Losing Control:
Understanding the Value of Privacy
After a Breach

Christopher T. Pierson, Ph.D., J.D.
Citizens Financial Group, Inc.
Chief Privacy Officer, SVP

August 20, 2008
Background

- Current Chief Privacy Officer, SVP for Citizens Financial Group, Inc. (Citizens and Charter One Banks)
- Former Corporate Attorney/Litigator for 250 person firm - Lewis and Roca LLP; established Cybersecurity Practice Group
- Handled 1st Data Breach in U.S. under California SB 1386
- President/Chairman of FBI’s Phoenix InfraGard corporation - homeland security information sharing program
- Arizona’s Office of Homeland Security Coordinating Council
- Arizona’s Information Technology Security Advisory Committee
- Vice President - High Technology Crime Investigation Association (HTCIA)
- Air War College - National Security Forum
- Programmer for EDS and Circuit City Corporation
Legal Disclaimer

Not Legal Advice

• All content contained herein is for informational purposes only and may not reflect the most current legal developments. Given the changing nature of laws, rules and regulations, and the inherent hazards of electronic communication, there may be delays, omissions or inaccuracies in information contained in this presentation.

• The content is not offered as legal or any other advice on any particular matter. The inclusion of any content in this presentation is not intended to create and does not constitute an attorney-client relationship between you and the author. You should not act or refrain from acting on the basis of any content included in this presentation without seeking the appropriate legal or professional advice based on the particular facts and circumstances at issue in your situation.

• The inclusion or use of company names is for factual and/or news purposes only. No link between a company name and the author should be presumed.

Not My Employer’s Opinions

• The opinions contained herein do not reflect the opinions and beliefs of the author’s employer.

• The opinions contained herein may reflect the opinions and beliefs of the author.

Not My Employer’s Information

• No information from the author’s employer has been used or is referenced within this presentation.
The Problem

Privacy as a Risk
• Companies do not understand Privacy as a risk until a they are impacted by a data breach

Privacy as an Enabler
• Companies do not understand Privacy as an enabler for business functions until a they are impacted by a data breach

Three Examples
1. ChoicePoint
   • In 2005 suffers breach on 145,000 persons information. ChoicePoint reported approx. $12 million in costs in the first half of 2005 ($9 million for legal, $2 million for communication with affected persons) and later a $15 million fine from the FTC.
   • In June 2005, ChoicePoint hires a Chief Privacy Officer to report directly to the Board (also as it’s General Counsel). The CPO bypasses any preexisting institutional governance problems and privacy becomes more readily understood and adopted from the top down.

2. TJX
   • In 2006/2007, TJX suffered a breach of 96 million persons information. To date, the costs are over $300 million and potentially could reach as high as $1 billion.
   • In December 2007, TJX names a senior executive as the Chief Privacy Officer and hires a Privacy Director.

3. HRMC
   • In November 2007, HMRC loses the details of 25 million Britons (7.5 million families) information on an unencrypted CD.
   • Investigation and analysis reports are released in late June 2008. Country laws are in the midst of being modified and many companies are now de facto notifying of a breach incident.
Suggested Solutions

Six Suggested Solutions
1. Define Privacy & Communicate Its Meaning
2. Articulate Privacy Harms
3. Showcase Other Data Breach Events
4. Use Metrics to Showcase Negative Impacts
5. Use Metrics to Showcase Positive Impacts
6. Highlight Similar Risks and Issues within Your Enterprise
7. Have a Solution in Mind
Solution 1 - Defining Privacy

• At its very heart of privacy is the philosophy of “control of information.”

• “Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others”

  Alan Westin: Privacy & Freedom, 1967

• Privacy refers to the protection of information against the unauthorized, illegal, or inappropriate collection, access, use, protection, storage, or disclosure of protected information. This applies to all data, in any form, and collected by any enterprise or its subsidiary or affiliate throughout the lifecycle of its existence.
Defining Privacy

U.S. - A Patchwork Quilt of Privacy Laws:
• Prior to July 1, 2003
  • Notifications done on ad hoc basis or not at all.
  • Incidents reported: actual ID theft, criminal arrest, or leaked.
• After July 1, 2003
  • California SB 1386 Data Breach Law took effect.
  • Company conducts business in California.
  • Required notification to California residents of any actual or suspected breach of the security of personal information.
  • Unencrypted: first initial/name and last name plus SSN, or drivers license/ID no., or account number, or debit/credit and PIN, or now medical/health information. (AB 1298)
• Additional Patchwork Quilt
  • Various requirements under GLBA, Sarbanes-Oxley, HIPAA, PCI DSS, contracts, governments, and regulated industries.
Defining Privacy

U.S. - Patchwork Quilt of Data Breach Laws

• 45 State Laws, 1 City Law (NY City), Countries (Japan, others).
• Federal Guidance for Financial Institutions (12 C.F.R. 30).
Solution 2 - Articulate Privacy Harms

Two Biggest Privacy Harms
1. Loss of Control of Information - i.e. a Data Breach
2. Violated Privacy Promises

Types of Harm
- Civil lawsuits
- Class action lawsuits
- Criminal penalties
- Regulatory penalties/C&D Orders
- Increased scrutiny from regulators
- Financial risks from lost business
- Damage to reputation and goodwill
- Notification, compensation, credit monitoring, and call center costs
- Damage to stock price
- Data recovery costs

©2007 Deloitte Touche Tohmatsu. All rights reserved.
Solution 3 - Showcase Data Breaches

“We apologize again to those consumers who may be affected by the fraudulent activity. We remain committed to helping them take active steps to protect their personal data and to assisting law enforcement officials who are investigating the attacks on consumers’ identities.”

“We deeply regret this unfortunate incident. The privacy of customer information receives the highest priority at Bank [Redacted] and we take our responsibilities for safeguarding it very seriously.”

“We apologize for any inconvenience or concern this situation may cause, but we believe it is important for you to be fully informed of any potential risk resulting from this incident. Again, we want to reassure you we have no evidence that your protected data has been misused. We will keep you apprised of any further developments... we are committed to ensuring that this never happens again.”

“Data Security Fears Growing, Could Lead to Lost Customers”
By Daniel Wolfe, American Banker, January 3, 2007

“New Phishing Attack Uses Fake Journalists to Target Bank Workers”
By Scott Berinato, CSO Magazine, October 18, 2006

“Bank of America Allowed $3B in Money Laundering”

“Dizzying Pace of Data-Breach Notifications In Recent Months Shows No Signs of Slowing”
Computer World, June 19, 2006
Data Breaches

Cost of data breach at TJX soars to $256m
Suits, computer fix add to expenses

By Ross Kerber, Globe Staff | August 16, 2007

TJX Co. said its costs from the largest computer data breach in corporate history, in which thieves stole more than 45 million customer credit and debit card numbers, have ballooned to $256 million.

The figure is more than 10 times the roughly $25 million the Framingham retailer estimated just three months ago, though at the time it cautioned it didn’t know the full extent of its exposure from the breach.

The costs include fixing the company’s computer system and dealing with lawsuits, investigations, and other claims stemming from the breach, which lasted more than a year before the company discovered the problem in December.

TJX disclosed the higher costs in its second-quarter earnings report, released yesterday. For that quarter alone, costs related to the data theft lowered TJX’s profit by $118 million, or 26 cents a share, after accounting for taxes. Yet the company noted that strong sales during the same period suggested customers were not scared away from its stores, which include TJ Maxx and Marshalls. After the disclosure yesterday, shares fell 8 cents to close at $27.50 on the New York Stock Exchange, 8 percent below their level the day before TJX disclosed the security breach in January.

In a statement yesterday, TJX chief executive Carol Meyrowitz said that after months of study, TJX now has a better sense of the exposure. “We have continued to learn more about the computer intrusion(s) and one is not with computer systems,” she said.

Previously this year, TJX has described how 45 million customer credit and debit cards were stolen. The company has sought to attract new customers with expensive electronics from Walmart and Canadian Tire.

TJX spokeswoman Sherry Lang said the company said it would take a charge of $185 million for the next fiscal year, which ends January 2009.

BBC NEWS

Data lost by Revenue and Customs

HM Revenue and Customs (HMRC) has lost computer disks containing confidential details of 25 million child benefit recipients.

The organisation says it does not believe the records — names, addresses, dates of birth and bank accounts — have fallen into the wrong hands. This is not the first time it has lost sensitive information.

STANDARD LIFE CUSTOMERS, NOVEMBER 2007

More than 15,000 Standard Life customers were put at risk of fraud after a courier lost a computer disk containing personal information.

The data was on a computer disk sent from the HMRC National Insurance contributions office in Newcastle to the insurer’s headquarters in Edinburgh.

But the disk containing names, national insurance numbers, dates of birth and pension data never arrived.

HMRC routinely sends computer disks containing personal data on taxpayers to the insurance companies that hold their pensions.
Solution 4 - Negative Impact Metrics

Data Breach Overview

- Since 2005 - Over 230 million lost records
  - TJX - 96 million records
  - HMRC - 25 million records
  - Fidelity National Financial - 8.5 million records
  - Mellon Bank of NY - 4.2 million records
  - BofA - 1.2 million records
  - VA - 26 million records
  - ChoicePoint - 145,000

- 2007 - 125 million lost records

- Actual Breach Costs
  - TJX - $300 million ($1 Billion est.)
  - ChoicePoint - $700 million (est.)
  - ChoicePoint fine - $15 million
Ponemon Institute Annual Survey of data breach costs:
• The total average costs of a data breach are $197 per compromised record.
• Total average costs of a data breach for financial institutions are $239 per compromised record.
• Average total cost per reporting company > $6.3 million per breach.

Do not just focus on data breach costs - show privacy compliance costs

- Gramm-Leach Bliley Act (GLBA) (Safeguards and Privacy Rules)
- Health Insurance Portability and Accountability Act (HIPAA) (Safeguards and Privacy Rules)
- Payment Card Industry Data Security Standard (PCI DSS)
- Fair and Accurate Credit Transactions Act (FACTA) and Disposal Rule
- Fair Credit Reporting Act (FCRA)
- Telemarketing Privacy Laws: CAN-SPAM Act and Do Not Call Rules
- Fines for Non-Compliance
  - ChoicePoint was fined $15 million for violating the Fair Credit Reporting Act and Fair (FCRA) and Accurate Credit Transactions Act (FACTA)
  - BJ’s Wholesale Club has a $16 million reserve to cover the costs related to its breach.
  - Discount Shoe Warehouse (“DSW”) has set aside $6.5 million for it’s breach, noting that costs could rise to $9.5 million.
Privacy Compliance (cont’d)

• Illinois-based American United Mortgage Company violated the GLBA Disposal, Safeguards, and Privacy Rules by failing to properly dispose of credit reports and was fined $50,000

• New York Attorney General fined CS Stars $86,000 because it failed to provide timely notice to 540,000 New York residents whose data went missing when a laptop was lost.

Other Regulatory Fines

• Financial Penalties for FTC Violations - include ongoing costs of bi-annual audits for up to 20 years.
Solution 5 - Positive Impact Metrics

Develop Internal Metrics Around:

• Privacy is About Protecting the Goodwill of the company’s name to Instill Trust in Customers and Brand
  • Value of your company’s name next to its competitors
  • Customer’s impressions of your brand
  • Customer’s impressions of data breach incidents

• The cost of lost business averaged $4.1 million.

• Encourage Worldwide Growth Opportunities
  • Need for Proactive Planning to Share/Use/Transfer Information
  • Need for Proactive Planning to Protect Information

• Global Breach Requirements and Response Programs

• Globally Important
  • Cannot transfer EU data to the United States unless EU requirements met
  • As global market barriers broken down, compliance increasing over use and protection of data
Research Similar Risk & Similar Industry Incidents

• Understand environmental context:
  • Privacy Rights Clearinghouse - http://www.privacyrights.org/ar/ChronDataBreaches.htm
  • Attrition.org - http://attrition.org/dataloss/
  • Etiolated.org - http://etiolated.org/

• Understand types of root causes of these data breach incidents:
  • Classify by type of harm
  • Classify by type of loss
  • Classify by mitigants/potential mitigants

• Conduct Privacy Risk Analysis
• Compare External Patterns to Risk Analysis
Solution 7 - Have a Plan in Mind

Pillars of an Effective Privacy Program:

- Governance
- Education
- Internal Training
- Internal Controls
- Compliance Testing
Contact Information

Christopher T. Pierson, Ph.D., J.D. (CIPP/G)
Chief Privacy Officer, SVP
Citizens Financial Group, Inc.
401.282.5422
christopher.t.pierson@citizensbank.com