ISOL 633 Legal regulations, investigation and compliance

Chapter 9 - Lesson 9
State Laws Protecting Citizen Information
and
Breach Notification Laws

Learning Objective

- Describe state legal compliance laws addressing public and private institutions.
- State regulation of privacy and information security
- State data breach notification
- State encryption regulations
- State data disposal regulations
- History of state privacy protection laws

CALIFORNIA NOTIFICATION LAW

- *California Database Security Breach Notification Act*
- *First breach notification law*
- *Enacted on July 1, 2003*
- *Purpose to give California residents timely information to protect themselves*
- *Serves as model for other states*

ChoicePoint Data Breach

- ChoicePoint was a data broker
- Databases contained public information and names, addresses, Social Security numbers, credit history, DNA information
- Breach in late 2004; disclosed in February 2005, notified California residents
- ChoicePoint data breach spurred creation of data breach notification laws in many states
- 35 states began looking at breach notification laws in 2005 alone

ChoicePoint Data Breach…Continued

- Second violation in 2008
- Changes in internal security controls led to additional breaches for which company was not alerted to unauthorized access to data
- Violations of the 2006 agreement

California Breach Notification

- Definition of Security Breach: Unauthorized acquisition of computerized data for which the confidentiality, security or integrity of the personal (unencrypted) information is compromised.
- Definition of "Personal Information" is very broad under the California law. It could include a person's name combined with SS#, Drivers' license number, Account number, credit or debit card number, medical or health information, email address combined with password or answer to security question.

CALIFORNIA NOTIFICATION LAW

Who Must Comply?				
State agencies	Nonprofit organizations	Private organizations	Business	Any entity storing info on California residents

California Breach Notification…continued

- Caveat - The law applied to businesses located outside the state of California, as long as the information they were storing was of a California resident.
- Trigger for notification:
  - When breach occurs
  - When company reasonably believes breach has occurred
- When to notify?
  - Asap
  - Exceptions: To determine scope of breach and to allow law enforcement to conduct criminal investigation

California Breach Notification

- Type of Notification Required (as the law was amended in 2011)
  - Written in plain language
  - Include name and address of entity making notice
  - List of information potentially compromised
  - Facts about the breach including but not limited to dates of breach
  - Contact information for major credit card reporting agencies
  - Notification to the Attorney General when the breach affects more than 500 customers for a single breach
- Exceptions to the written notice requirements

California Breach Notification

- What is the “safe harbor”?
  - Legal concept where a party can demonstrate that it took specific good faith actions to follow the law.
  - Properly encrypted data is a safe harbor when data breaches occur in spite in spite of encryption
- Private causes of action exist under California lBreach notice laws

DIFFERENCES IN DATA BREACH NOTIFICATION LAWS BETWEEN STATES

- *Activities that constitute a breach*
  - Arizona uses two-part test
  - Ohio –material risk of theft or fraud
- *Entities covered by the law*
  - Georgia –Applies to information brokers and exempts government agencies, applies to

DIFFERENCES IN DATA BREACH NOTIFICATION LAWS BETWEEN STATES…CONTINUED

- *Time for notifying residents*
  - California vague – Ohio – 45 days of discovery
- *Content of notice*
- *Minimum encryption requirements*
  - Undefined under California law. Compare to Indiana law
- *Civil and/or criminal penalties*
- *Private Causes of Action*
  - Allowed in California

Breach Notification and Federal Legislation

- No federal breach notification law exists today
- State laws differ in the area of breach notification
- Book's hypothetical question of "what happens with state laws if a federal breach notification law is passed?"

Data-Specific Security and Privacy Regulations

- Minnesota and Nevada
  - Require businesses to comply with Payment Card Industry standards
- Indiana
  - Limits SSN use and disclosure

Encryption Regulations

- Massachusetts
  - "Standards for the Protection of Personal Information of Residents of the Commonwealth"
  - Applies to data in paper and electronic form
  - Applies to any person that uses and stores personal information about a resident as a part of the sale of goods of services.
  - Requires the creation of an information security program similar to Gramm-Leach-Bliley
  - Requires encryption of personal information while stored on the entity's system
  - Unique and controversial by attempting to regulate business outside its state

Encryption Regulations

- Nevada
  - Standards-based Encryption
  - Data collectors must use encryption when transmitting personal information outside of their business network
  - Applies to data when stored and when transmitted
  - References and requires industry standards to be used for encryption – Federal Information Processing Standards issued by the NIST
  - Safe Harbor applies

Data Disposal Regulations

- Washington
  - Record – any material that holds information in either electronic or paper form
  - Destroy means changing it to a form that is no longer readable or decipherable. (examples, shredding, erasing, or modifying)
  - Health and financial data must be destroyed when no longer needed
  - Law applies to any person or entity in the state
  - Allows private causes of action
- New York
  - No person or business may dispose of a record containing "personal identifying information" without shredding, destroying, or modifying it
  - Record is any information held in any physical form, both paper and electronic

Thank you!

- Questions?

– Dr. Les Stovall

– Leslie.Stovall@ucumberlands.edu