



# Ripped from the Headlines: Data Security and Data Breaches

The webinar will begin momentarily

Audio Instructions:

U.S. Toll Free: 877-366-0713

Canadian Toll Free: 866-627-1653

International Toll: 302-607-2000

Participant Code - 89610045#

Technical Support:

Audio: (302)709-8255(TALK)

WebEx: +1-408-435-7088

Trusted Advisors  
*industry experts*  
LEGAL ADVOCATES  
MINTZ LEVIN COHN FERRIS GLOVSKY AND POPEO PC



**MINTZ LEVIN**  
MINTZ LEVIN COHN FERRIS GLOVSKY AND POPEO PC

# Ripped from the Headlines: Data Security and Data Breaches

Cynthia J. Larose, Esq., CIPP

June 21, 2007



## Today's Agenda

- What we'll cover today
  - *Privacy vs. Security and how they relate*
  - *Data Breach Notification*
  - *The View from Capitol Hill*
  - *The Incident Response Plan*
  - *Other Privacy-Related Issues*
- What we WON'T cover today
  - *Specific privacy laws (GLB, HIPAA, FACTA, etc.)*
  - *European Union Data Privacy Directive*

### Technical Support:

Audio: (302)709-8255(TALK)

WebEx: +1-408-435-7088

Trusted Advisors  
industry experts  
LEGAL ADVOCATES  
MINTZ LEVIN COHN FERRIS GLOVSKY AND POPEO PC



# “Privacy” - Why All the Buzz?

2005 - ID thieves - 623,000



2005 - Lost backup tape -- 1,200,000



2005 - Hacking -- 1,400,000



2006 - Dishonest insiders -- 676,000



WACHOVIA

2006- Hacking ..... 40,000,000 accounts *CardSystems Solutions*

2006/07 - “Unauthorized intrusion” - 45,000,000 accounts



2007 - **YOUR COMPANY OR CLIENT???**

Trusted Advisors  
COMMITTED CITIZENS industry experts  
LEGAL ADVOCATES  
MINTZ LEVIN COHN FERRIS GLOVSKY AND POPEO PC



## Since ChoicePoint

- Since the report of the ChoicePoint incident in February of 2005 through last week:
  - 155,160,842 + individual records affected
- Compromise has occurred through hacking, insider misconduct, loss of encrypted or unencrypted data, loss or theft of computers/laptops
- Retail, banking, educational institutions, state & federal government agencies -- no sector immune

*Source -- Privacy Rights Clearinghouse*



## Not Only the Press

- Privacy/security is also getting the attention of regulators
- BJ's Wholesale Club and DSW Inc. -- nearly identical FTC Consent Orders
  - *Customer PII not adequately secured*
  - *Security audits every two years for next 20 years*
- ChoicePoint -- FTC Consent Order
  - *Largest civil penalty in FTC history*
  - *\$10 million in civil penalties*
  - *\$5 million in consumer redress*
- TJX Companies????????????? Under investigation at FTC



# Back to the Basics -- Privacy = Security = Privacy

- Data privacy and information security are linked
- Information security is a legal issue and a technology issue
- It applies to all companies
- There is a legal standard for security
- The law is a “work in progress”



## Security - Privacy Nexus

- Responsible data security practices are a prerequisite for meaningful privacy
- Privacy and security teams working together: *It's all about the data*
  - *Complementary resources in ascertaining data collection, use and repositories*
  - *Occasional tensions between privacy and security considerations*
  - *Senior management sometimes*



## Security - Privacy Nexus

Of the reported breaches of approximately 70 million records:

- 4% - Lost backup tapes
- 7% - Unauthorized access to paper
- 19% - Programming or other human error
- 25% - Hacking resulting in unauthorized access
- 45% - **Stolen/Lost computer/portable device**

*Source: Privacy Rights Clearinghouse*



## Law Addresses Security in Three Ways

- It protects the security of your assets
- ➔ • It imposes security obligations
- It gives you legal benefits for implementing security

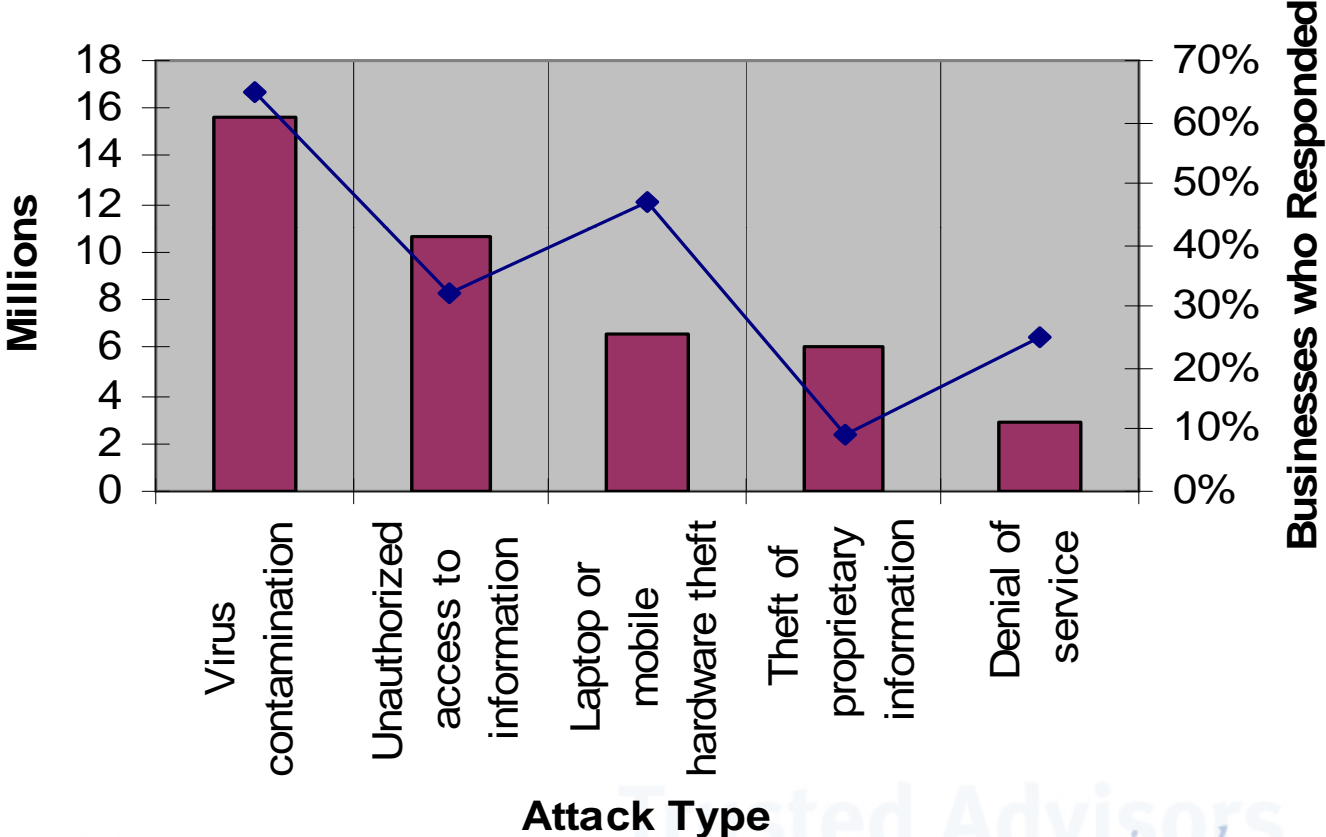


## What Type of Legal Obligations?

- Duty to provide appropriate security
  - *To prevent breaches*
  - *To detect breaches*
  - *To respond to breaches*
- Duty to warn
  - *Duty to disclose breaches to those who may be affected/injured*
- Duty to disclose state of security readiness
  - *Transparency for investors, customers, and others who may be affected*



# 2006 CSI/FBI Survey: Top 5 most costly attacks





# The Duty to Warn: Breach Notification

COMMITTED CITIZENS **Trusted Advisors** *industry experts*  
**LEGAL ADVOCATES**  
MINTZ LEVIN COHN FERRIS GLOVSKY AND POPEO PC



# The Breach Notification Obligation

- Covered Information
  - *Any combination of PII*
- Triggering Event
  - *Any unauthorized acquisition of [unencrypted] computerized data. Almost any breach of security will trigger notice obligations in most states*
- Who?
  - *Owners of the PII affected by the breach*
- What?
- When?
  - *“in the most expedient time possible and without unreasonable delay”*
- How?



## The Breach Notification Obligation (2)

- How?
  - *In writing (on paper and sent by mail)*
  - *In electronic form (by e-mail, but only if the individual has consented in advance to receive the notice in electronic form)*
  - *By substitute notice*
  - *Montana, NY and NC also provide for telephonic notice*
  - *ME does not authorize e-mail notice*
  - *Interagency Guidance: “Customer notice should be delivered in any manner designed to ensure that a customer can reasonably be expected to receive it. For example, the institution may choose to contact all customers affected by telephone or by electronic mail for those customers for whom it has a valid e-mail address and who have agreed to receive communications electronically.”*



# Security Breach Notification Laws -- Federal vs. State

- Issues?
  - *Security Practices*
    - Develop, implement and maintain an effective information security program for sensitive personal information.
    - Develop procedures for verifying the credentials of any third party seeking to obtain the sensitive personal information of another person.
    - Develop disposal procedures to be followed by covered entities that (a) dispose of sensitive personal information or (b) transfer sensitive personal information to third parties for disposal.



## Current Legislative Environment

- Omnibus privacy legislation being touted by senior members of Congress
- Activity on spyware legislation
- States still focusing on data breach notification laws



# State Data Breach Notification Laws California

- The big daddy -- the trigger for ChoicePoint notification
- Companies must notify consumers if there is/believed to be a breach of “unencrypted personal information” from computerized data
- If encrypted, but there is a breach = no notification
- “Personal information” defined as first and last name plus
  - *Social Security number;*
  - *Driver’s license or California Identification number; or*
  - *Account number, credit/debit card number, in combo with password or access code*



## Other State Laws

- Multiple states followed the California lead -- up to 38 states
- Some states have also passed laws requiring reasonable security procedures
- Differing standards and requirements (even for those based on California law) have led to industry requests for federal action that includes preemption.



## Enforcement

April 26, 2007

- CUOMO OBTAINS FIRST AGREEMENT FOR VIOLATION OF SECURITY BREACH NOTIFICATION LAW
  - *CS Stars failed to notify that computer containing info on 540,000 New Yorkers went missing. Paid NY AG \$86,000 for costs of investigation*

May 24, 2007

- AG ABBOTT TAKES ACTION AGAINST NATIONWIDE LENDING FOR EXPOSING CUSTOMER RECORDS
  - *Check 'n Go case is sixth ID theft enforcement action by Texas AG in recent weeks.*



## The response to TJX?

COMMITTED CITIZENS **Trusted Advisors** *industry experts*  
**LEGAL ADVOCATES**  
MINTZ LEVIN COHN FERRIS GLOVSKY AND POPEO PC



## New Minnesota Law

- On May 25, 2007, governor signed Minn. Stat. 365E.64
- Effective August 1
- Prohibits persons and businesses doing business in MN from retaining data from mag strips on payment cards -- as well as security codes and PINs -- for more than 48 hours after a card transaction is approved
- Authorizes financial institutions to recover “reasonable costs” incurred to respond to theft of cardholder data
- Five other states (including MA) considering similar laws  
(TX, IL, CT, MA, CA)



## Massachusetts?

- Two versions pending, a House and Senate version.
- Slated for a Conference Committee, which has yet to have members of both branches appointed, but is expected to happen in the near future (possibly tomorrow).
- From there, the Committee will review the multiple ID theft versions, searching for some sort of compromise, specifically on their two main differences: 1) threshold triggers for fees; and 2) levels of responsibility for the thefts.



## Federal Update

- **Four Proposed Bills in the Senate**
- S.495 (Sponsored by Leahy-Specter): Personal Data Privacy And Security Act of 2007. Reported out of Judiciary Committee and on May 23rd placed on Senate legislative calendar.
- S. 239 (Sponsored by Feinstein): Notification of Risk to Personal Data Act of 2007. Reported out of Judiciary Committee with an Amendment on May 3, 2007.
- S. 1178 (Inouye-Stevens): Identity Theft Prevention Act. Reported out by Commerce Committee with amendments on April 25, 2007.
- S. 1368 (Carper-Bennett): Data Security Act of 2007. Introduced, referred to Banking Committee.



## Federal Update

- Security program implementation:
- Three of the four bills (S.239 is the exception) require businesses or “covered entities” to implement a data security program.
- S. 495 excludes those covered by GLBA or HIPAA. S. 1178 excludes those that meet certain GLBA requirements and electronic communication that is stored by a third party for purposes of transferring or transmitting communication.



## Federal Update

- Notice:
- S. 495 and S. 239- notice required without unreasonable delay.
- S. 1178 - notice required if it is determined that the breach creates a “reasonable risk of identity theft.”
- S. 1268 - notice required *after* (1) determined that breach may have occurred; (2) investigation into scope of breach; (3) PII likely to be misused; and (4) appropriate regulators notified.



## Federal Update

- When Notice is not Required:
- S. 495 and S. 239 - not required (1) if notice could cause damage to national security (requires coordination with Secret Service); (2) if no significant risk of harm based on encryption of information; or (3) if entity participates in Financial Fraud Prevention security program.
- S. 1178 - notice not required if reasonable risk of identity theft does not exist.
- S. 1268 - in compliance with federal requirements if entity has own notice and compliance policies and procedures that include notice to individuals and government agencies.



## Federal Update

- Digital And Paper Records Covered:
- S. 495 and S. 239 covers only electronic or digital records.
- S. 1178 and S. 1268 covers electronic or digital records and paper.



## Federal Update

- Federal Penalties:
- S. 495- for violations of data security requirements maximum fine of \$500,000 (\$5,000 per day per individual) and injunctions and an additional maximum of \$500,000 for willful violations.
- S. 495 and S. 239 - for violations of notice requirements fines of up to \$1,000 per individual per day with a maximum of one million dollars per violation.
- S. 1178 and S. 1268 do not establish penalties specific to the Act.



# Federal Update

- State Enforcement:
  - *S. 495 and S. 239 - similar to federal penalty provisions.*
  - *S. 1178 permits civil action by State AG to enforce provisions of the Act.*
- Private Right of Action:
  - *None of the bills appear to permit a private right of action.*
- Criminal Penalties:
  - *Only S. 495 has a provision for criminal penalties when a security breach is concealed.*



## Federal Update

- State Preemption:
- S. 495 supersedes state laws regarding data security and notice of data breaches. S. 239 supersedes state notice laws.
- S. 1178 and S. 1268 preempts state laws regarding data security and notice of data breaches.



## International Update

- CANADA:
- Report issued in May -- endorsed passage of a data breach notification law, but recommended that notifications be made to the Privacy Commissioner
- EUROPEAN UNION:
- No current requirement for data breach notification
- Opened consultation last fall on issue of data breach notification (ePrivacy Directive)
- Initially scheduled for early 2007, proposals are expected to be published in October 2007

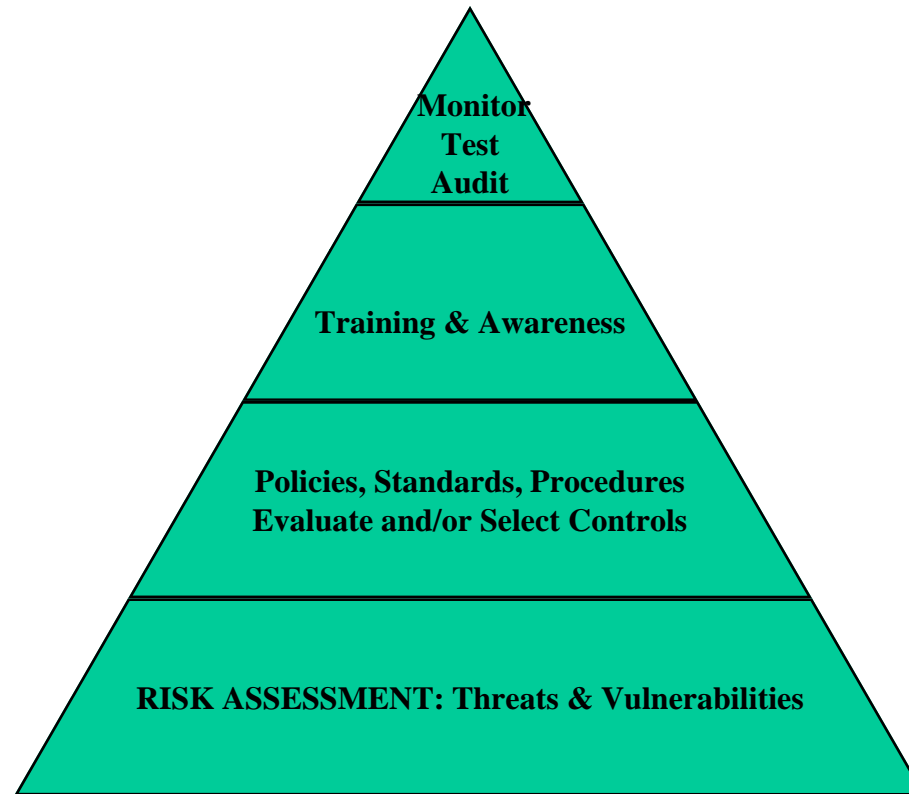


## So, What's Next?

- It's all about the process
- Security consultants have been saying for some time:  
"Security is a process, not a product"
- Developing legal standard does not literally dictate what is  
"reasonable security"
- Sets out requirements for a fact-specific process



# Building Blocks for Both Privacy and Security Programs





Desired result:

# The Comprehensive Information Security Program

COMMITTED CITIZENS **Trusted Advisors** *industry experts*  
**LEGAL ADVOCATES**  
MINTZ LEVIN COHN FERRIS GLOVSKY AND POPEO PC



# How to Plan for a Breach

COMMITTED CITIZENS **Trusted Advisors** *industry experts*  
**LEGAL ADVOCATES**  
MINTZ LEVIN COHN FERRIS GLOVSKY AND POPEO PC



# Incident Response Planning

- Plan for the worst
- Approach should not be from the “if” a breach happens -- should be from the “what will we do WHEN”
- Have plans and procedures in place
- Draft notices should be ready to go -- and know who needs to be notified and when



# Incident Response Planning

- Incident Response Team (IRT) Goals
  - *Protect the institution from significant financial loss or reputation damage*
  - *Protect customers from loss of confidential information*
  - *Contain the intrusion, restore systems, and provide assistance to customers*
- How?
  - *Core team to manage a security breach*
  - *Clearing house for investigation, containment, compliance, law enforcement, and the media*
  - *Empowered to take swift and decisive action*



# Incident Response Planning

- Elements to consider:
  - *Designate person responsible for coordination*
  - *ID participants/roles/24/7 contact information*
  - *Identify regulatory, law enforcement, other external contacts*
  - *Procedures to ensure prompt internal notification of team, management, and internal owner of data*
  - *Procedures to contain, control and correct any incident*
  - *Procedures for notification of stakeholders, regulatory and law enforcement (as appropriate)*
  - *Address responses to likely inquiries and train responders*
  - *Procedure to document all responsive actions*
  - *Regularly review and revise the incident response plan*



# Incident Response Planning IRT Members

- IT Security Officer
- Legal Issues Contact - Inside/Outside Counsel
- Public Relations Contact - Crisis Management
- Human Resources / Personnel Contact
- Security Incident Investigations & Forensics
- Information Systems Officer
- and other Business Managers as appropriate



# How do you know your incident response plan works?

COMMITTED CITIZENS **Trusted Advisors** *industry experts*  
**LEGAL ADVOCATES**  
MINTZ LEVIN COHN FERRIS GLOVSKY AND POPEO PC



**PRACTICE, PRACTICE, PRACTICE!**

COMMITTED CITIZENS **Trusted Advisors** *industry experts*  
**LEGAL ADVOCATES**  
MINTZ LEVIN COHN FERRIS GLOVSKY AND POPEO PC



## Related Security/Privacy Issues

COMMITTED CITIZENS **Trusted Advisors** *industry experts*  
**LEGAL ADVOCATES**  
MINTZ LEVIN COHN FERRIS GLOVSKY AND POPEO PC



## Social Security Numbers

- Key to a person's electronic identity
- Government has begun to limit use of SSNs as identifiers
- Laws will most likely increase -- many new laws already proposed for 2007
- "Best practice" = adoption of use of identifiers in lieu of SSNs wherever possible and limiting or elimination display of customer SSNs in internal data access



# Social Security Numbers

- Federal laws
  - *5 USC 552a limits federal government's use and display of SSNs and other PII in an agency's "system of records". It allows individuals to review and correct information the government collects on them.*
  - *31 USC 3327(b) requires that SSNs not be visible through window envelopes in which the Treasury mails federal government checks.*



# Social Security Numbers

- California prohibits the following:
  - *Posting or publicly displaying SSN*
  - *Printing SSN on ID cards or badges*
  - *Requiring SSN to be transmitted over non-secured Internet connection*
  - *Requiring the use of an SSN as a log-in without a password*
  - *Printing SSN on materials to be mailed to individuals (except as required by law)*



# Identity Theft

- Fastest growing crime
- \$12 billion+ fraud losses worldwide
- Globally impacts 2,000+ people per day
- 10 million US victims in 2004 per FTC (4.6% of adult population)
- 27 million Americans victimized in past 5 years
- Forecast: 1 in 4 Americans in next 4 years

Source: *Consumer Awareness Against Identity Theft, Federal Trade Commission*

Trusted Advisors  
COMMITTED CITIZENS  
industry experts  
LEGAL ADVOCATES  
MINTZ LEVIN COHN FERRIS GLOVSKY AND POPEO PC



## Identity Theft (2)

ID Fraud = Creating a brand new identity from several different sources to commit crimes and evade detection.

**“Social Engineering”**



Area of Risk	Hacker Tactic	Combat Strategy
Phone (Help Desk)	Impersonation and persuasion	Train employees/help desk to never give out passwords or other confidential info by phone
Building entrance	Unauthorized physical access	Tight badge security, employee training, and security officers present
Office	Shoulder surfing	Don't type in passwords with anyone else present (or if you must, do it quickly!)
Phone (Help Desk)	Impersonation on help desk calls	All employees should be assigned a PIN specific to help desk support
Office	Wandering through halls looking for open offices	Require all guests to be escorted
Mail room	Insertion of forged memos	Lock & monitor mail room
Machine room/Phone closet	Attempting to gain access, remove equipment, and/or attach a protocol analyzer to grab confidential data	Keep phone closets, server rooms, etc. locked at all times and keep updated inventory on equipment
Phone & PBX	Stealing phone toll access	Control overseas & long-distance calls, trace calls, refuse transfers
Dumpsters	Dumpster diving	Keep all trash in secured, monitored areas, shred important data, erase magnetic media
Intranet-Internet	Creation & insertion of mock software on intranet or internet to snarf passwords	Continual awareness of system and network changes, training on password use
Office	Stealing sensitive documents	Mark documents as confidential & require those documents to be locked
General-Psychological	Impersonation & persuasion	Keep employees on their toes through continued awareness and training programs



## Resources

Summary of State Data Breach Notification Provisions -  
[www.mintz.com/newsletter/2007/PrivSec-DataBreachLaws-02-07/state\\_data\\_breach\\_matrix.pdf](http://www.mintz.com/newsletter/2007/PrivSec-DataBreachLaws-02-07/state_data_breach_matrix.pdf)

Privacy Rights Clearinghouse - [www.privacyrights.org](http://www.privacyrights.org)

Federal Trade Commission - [www.ftc.gov](http://www.ftc.gov)



MINTZ LEVIN

MINTZ LEVIN COHN FERRIS GLOVSKY AND POPEO PC

## Questions?

Cynthia J. Larose  
[cjlarose@mintz.com](mailto:cjlarose@mintz.com)

617-348-1732



For more information on the International  
Technology Law Association...

Visit [www.ITechLaw.org](http://www.ITechLaw.org)  
or call  
1-781-876-8877

COMMITTED CITIZENS *Trusted Advisors* *industry experts*  
LEGAL ADVOCATES  
MINTZ LEVIN COHN FERRIS GLOVSKY AND POPEO PC