What To Do When Your Data Winds Up Where It Shouldn't

Don M. Blumenthal

Defcon 16

Las Vegas, Nevada

August 9, 2008

© 2008 – Don M. Blumenthal

Disclaimer

- Opinions expressed are my own and intended for informational purposes. They should not be attributed to any organization or used as a substitute for direct legal advice.

© 2008 – Don M. Blumenthal

Questions and more Questions

- What is PII
- What is a Security Breach
- To Whom Does the Law Apply
- When and How Is Notice Given
- Whom Do I Have to Notify?
- What Do I Offer?
- How Do I Plan Ahead?

© 2008 – Don M. Blumenthal

PII Definition - AICPA/CICA

- Information related to identified or identifiable individual
  - Name, Address, Telephone, SS # or Other Govt ID Numbers
  - Employer, Employment History
  - Credit Card Numbers, Credit History, Purchase History
  - Personal or Family Financial or Medical Information

© 2008 – Don M. Blumenthal

PII Also May Include

- "Sensitive PII"
  - PII Specifying Medical or Health Conditions
  - Racial or Ethnic Origin
  - Political Opinions
  - Religious or Philosophical Beliefs
  - Trade Union Membership
  - Sexual Preferences

© 2008 – Don M. Blumenthal

Legal Framework Overview

- US - Sectoral approach to security and privacy with patchwork of laws
  - Specific types of records
  - Specific types of institutions
- EU Model - Societal approach
  - EU member states
  - Argentina, Australia, Canada, Switzerland
- Hybrid Model
  - Japan, Chile, APEC
- No law
  - China, India, Philippines, most of South America

© 2008 – Don M. Blumenthal

Scope

- Laws concern
  - Personal information
  - Personally Identifiable Information
  - Sensitive Consumer Information
- Don’t forget
  - Non-consumer data; e.g., trade secrets
  - PAPER

© 2008 – Don M. Blumenthal

Know Relevant Data Security/Privacy Laws

- Gramm-Leach-Bliley Act
- Fair Credit Reporting Act/Fair and Accurate Credit Transaction Act
- Health Insurance Portability and Accountability Act
- Family Educational Rights and Privacy Act

© 2008 – Don M. Blumenthal

Know Other Important Laws

- FTC Act Section 5
- Sarbanes Oxley Act

© 2008 – Don M. Blumenthal

Know the Regulators

- GLBA – eight agencies
- FCRA/FACTA - FTC
- Sarbanes Oxley – SEC
- HIPAA - HHS
- FERPA - DoE

© 2008 – Don M. Blumenthal

Know the Regulations

- GLBA – FCRA/FACTA
  - Safeguards, Privacy, Disposal Rules
  - Red Flag Rule in October, 2008
  - FFIEC guidelines - track GLB Safeguards but set out processes and criteria in more detail
- HIPAA
  - Security and Privacy Rules
- SOX
  - Section 404

© 2008 – Don M. Blumenthal

Don’t Forget

- International laws and directives
- Common law/private rights of action
- Private standards

© 2008 – Don M. Blumenthal

Common Law

- Private sector privacy issues
- Tort
- Contracts – explicit or implied data protection

© 2008 – Don M. Blumenthal

Standards - examples

- Private
  - Payment Card Industry-Digital Security Standard (PCI-DSS)
  - ISO; e.g., 27001, 27002
  - CoBIT
- Federal
  - FISMA
  - FIPS 200
  - NIST 800-53

© 2008 – Don M. Blumenthal

But For All of That

- Only two explicit sets of national requirements exist concerning breach response planning
  - Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice
  - FISMA
- No non-US government or government alliance has a breach notification requirement

© 2008 – Don M. Blumenthal

Interagency Guidance

- Issued by four GLBA agencies
- OCC, Federal Reserve, OTS, FDIC
- Introduces yet another definition – Sensitive Consumer Information
  - PII or combination of customer information that would allow someone to log onto or access the customer's account; *e.g.*, user name and password or password and account number.

© 2008 – Don M. Blumenthal

Breach Response under Guidance

- Must have plan to assess nature & scope of incident and identify what PII has been accessed or misused
- Must notify primary GLBA regulator and other relevant law enforcement
- Must notify data owners if breach involves Sensitive Consumer Information
  - Describe incident and how handled
  - Provide data protection consumer education and services

© 2008 – Don M. Blumenthal

FISMA

- Requires procedures for detecting, reporting, and responding to security incidents
- No requirement of notice to individuals whose information has been compromised
- Application of FISMA and related guidelines outside of federal agencies is a subject of debate

© 2008 – Don M. Blumenthal

FTC "Protecting Personal Information"

- Business education pamphlet/video
- Breach response plan is one element
  - Have plan
  - Designate coordinator
  - Disconnect compromised computer from Internet
  - Know applicable laws and regulations
  - Know who should be notified, including consumers

© 2008 – Don M. Blumenthal

Response Elements

- Regulators will look for these items
  - Risk based plan, appropriate to size and complexity
  - Response that addressed nature and scope of incident, including what systems and data compromised
    - Even if no prior plan
  - Inform relevant law enforcement
  - Contained and controlled
  - Notified affected parties where appropriate

© 2008 – Don M. Blumenthal

To Keep Regulators Happy

- Be proactive
- Have a comprehensive enterprise security plan, including steps to respond to data compromise
- Read cases, regulations, guides, decisions, standards
- Distill and apply to your environment
- Must plan to prevent/mitigate data compromise but also to react well if it happens

© 2008 – Don M. Blumenthal

Enforcement Factors

- Representations
- Practices to protect and detect
- Reasonableness
- Demonstrable harm
- ***Reaction***

© 2008 – Don M. Blumenthal

State and Local Governments

- Far ahead in breach notification
- As of 04/08:
  - 39 dates
  - DC
  - New York City
  - Puerto Rico

© 2008 – Don M. Blumenthal

Usual State PII Definition

- First and last name OR last name and first initial - plus
  - Social Security Number OR
  - Drivers' License Number OR
  - State Identification Number OR
  - Debit or Credit Card Number OR +
  - Financial Account Number OR
  - Medical Information OR
  - Health Insurance Information
- Most state notification laws require PIN or access code be disclosed to include account numbers in definition

© 2008 – Don M. Blumenthal

Some Common Elements

- Personally identifiable information
- Exemptions if data encrypted
  - Check encryption definition
  - No exemption if PIN included
- Delay notice at LE request
- Financial data
  - A few cover medical also
- Allowable forms of notice
- Most have some exemption if company covered by federal law such as GLBA

© 2008 – Don M. Blumenthal

Coverage Issues to Check

- Triggers
  - Access; accessed and “used”
  - Disclosed
  - Likely/unliked to have been used
  - Harm likely/unlikely
  - Who makes determination
- Whether applies outside jurisdiction
- Provisions for third party data holders

© 2008 – Don M. Blumenthal

Notification Rules Vary

- How much delay is permissible
- Which state and local agencies to notify
- Credit reporting agencies
- May be thresholds that trigger requirements

© 2008 – Don M. Blumenthal

Potential Consequences Differ

- Penalties that can be levied by government
- Private rights of action

© 2008 – Don M. Blumenthal

Moving from Law to Reality

- Laws, regulations, and standards provide solid guidelines
- Real world fleshes out for specific enterprise and situations

© 2008 – Don M. Blumenthal

Breach Risk Management Necessities

- Management commitment to privacy and compliance with laws/regs/etc.
- Management commitment to maintain and fund enterprise security and privacy programs
- Cross-organizational structure with solid communications
- Targeted training
- Response plan

© 2008 – Don M. Blumenthal

Can't Be Done in Vacuum

- Breach response plan must be part of overall data security plan
- Coordinate with other information management systems
- Ensures comprehensive approach
- Helps make program more efficient and cost effective

© 2008 – Don M. Blumenthal

To Be Able to React to Loss

- Know where data is
- Know what's in data
- Know stakeholders
  - In and outside enterprise
- Know lines of authority and communication in enterprise
- Devise structure that allows all necessary stakeholders to coordinate

© 2008 – Don M. Blumenthal

Response Plan Elements

- Evidence preservation
- Internal crisis communications
- Customer and other notification; *e.g.*, employees and retirees
- Investor and employee communications

© 2008 – Don M. Blumenthal

If The Worst Happens

- Notify necessary individuals in organization
  - According to existing response plan, of course
- Include business, legal, tech, PR, and HR at minimum in response activities
- Notify law enforcement
  - Follow LE lead if requested
- Listen to your in-house subject matter experts
- Document every step of response

© 2008 – Don M. Blumenthal

Identify Loss

- Lost PII/SCI
- Form line of business teams if necessary
- Provide ongoing legal and business guidance to analysts
  - Elements of sensitive data under relevant statutes
  - Necessary combinations to invoke PII or SCI
- Don’t forget sensitive info that may not have regulatory ramifications; *e.g.*, trade secrets

© 2008 – Don M. Blumenthal

Engage Outside Counsel

- Unlikely that in-house staff will have sufficient expertise
- Vet your outside counsel choice
  - Don't automatically go with usual firm
  - Check qualifications of lawyers working the matter; "X was with the FTC" doesn't necessarily mean that "X has GLBA experience"
- Engage two organizations if necessary to have both security/privacy and litigation experience.
  - Make sure they work together

© 2008 – Don M. Blumenthal

Other Outside Help

- Forensics
  - May want to cross-check data analyses
  - Especially if loss involves hardware theft
- Crisis management company
  - Consider hiring organization with experience in handling public aspects
    - PR
    - Required notifications
- Assistance for individuals whose information was compromised

© 2008 – Don M. Blumenthal

Role of Counsel

- Lawyers should be lawyers
- Be careful about “good old boy/girl” network
  - Don’t necessarily have expertise to choose forensic or other specialists
- Ask who is doing data review for PII
  - Are lawyer hourly rates necessary

© 2008 – Don M. Blumenthal

Going Above and Beyond

- Do the right thing
- Public perception can be everything
- Data holders may expect notification and other protections even where not required
- Respond positively to press

© 2008 – Don M. Blumenthal

If Regulators Call

- Know what the laws require
  - Relevant security/privacy requirements
  - Notification statutes, regs, and guidelines
- Show respect
- Don’t play games

© 2008 – Don M. Blumenthal

Things to Watch - US

- Report of the President's Identify Theft Task Force
- Legislation; *e.g.* extension of GLBA to all entities and federal breach notification law
- Application of FISMA and regs to outside holders of federal government data
- Federal Agency Data Protection Act (HR 4791)
  - Feds must notify victims if data compromised
  - Passed House 06/03/08

© 2008 – Don M. Blumenthal

Things to Watch – Outside US

- Proposed EU breach notification for Privacy and Electronic Communication Directive
- Canadian Privacy Commissioner voluntary breach notification guidelines; linked to PIPEDA

© 2008 – Don M. Blumenthal

Questions Later?

Don M. Blumenthal
don@donblumenthal.com
(734) 997-0764
(202) 431-0874 (m)
www.donblumenthal.com

© 2008 – Don M. Blumenthal