IT RISK MANAGEMENT
PROTECTING THE INFORMATION WE SHARE

ISEC Seminar : Protecting Personal Data in the Electronic Media

Personal Data Security @ JPMorgan

Micky Lo

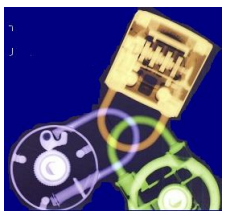
March 2007

JPMorganChase

Agenda

IT RISK MANAGEMENT
PROTECTING THE INFORMATION WE SHARE

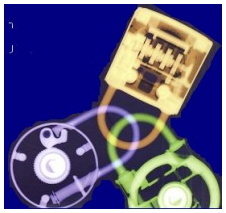
- Data Theft Incidence & Industry Figures
- Threats and Vulnerabilities
- Data Protection Initiatives @ JPM



JPMorganChase

IT RISK MANAGEMENT
PROTECTING THE INFORMATION WE SHARE

- **Data Theft Incidence & Industry Figures**
- Threats and Vulnerabilities
- Data Protection Initiatives @ JPM



JPMorganChase

Personal Data Theft – Myth or Real

IT RISK MANAGEMENT
PROTECTING THE INFORMATION WE SHARE

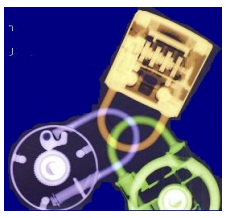
Stolen Devices (Laptops/Tapes/etc)	❖ BOA – 12 million Gov't indiviauls charge-card client SSNs lost on backup tapes ❖ Ameritrade – 200,000customers' private data lost on backip tapes ❖ Time Warner – 600,000 employee SSNs lost on backup tapes ❖ Boeing – Laptop stolen contained 380,000 employee PII ❖ CitiFinancial –3.9 million customer records (name, SSN, payment history) lost with a backup tape ❖ BOA – 18,000 customers' private data lost due to a stolen laptop
Unauthorized Access	❖ Choice Point – 145,000+ individuals' records (name, address, SSN) stolen ❖ LexisNexis – 300,000 consuers' records stolen by hackers ❖ Boston College – 120,000 alumni records (SSN, address) stolen by hackers ❖ Polo Ralph Lauren/HSBC – 180,000 consumer's credit card records stolen by backers ❖ Card Systems – 40 million customer records exposed to hackers
Internal Theft	❖ mPhasis – 4 Call Center agents in India arrested for stealing customer funds after disclosing passwords and PINs ❖ BOA/Wachoiva – 670,000+ customers' account data stolen by bank employees paid by criminal ❖ Mizuho Bank Privacy Manager passed PII to gangster ring ❖ Indian Call Center – undercover reporter able to purchase customer data from call center workers for £3.00
Human Error	❖ Files sent to wrong client ❖ Customers' SSN posted on Internet Website ❖ PII sent to customers
Phishing & Keylogging	❖ Major financial institutions are prime target

JPMorganChase

Identity Theft – Industry Figures

- Identity Theft is the #1 complaint received by the Federal Trade Commission
  - In 2004-2005, over 40% of the complaints received by the FTC were about Identity Theft
- Identity Theft impacts 4.6% of US population per year and growing at 80% in 2004-2005
  - 15 million people in US were victims in 2005-2006 (50% increase)
- Identity fraud cost over USD50 billion losses to business in 2004-2005
- Types of Identity Theft
  - Credit Card fraud (28%)
  - Phone or utility fraud (19%)
  - Bank fraud (18%)
  - Employment fraud (13%)
  - Loan fraud (5%)
- Sources – offline (60%) vs online (11%)
  - PII lost through traditional channel is still higher than electronic channel
  - Electronic channel theft is increasing
- Identity Theft is becoming wider scale and more sophisticated
  - Recent massive identity theft schemes at information brokers and financial institutions have indicated the increase in scale and sophistication.

- Data Theft Incidence & Industry Figures
- Threats and Vulnerabilities
- Data Protection Initiatives @ JPM



Common Pitfalls

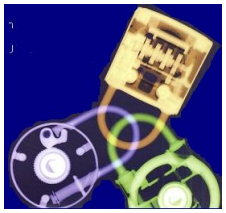
- Lack of comprehensive IT Control Policies on data privacy protection
  - Data classification standard
  - Commensurable security measures
- Inadequate user awareness and training
- Security measures not being extended to PCs at home
  - Personal firewall, anti-virus, anti-spyware, anti-spamware
- General assumptions from users that information stored in a computer is safe
- Over reliance on IT security measures – OS, Firewall and application security
- Overlook the various threats of Data at different stages :
  - In Memory, in Transit, in Storage, at Offsite
- Inadequate security and control measures for portable/mobile devices
  - PDA, Blackberry, Mobile phones, Laptops/Notebooks, etc
  - USB drive, Flash disk, CD/DVDs, etc
- Weak or non-existence of Hardware Disposal and Data Cleansing procedures

Common Pitfalls (cont'd)

- Over reliance on courier to implement adequate security for the transportation of backup tapes
- Passwords and PIN numbers are easy to guess
- Inadequate security for wireless network (business and personal)
- Lack of low tech security and protection awareness
  - Inadequate physical security over sensitive documents
  - Home mailboxes are not locked for convenience
  - Giving out personal information over phone to un-verified parties
  - Unaware of "dumpster diver" existence – forget to shred sensitive documents prior to disposal
  - Unsafe disposal of old PCs
  - Inadequate measures to prevent eavesdropping and shoulder surfing
- Assume Outside Service Providers will implement Data Protection Security

- Data Theft Incidence & Industry Figures
- Threats and Vulnerabilities
- **Data Protection Initiatives @ JPM**

JPMorgan Challenges



Regulatory Requirements

it RISK MANAGEMENT
PROTECTING THE INFORMATION WE SHARE

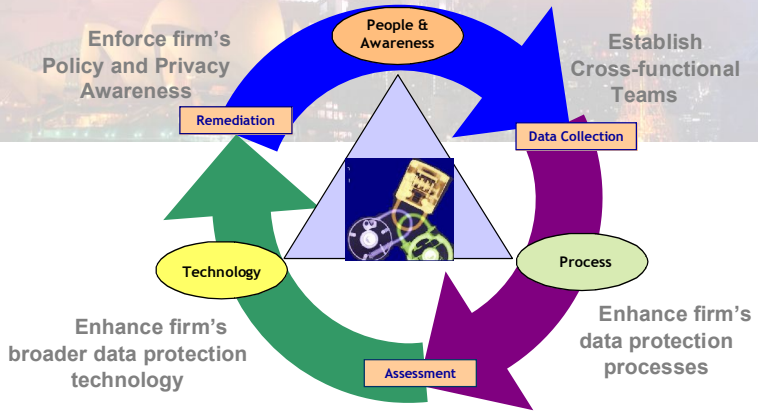
- **Overall**
  - Africa, Asia, Europe and North/South America have adopted new data protection laws over the past decade with many countries modeling their approach after European Union
  - Europe has omnibus approach while US relies on sectoral approach (e.g. financial services and health records)
- **European Union (EU):** 32 countries with laws stemming from EU Data Protection Directive which governs processing of personal data in electronic or paper form
  - Protection of right of natural persons to privacy with respect to personal data:
  - Protection when personally identifiable information (PII) is transferred to another country
- **Asia Pacific (AP):** laws in 5 countries (Australia, Hong Kong, Japan, New Zealand, Taiwan) with most based on EU Directive
- **US : Financial institution privacy law regulates sharing of customer information with affiliates and 3rd parties and safeguarding of customer information**
  - California Senate Bill 1386 on breaches of computerized information
  - Gramm-Leach-Bliley Act of 1999 (GLBA, Section 501(b) on safeguarding customer information
  - Health Insurance Portability and Accountability Act (HIPAA) on computerized health records
  - Fair and Accurate Credit Transactions Act of 2003 (FACT Act) on consumer information
- **Americas (except US):**
  - **Canada**: 10 "fair information" principles protect collection, use and disclosure of "personal information" about identifiable individual
  - **Latin America**: Constitutional protection of *habeas* data rights, i.e. individuals have right to access data about them, and EU style laws

JPM Data Protection - Background

- **Data privacy laws exist in many countries where JPMC does business. Laws are complex and sometimes contradictory**
- **JPMC complies with these laws through LoBs or corporate groups via:**
  - Written contracts or consent regarding data flows between parties and across borders
  - Consumer privacy policies
  - IT Risk Management Program
  - Event management for unauthorized access to or use of information
- **Need to work beyond compliance in order to manage reputation risk**
  - Ensure appropriate event management since we cannot prevent all incidents
    - Oversight from Office of the Executive
    - Multi-disciplinary, leveraging LoB response teams
    - Integrate 24x7 Computer Security Incident Response Team
    - Include media communications and customer notification plans
    - Incorporate lessons learned from internal and external events
  - Expand IT Risk Management Program with Data Protection Initiative
- **A comprehensive firmwide approach is needed to ensure global consistency**

Firm-wide DPI Program

Earlier in 2005, JPM launched the Data Protection Initiative, supplementing our existing IT Risk Management program, to reduce the probability of compromise of our customers' and employees' Personally Identifiable Information (PII).



Data Protection Intiative

IT RISK MANAGEMENT
PROTECTING THE INFORMATION WE SHARE

JPMC IT Risk Management Response: Data Protection Initiative

- Maintain focus on foundational elements of IT Risk Management Program AND expand with Data Protection Initiative
- Data Protection Initiative covers all data classified within JPMC as Confidential & Highly Confidential; however, initial focus is on Personally Identifiable Information (PII) with subsequent expansion to additional data categories
- Protect PII belonging to customers and employees of JPMorgan Chase
- Focus on activities that have a high reduction in risk and a high level of achievability
- Ensure that appropriate incident response procedures are in place and integrated with Corporate event management
- Slow down the *velocity* of leakage of confidential data
- For each area of focus, employ a combination of awareness, technology, and process controls to effect stronger mitigation strategies

Areas of Focus

- When data leaves JPMC
- When data is resident on portable media
- When data is widely available

JPMorganChase

Basic Tenets of Data Protection

IT RISK MANAGEMENT
PROTECTING THE INFORMATION WE SHARE

- Focus on those initiatives that will have a high reduction in risk, and a high level of achievability
- Place a high priority on initiatives that will help your company to comply with laws and regulations regarding the safeguarding and privacy of customer data
- Preventive controls (vs detective and limitative controls) are the most robust for reducing the risk of unauthorized access to data.
- Data stored on portable devices and media poses a high inherent risk to information, due to lack of reliance on physical controls.
- Confidentiality and integrity (non-repudiation) controls provide the highest levels of protection for data transported outside the firm.
- Data must not be transmitted external to the organization without adequate protection measures to prevent unauthorized access.
- Encryption of data in removable storage decreases the risk associated with unauthorized disclosure, and avoids the costs and embarrassment associated with notifying customers in the event of data loss/theft.
- We cannot eliminate incidents related to protection of customer data, so we must be prepared with programs and response processes to mitigate their impact

JPMorganChase