Security & Data Breach Prevention

A Case Study – ChoicePoint Inc (2005)

Presenters:
David T. Lee – Robinson
School of Business, Georgia State University
Steve Travis - IBM
There are two types of Risk:
- The risk you can afford not to take
- The risk you cannot afford not to take

Wisdom is knowing the Difference

-Robert Holden
British psychologist, author
Reminder of Risk

- Legal Risk (Criminal, Civil)
- Financial Risk (Revenues and Costs)
- Regulatory Risk
- Reputational Risk

ChoicePoint suffered them all!!
Discussion Agenda

- ChoicePoint Overview
- Setting the Stage
- Defining the Risk
- The Incident (Fraudulent Data Breach)
- The Fall-Out
- The Remediation
ChoicePoint toughens data security, CNN
Report: Company will now electronically mask sensitive personal info in aftermath of data breach.

ChoicePoint Settles with FTC, Wall Street Journal
January 27, 2006, 8:31 AM

ChoicePoint Settles  Data Security, New York Times
By REUTERS
Published: June 1, 2007

SEC probing ChoicePoint stock sales, MSNBC
Execs sold shares before ID thefts made public
ChoicePoint Security Breach May Affect More Than 140,000
by Jackie Northam, NPR

FTC looks for more victims of ChoicePoint breach
June 19, 2007, Infoworld

FTC Launches Program for ChoicePoint Breach Victims, CIO Magazine

The Five Most Shocking Things About the ChoicePoint Data Security Breach – May 2005, Data Protection Magazine
http://www.msnbc.msn.com/id/7087572/ns/business-us_business/t/sec-probing-choicepointstock-sales/#.T1zjwDF8DHE

http://www.youtube.com/watch?v=VrlO8WtZ-1Y
Company Overview

- Publicly Traded (NYSE), sold to Reed Elsevier for $4.0b plus assumption of debt
- 1997 Spin-out of Equifax
- Information Services Industry
- $1.0B in Annual Revenues
- 3000 Employees - US, Europe
- CEO, President, CAO, CFO - Profiles
Setting the Stage

- **Products** – Reports containing data from Client Files, Public Record Sources and 3rd Parties (i.e. Credit Bureaus)

- **Customers** – Insurance, Banking, Government, Collections, Private Investigators, Mortgage Cos

- **Data Privacy** - FCRA, GLB, DPPA, provider restrictions, Societal Standards

- **Challenge:**
  - Client acceptance (including brokers)
  - Client access (who could see what)
Existing Policies

- Client Acceptance Procedures defined by the Legal Department and Administered by BU Accounting Departments (credentialing dept, defined procedures)

- Customer Access policies were defined by Product Managers and approved by Legal Department (product audits)

- Strong Legal and Internal Audit Department, with good working relationship with the business units.
Defining the Risk

- How to verify applicant credentials
  - is the represented client legit (St. Farm vs. Dave’s Mortgage Co.?)
  - is the applicant associated with the represented client?

- How to determine if customer use of the data is permissible under FCRA (Credit, Insurance, HR, Debts)

- How to determine if customer use of the data is for legitimate purposes

- Rogue users/Password theft (Miami/Dade Police)
Nigerian Fraud Ring used legit California business credentials to pass credentialing, gain access as Non-FCRA customer
- Over several months, ordered 163k reports
- Was opening and closing accounts – customer service noticed suspicious activity
- Sting was set up, 41-year-old Nigerian citizen, Olatunji Oluwatosin, arrested with five cell phones and three credit cards that belonged to other people. Was later sentenced by the Los Angeles County Superior Court to 16 months in prison
The Fall-Out

- California Law called for Notification on Consumers - Media firestorm began (Feb 2005)
- Poster-Child for Security Breaches
- Customer demands for explanations were overwhelming
- Investigations by SEC, FTC, most state’s attorneys general
- Congressional Hearings
- 3rd Party data providers implemented contract audits
ChoicePoint paid a $15m dollar fine/redress to FTC

Signed a Consent Decree with FTC (agreeing to a number of conditions)

Signed Consent Decree’s with over 40 States

Lost over $50m in revenue over next two years

SEC investigation revealed nothing
Immediate Reaction

- Developed Customer Notification Mgt. Plan
- Developed “Affected Consumer Plan”
- Turned off access to over 20k small business accounts in affected business unit.
- Evaluated existing credentialing procedures, made improvements, and began re-credentialing 135k customers. Any suspicious account was site visited.
Hired Chief Privacy Officer, reporting to Board, to oversee remediation efforts and address the “public”

Set up a Board Committee on Privacy

Centralized all Credentialing, rebuilt processes and automated the entire process (where IBM was helpful)

Bolstered Intrusion detection processes

Implemented transaction monitoring, with IP blocking
Remediation

- Developed a full Security Information Framework using GLB, ISO Standards (i.e. internal access, mobile risks, internet monitoring, physical security, executive security/disaster planning, segmentation of duties/communications, etc.)

- Proactive User/Password recycling and auto-canceling

- Bolstered protections in customer contracts, created zones of accountability (i.e. notification rules)

- Implemented Corporate-wide security training program
Considerations moving forward

- Selling Data is not like selling dresses – know your risks and the consequences of the risks

- Continual evaluation of risks vs. costs of risk avoidance or risk reduction methods

- Strong working relationships with your business unit partners – professional disagreement encouraged

- Standardization and automation are keys to understanding what happens in your business each day

- S#!t happens – be ready to deal with it!!
IBM’s Involvement

- Workflow Automation Tools
- Expertise in the Tools was critical to quickly implementing a new solution
Customer Credential Verification System Framework

- Application Studio
- Visibility
- Community Management
- Business Process Management
- Integration and Transformation
- Communications and Security
Customer Credentialing - Solution Footprint

State-of-the-art architecture providing allowing a mix of automated and manual steps to verify the quality of new potential customers.
Security Services Architecture

- Consistent policy enforcement from perimeter to back-end
- Provable regulatory compliance
- Protection of sensitive information
- Strong authentication of parties to transactions

Secure Perimeter Services
Process Automation & Extensibility

- Business Process Models
  - Graphical configuration of processes and services
  - Version management
Each executive has customized view into business unit credentialing status.

Real-time visibility into transactions

Visibility into all incoming and outgoing transactions
Visibility Drill-down to Detail – Resolve Errors

Detail to resolve the problem
Best practices security model

- **Business drivers measure value, risk, & economic costs that influence the approach to Security.**

- **IT drivers represent technical considerations that affect the trustworthiness of the IT environment.**

- The **IBM Security Framework Model** comprehensively supports Business and IT drivers for file transfer security and performance.

---

**Business drivers influencing security**
- Correct & reliable operation
- Service-level agreements
- IT asset value (data)
- Protection of asset value or brand image
- Legal & regulatory compliance
- Contractual obligations
- Financial loss and liability
- Critical infrastructure

**IT drivers influencing security**
- Internal and external threats and threat agents
- IT service management commitments
- IT environment complexity
- Business environment complexity
- Audit and traceability
- IT vulnerabilities: configuration, flaws, exploits

---

**IBM Security Framework Model**
- Security Governance, Risk Management, and Compliance
- People and Identity
- Data and Information
- Application and Process
- Network, Server and Endpoint
- Physical Infrastructure

---

Thank you