Carol DiBattiste

General Counsel and Chief Privacy Officer

ChoicePoint

Responding to Security Breaches

- Information security breaches are a nationwide, industry-wide problem affecting:
  - Government/Military
  - Educational Institutions
  - Health Care
  - Banking/Credit/Financial Services
  - Businesses
  - Non Profits
- Information security breaches reported during the past three years:
  - 2005, approximately 151
  - 2006, approximately 314
  - 2007, 186 (as of July 2, 2007)

Responding to Security Breaches

- Responding to an information security breach
  - Crisis response plan
  - Notification plan
  - Investigations/lawsuits
  - Conduct enterprise-wide review of privacy and security programs

Responding to Security Breaches

Seven Point Plan to Assist in Protecting Information Against Fraudulent Access and/or Misuse

Responding to Security Breaches

1. Limit access to Sensitive Personally Identifiable Information (“SPII”)
   - Exit high risk markets
   - Remove or truncate SPII when possible
   - Restrict resellers access to certain data

Responding to Security Breaches

2. Credential Customers, Employees and Vendors
   - Centralized credentialing
   - Internal and external verification
   - Site visits
   - Recredentialing program
   - Third party service provider self-assessment questionnaire

Responding to Security Breaches

3. Establish Corporate Accountability

- Chief Privacy Officer reports to Board of Directors Privacy and Public Responsibility Committee

- Working groups
  - Security Advisory Committee (Senior Leadership)
  - Security Working Group (Key Managers)
  - Policy, risk and credentialing sub-working groups

- Privacy and security positions within business units

Responding to Security Breaches

4. Execute Policies, Procedures and Guidelines
   - Data access, protection, transport, restriction, retention, and classification
   - Incident response
   - Credentialing and recredentialing
   - Physical security
   - Information security
   - Public representations
   - Code of Conduct

Responding to Security Breaches

5. Self Regulate Through Audit and Compliance
   - Third party audits
   - In-house audits
     - Customer
     - Consumer sampling
     - Random
     - Suspicious activity
     - Event driven
     - Policy
     - Regulatory compliance

Responding to Security Breaches

6. Implement Technology Solutions
   - Network security
   - External web server scans and application scanning services
   - Encryption
   - Data classification tool
   - Password assessments
   - Risk Management Control Framework

Responding to Security Breaches

7. Enhance Education and Outreach
   - Mandatory annual training programs with assessment
     - Privacy
     - Information Security
     - Code of Conduct
   - Relationship building with privacy advocates, media, government, educational institutions, consumers and customers.