim has risen by 38% over the last 4 years.

Average cost of a data breach in 2008 rises to US$6.65M

46% increase in cost from 2005 - 2008

Source Ponemon Institute: Fourth Annual US Cost of Data Breach Study - Benchmark Study of Companies 2009

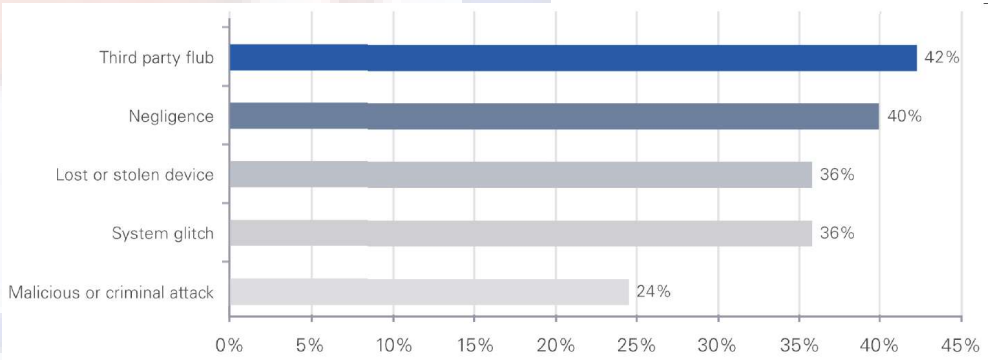
"Today, database security is a lot more challenging than it was a decade ago largely because compliance requirements are more pressing and more complex. Enterprises are dealing with tougher regulatory compliance requirements such as the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), the Sarbanes-Oxley (SOX) Act, and the Payment Card Industry Data Security Standard (PCI DSS). In addition, since compliance requirements do not offer guidelines, confusion exists around what needs to be done to make databases more secure in order to comply."

- *Forrester Research, "A New Role Is Emerging Within IT: Database Security Analyst (DSA)", Noel Yuhanna, 4 April 2008*

2010 Ponemon update

- Most expensive data breach event from 2010 study cost a company US$31 million to resolve - least expensive was US$750,000
- Breach costs avg of $204 per compromised record - $144 pertains to indirect cost including abnormal turnover or churn of existing and future customers.
- 42% of all cases involved 3rd party mistakes / flubs. Data breaches involving outsourced data to 3rd parties, particularly when offshore were most costly.
- Malicious attacks doubled from 12% to 24% from 2008 to 2009
- Recommendation : "*Organizations should consider a holistic approach to protecting data wherever it is - at rest, in motion and in use. Manual and policy approaches may come to mind first but are not as effective as a multi-pronged approach that includes automated IT security solutions.*"

Average cost of a data breach in 2009 rises to US$6.75M



3rd parties – primary cause of a data breach

Source Ponemon Institute: 2010 Annual Study : Cost of a Data Breach Understanding Financial Impact, Customer Turnover and preventative solutions

The PCI Data Security Standard

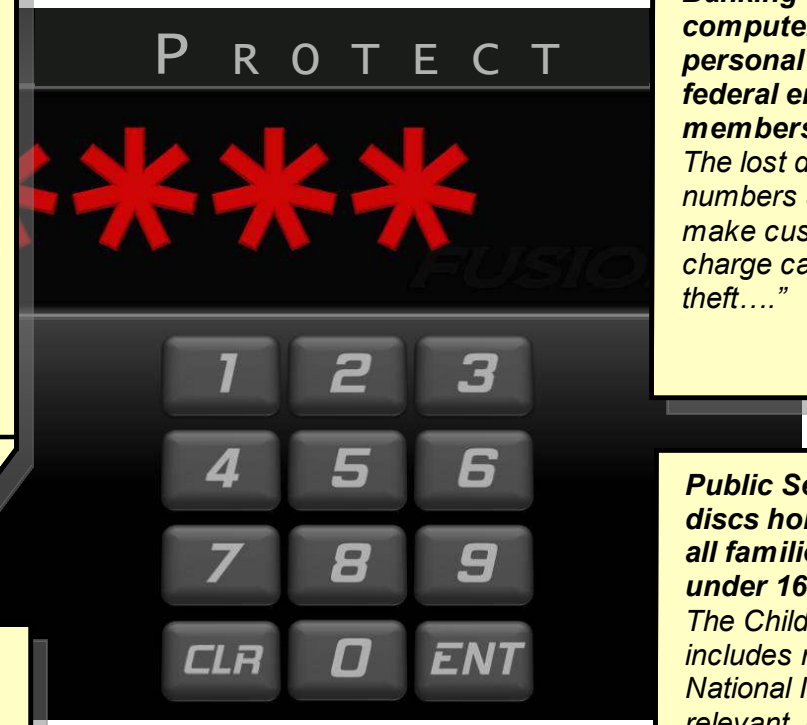
The PCI DSS version 1.2 is the global data security standard adopted by the card brands for all organizations that process, store or transmit cardholder data. It consists of common sense steps that mirror best security practices.

Goals	PCI DSS Requirements
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 across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 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 for employees and contractors

If you don't look after your data – someone else will…

Banking – "A rogue trader accused of the world's biggest banking fraud was on the run last night after fake accounts with losses of £3.7 billion were uncovered…."
The trader used his inside knowledge of the bank's control procedures to hack into its computers and erase all traces of his alleged fraud. Mr Leeson said "Rogue trading is probably a daily occurrence within the financial markets. What shocked me was the size. I never believed it would get to this degree of loss."

Retail – "Hackers have stolen 4.2 million credit and debit card details from a US supermarket chain by swiping the data during payment authorization transmissions in stores.."



Banking – "A major US bank has lost computer data tapes containing personal information on up to 1.2 million federal employees, including some members of the U.S. Senate…."
The lost data includes Social Security numbers and account information that could make customers of a federal government charge card program vulnerable to identity theft…."

Public Sector – "Two computer discs holding the personal details of all families in the UK with a child under 16 have gone missing…."
The Child Benefit data on them includes name, address, date of birth, National Insurance number and, where relevant, bank details of 25million people…"

…. Resulting in a broad range of consequences

Banking – Rogue trader accused of the world's biggest banking fraud was on the run last night after fake accounts with losses of £3.7 billion were uncovered….

Poor Internal Controls..

Bankruptcy, Financial ruin, penalties

Banking – A major US bank has lost computer data tapes containing personal information on up to 1.2 million

Physical Data Loss..

Identity Theft

Ineffective Security..

Brand damage Financial loss

Physical unprotected Data Loss..

Fraud on a massive scale

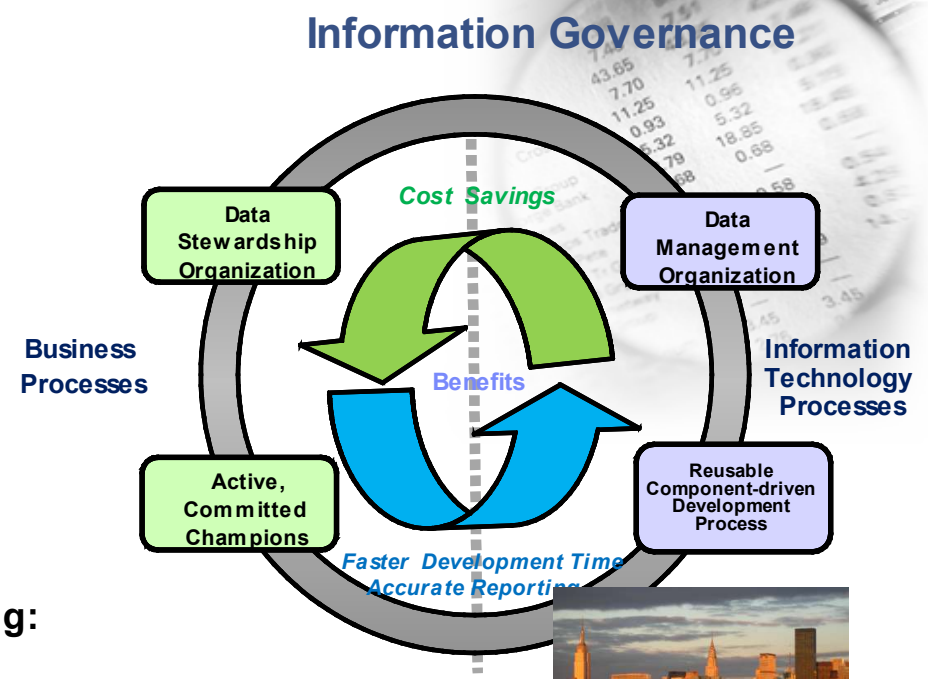
Agenda

- The need to protect data
- Information Governance and the market place
- Information Protection entry point to Information Governance
- IBM's Information Protection capabilities
- Summary

Information Governance – holistic management of data.

*Information governance is the orchestration of **people, process and technology** to enable an organization to leverage information as an enterprise asset.*

*Information Governance **safeguards information, keeps auditors and regulators satisfied,** uses improved data quality to improve customer satisfaction, lower business risk retain customers and constituents and drive new opportunities*

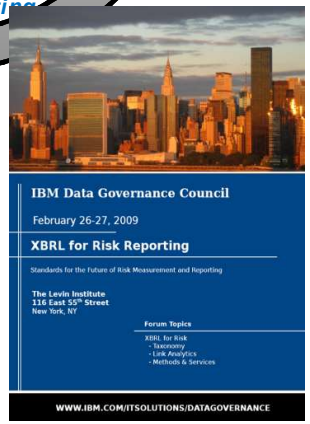


IBM Information Governance Council

Formed in 2004 with 50 Global Companies Including:

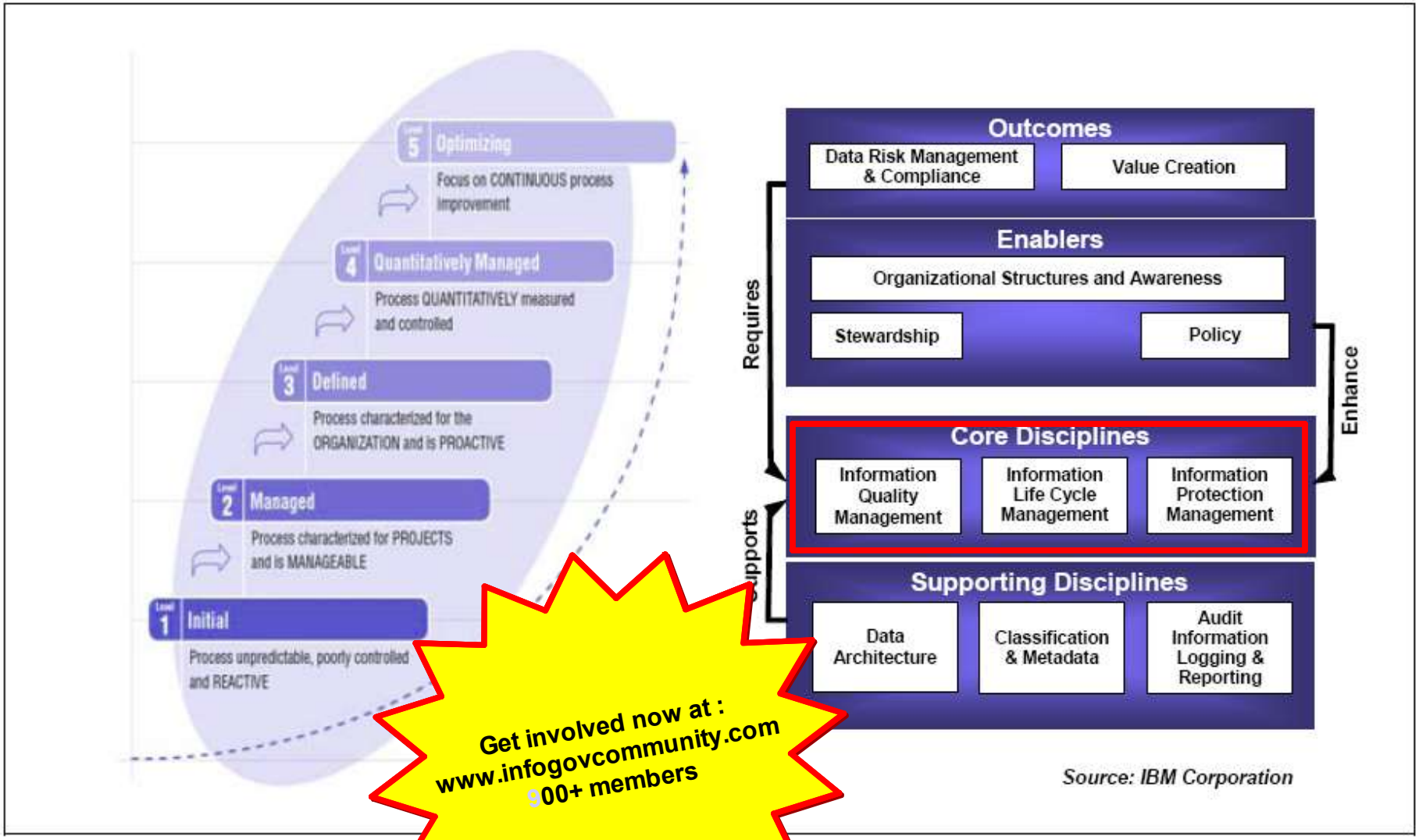
Abbott Labs, American Express, Bank of America, Bank of Tokyo-Mitsubishi UFJ, Ltd, Bank of Montreal, Bell Canada, BMO Financial Group, Citibank, Deutsche Bank, Discover Financial, Kasikornbank, MasterCard, Nordea Bank, Wachovia, Washington Mutual, the World Bank and others…

….and many rely on IBM System z



Information Governance embraces People, Process AND Technology– Puts information at the top of the Agenda…spans both Business and Information Technology in order to successfully manage data

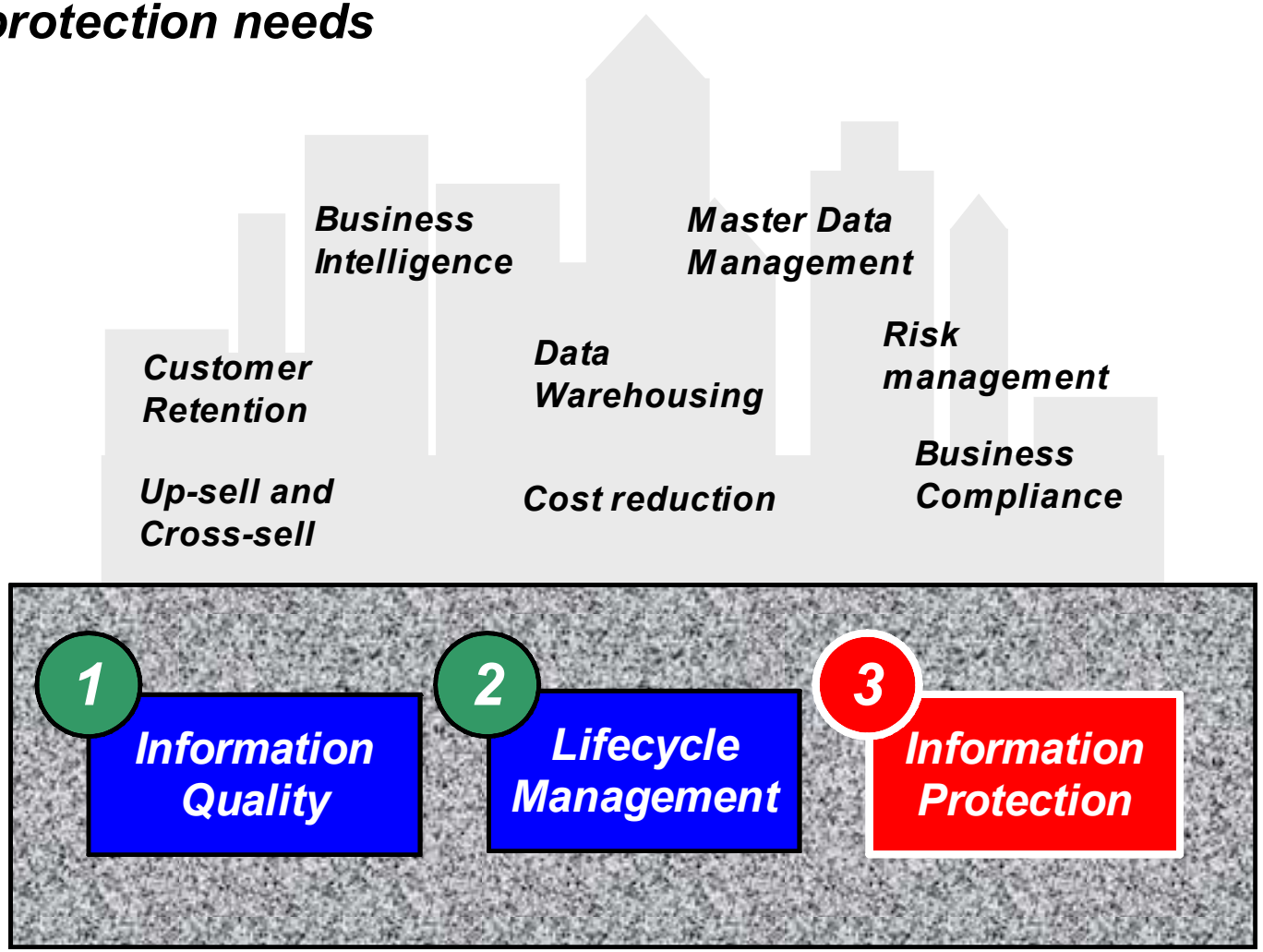
Core disciplines need to be in place to achieve benefits



Get involved now at :
www.infogovcommunity.com
900+ members

Figure 1. IBM's Information Gove… …odel

Information Protection : And 'entry point' to address your most pressing protection needs

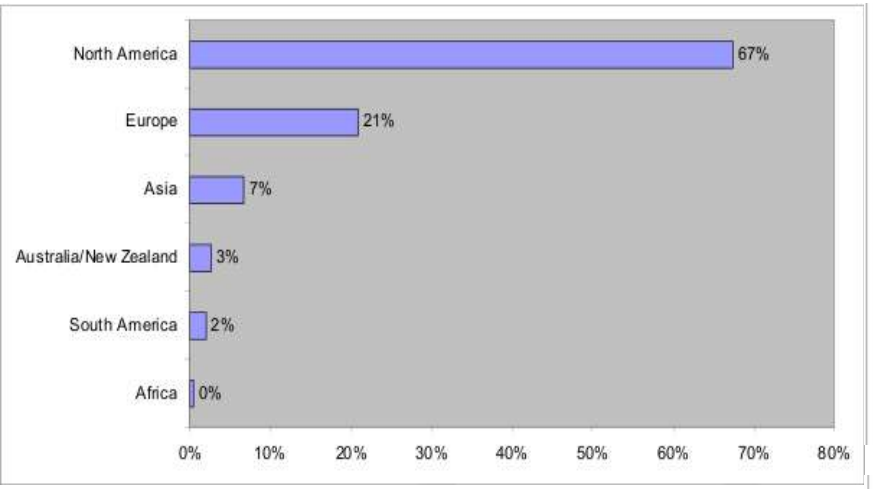


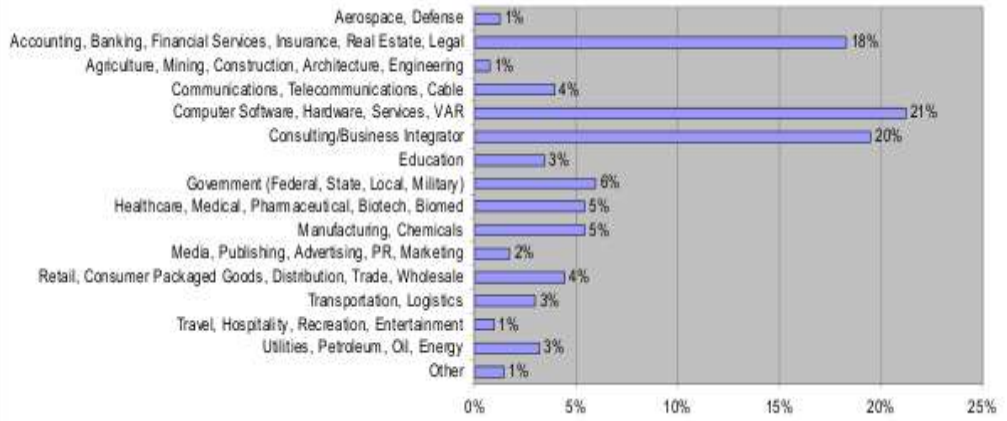
Information Governance underpins and is foundational to your Information Management projects

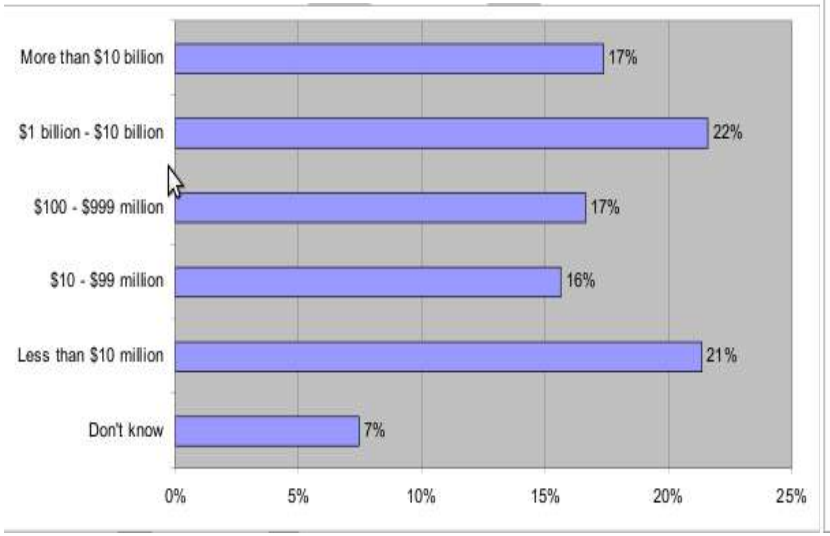
IBM 2010 Information Governance Study

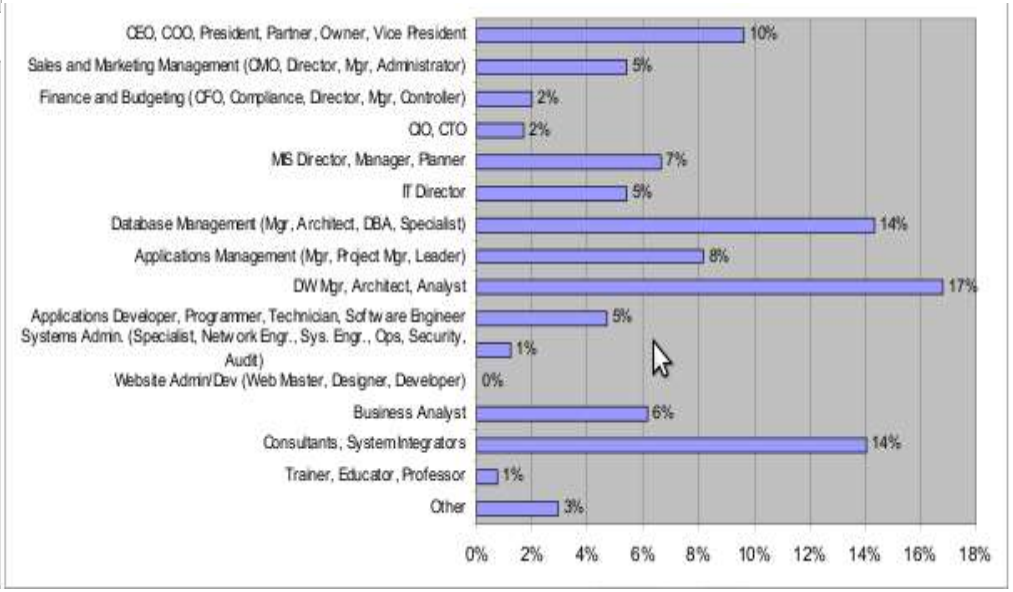
407 Organizations Surveyed Worldwide

available at www.beyeresearch.com/study/14243

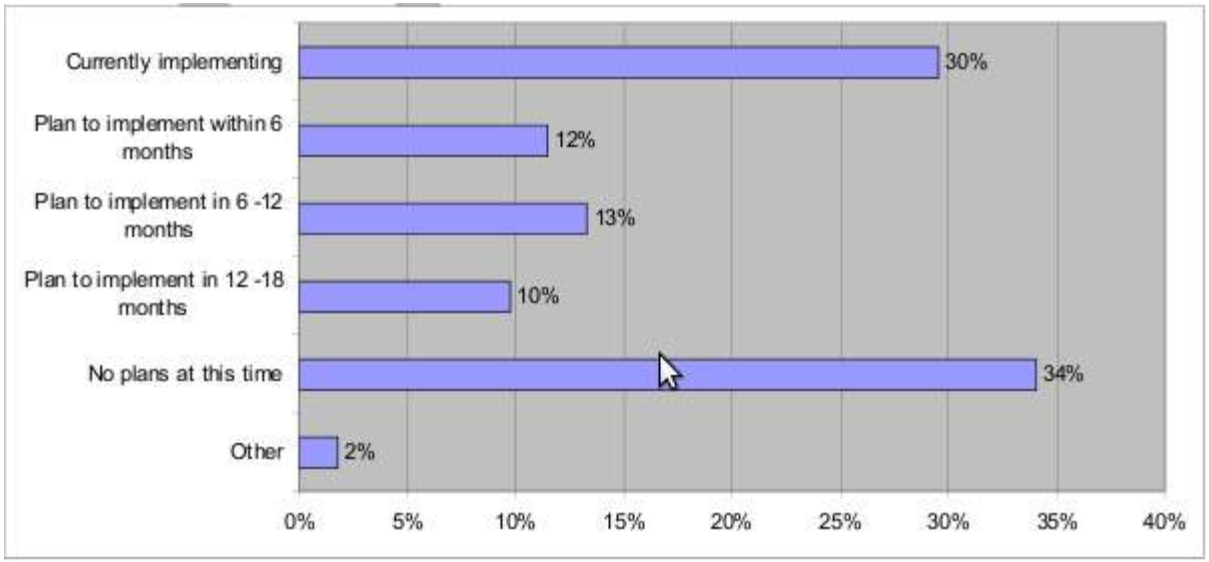






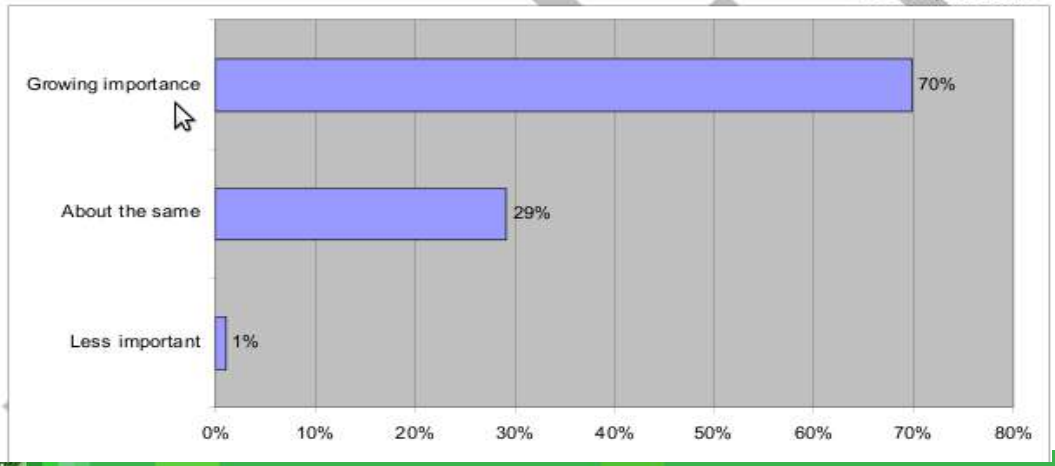


Planning to Implement an Information Governance Program

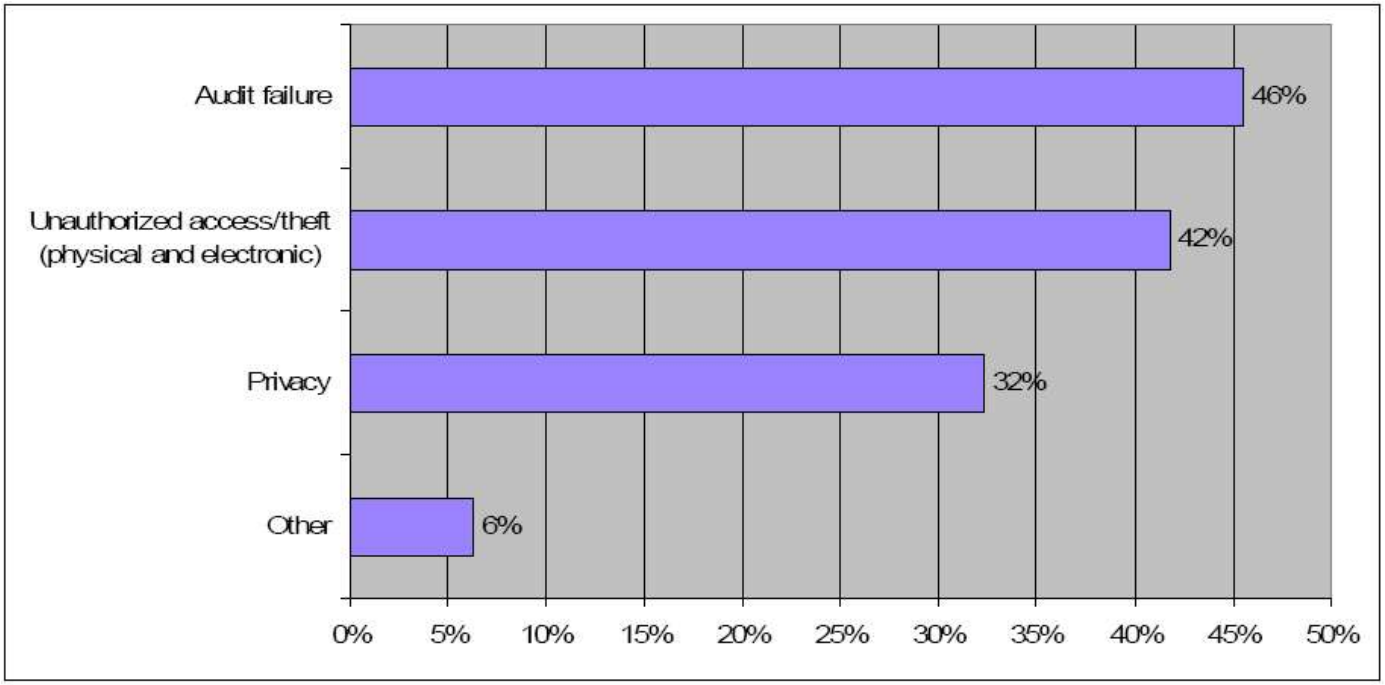


24. How you see the importance of information governance changing over the next 3 to 5 years in relation to business success within your organization?

291 respondents



2010 Information Governance Survey



- *If your organization has experienced information breaches in the last three years, what was the nature of the breach(es)? (Please check all that apply.)*

Enterprise Information is on System z

Information on Demand for System z Delivers Competitive Advantages

DB2: 59 out of the top 60 banks in the world

DB2: 9 of the top 10 global life/health insurance providers

DB2: 23 of the top 25 US retailers

UPS runs DB2 for z/OS to support the world's largest known peak database workload

1.1 Billion SQL statements per hour!

24x7 ATM Deposits & Withdrawals

Runs the world's stock exchanges & banking

Reserves airline seats

Tracks the world's packages

8 of every 10 of the largest retail banks in Australia, Germany, Japan, and the United States use IMS for their core banking

$3 trillion/day transferred through IMS by one customer

95% of top Fortune 1000 companies use IMS

Over 15 billion GBs of production data in IMS…

Agenda

- The need to protect data
- Information Governance and the market place
- Information Protection entry point to Information Governance
- IBM's Information Protection capabilities
- Summary

Information Protection
Entry Point

Information Protection

- *A set of capabilities for Information Protection that secure access, provide encryption of your data, ensure privacy controls are in place, combining powerful but flexible analysis and reporting tools.*

Secure Data
- Prevent Access
- Restrict Access
- Monitor Access

Ensures that data is secure, available to only those that are authorized and all access monitored

Protect Data Privacy
- Mask Data
- Encrypt Data

De-identification that enables organizations to substitutes sensitive data with realistic and fully functional masked data and encryption of online and off line data sources

Audit Data
- Audit Access
- Audit Privileges
- Audit Users

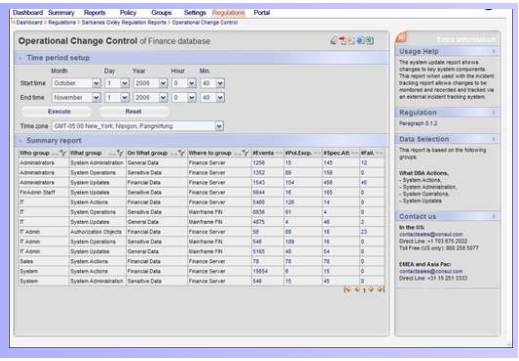
Timely data and flexible reporting for use in internal and external auditing activities – The "who, what, when where, how."

"A company with at least 10,000 accounts to protect can spend, in the first year, as little as $6 per customer account for just data encryption, or as much as $16 per customer account for data encryption, host-based intrusion prevention, and strong security audits combined. Compare [that] with an expenditure of at least $90 per customer account when data is compromised or exposed during a breach,"

Key System z products for Information Protection

Tivoli Security Management for z/OS

- *Facilitate compliance with security requirements and policies*
- *Reducing administration time, complexity, implementation efforts, and costs*
- *Monitor and audit for threat incidents,*
- *Comprehensive enterprise-wide viewand sophisticated analysis of audit*
- *Integrate RACF, mainframe security capabilities for comprehensive identity management, access control, data protection, audit and compliance reporting*



IBM Optim Data Privacy for z/OS

- *Protects sensitive data as it is used for other purposes:*
- *Removes, masks or transforms elements that could identify an individual*
- *Masked or transformed data must be appropriate to the context*

Guardium for z

- *Helps auditors answer Who, What, Where, Why, When, How*
- *Centralizes audit data*
- *Automates auditing process*
- *Creates segregation of duties*
- *Flexible reporting and analysis*

Information Protection Customer Examples

Security - needed improve its system security management and monitoring capabilities. Benefits - robust audit and compliance reporting that can adapt to evolving requests from auditors and compliance officers - Respond quickly to security events, such as breaches or misconfigurations – Improved efficiencies by replacing home grown solutions with off-the-shelf solution

"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

Privacy - protect its confidential employee salary and pension information in non-production (development, testing and training) environments to satisfy data privacy and meet TyEL compliance requirements. Benefit -able to protect confidential data to strengthen public confidence and adhere to TyEL compliance requirements as well.

"Optim's data masking capabilities ensure that we can protect privacy in our development and testing environments," Katri Savolainen, Arek Oy.

Audit and Compliance - Needed to guard against compliance failures

Benefits - Details on who made changes to the data, as well as where and when the changes were made - Let auditors participate in data auditing activities with less database administrator involvement - Free up valuable IT staff resources - Eliminate manual auditing processes that can be time-consuming and error-prone

American Family Insurance leveraged IBM's integrated System z solutions to surpass internal and external audit and compliance requirements – while decreasing IT costs 20%.

Agenda

- The need to protect data
- Information Governance and the market place
- Information Protection entry point to Information Governance
- IBM's Information Protection capabilities
- Summary

Organizations facing many of the following challenges

- Discovering what data needs to be secured
- How to secure your data
- Audit and separation of roles – privileged user conundrum
- Encryption and data obfuscation
- Data in a test environment
- Data life-cycle management and data growth

IBM Information Management Solutions for System z – End to end Solution

Useful urls

- The 2010 Information Governance Market report
  - ftp://public.dhe.ibm.com/software/os/systemz/IBM_Information_Governance_Survey_Report.pdf
- Information Governance Community
  - www.infogovcommunity.com
- Information Protection whitepaper
  - ftp://public.dhe.ibm.com/common/ssi/sa/wh/n/imw14299usen/IMW14299USEN_HR.PDF
- Ponemon Institute report
  - http://www.ponemon.org/data-security

Agenda for this morning….

- ***7:30** Registration / Continental Breakfast*
- **8:15 Session 1 : "End to end Information Protection – the complete picture"**
- *Break (15 mins)*
- **9:30 Session 2 : "Taking back control through Security, Audit and Encryption"**
- *Break (15 mins)*
- **10:45 Session 3 : "Discovery, Privacy and Archiving as part of your information protection strategy"**
- ***11:45** Close and next steps*
- ***12:00** Lunch*

Summary

- **Take Back Control with IBM Information Protection solutions on System z:**
  - Transform your information from a Liability into your most strategic, valuable Asset
  - Help manage business risk by enforcing security, audit, privacy and policy controls
  - Lower operational costs by optimising data management, retention and archiving

- **Software, Hardware and Expertise.**
  - Information Management - the most complete end-to-end Information Protection software solutions
  - Information Protection Entry point as part of your wider Information Governance strategy
  - System z - the ultimate platform to for security
  - Clear ROI business cases for each area of Information Protection .

- For more information visit
  - www.ibm.com/software/data/db2imstools/solutions/data-governance.html


Thank
You