PRESENTATION

The Matrix Reloaded: Cybersecurity and Data Protection for Employers

Zachary Busey & Bill O'Connor

Why talk about this now?

- Landscape is Changing
- Enforcement by Federal and State Government on the Rise
- Legislation on the Rise
- Costing Businesses More Money Than Ever
- Confusion in Marketplace – Who's Responsible?

Federal Legislation

- Consumer Privacy Bill of Rights Act of 2015
  - Intended to address personal data processing
  - Provide reasonable notice to individuals about a covered entity's privacy and security practices
  - Provide individuals with reasonable means to control the processing of personal data about them
  - Covered entity may only collect, retain, and use personal data in a manner that is reasonable in light of context
    - Must consider ways to minimize privacy risk when determining its personal data collection, retention, and use practices
    - Must delete, destroy, or de-identify personal data within a reasonable time

Federal Legislation

- Consumer Privacy Bill of Rights Act of 2015 (cont.)
  - Covered entity must conduct a privacy risk analysis if it processes personal data in a manner that is not reasonable in light of context
  - Covered entity must conduct a disparate impact analysis if it analyzes personal data in a manner that is not reasonable in light of context and such analysis results in adverse actions concerning multiple individuals
  - Identify reasonably foreseeable risks
  - Implement and maintain safeguards reasonably designed to ensure the security of personal data
  - Regular assessment, evaluation and adjustment of security safeguards

Federal Legislation

- Consumer Privacy Bill of Rights Act of 2015 (cont.)
  - Implement and maintain procedures to provide access to personal data, ensure accuracy of personal data, and correct or delete personal data
  - Enforcement by the Federal Trade Commission, State Attorneys General
  - Civil penalties up to $35,000 per day or $5,000 per affected consumer, with a maximum penalty of $25 million
    - No private right of action
  - Safe harbor – Enforceable Codes of Conduct
    - Must provide equivalent or greater protections for personal data
    - Must provide for periodic review of code of conduct

Federal Legislation

- Executive Order Promoting Private Sector Cybersecurity Information Sharing
  - Encourage the development of Information Sharing Organizations
  - Develop a common set of voluntary standards for information sharing organizations
    - will include privacy and civil liberty protections
  - Streamline private sector companies' ability to access classified cybersecurity threat information
  - Provide legal safe harbor for companies that share cyber threat information with the government or each other through a special Department of Homeland Security portal

Federal Legislation

- Executive Order Authorizing Sanctions Against Persons Engaged In Significant Malicious, Cyber-related Activities
  - Significant threats to the national security, foreign policy or economic health or financial stability of the United States
    - Critical infrastructure sectors, computers or computer networks, economic espionage
  - Includes persons who aid and abet such activities
  - Identified individuals or entities will be added to list of Specially Designated Nationals and Blocked Persons (SDN List)
    - U.S. assets are frozen
    - Prohibited from doing business with U.S. persons/entities
    - Cannot engage in dollar-denominated transactions (effectively cut off from the U.S. banking system)

Federal Legislation

- Data Security and Breach Notification Act of 2015
  - Companies must implement and maintain reasonable security measures and practices to protect and secure personal information
  - Broader definition of “personal information” than most state data breach laws
  - Only required to provide notice if there is a reasonable risk of identity theft, economic loss, economic harm, or financial harm
  - Must provide notice to affected individuals within 30 days after discovery of a breach
  - Preempt all state data breach notification laws
  - Enforcement by the FTC or state attorneys general (no private right of action)

State Legislation

- Tennessee (T.C.A § 47-18-2107)
  - Application - Any person or business that conducts business in TN, or any agency of TN or any of its political subdivisions (collectively "Entity"), that owns or licenses computerized data that includes personal information ("PI")
  - Security Breach Definition - Unauthorized acquisition of unencrypted computerized data that materially compromises the security, confidentiality, or integrity of PI maintained by the Entity
  - Notification Obligation – Must disclose to any resident of TN whose unencrypted PI was, or is reasonably believed to have been, acquired by an unauthorized person

State Legislation

- Tennessee (T.C.A § 47-18-2107) (cont.)
  - Notification to Consumer Reporting Agencies - If required to notify more than 1,000 persons at one time, must also notify all consumer reporting agencies and credit bureaus that compile and maintain files on consumers on a nationwide basis of the timing, distribution and content of the notices
  - Third-Party Data Notification - Any Entity that maintains computerized data that includes PI that the Entity does not own must notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the PI was, or is reasonably believed to have been, acquired by an unauthorized person

State Legislation

- Tennessee (T.C.A § 47-18-2107) (cont.)
  - Timing of Notification – Must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system
  - Personal Information Definition - An individual's first name or first initial and last name, in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:
    - Social Security Number;
    - Driver license number; or

State Legislation

- Tennessee (T.C.A § 47-18-2107) (cont.)
  - Account number or credit card number or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account
  - PI does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records
  - Substitute Notice Available – If the cost of providing notice exceeds $250,000, or if the number of persons to be notified exceeds 500,000, or the Entity does not have sufficient contact information,
    - Substitute notice must consist of all of the following:

State Legislation

- Tennessee (T.C.A § 47-18-2107) (cont.)
  - Email notice when the Entity has an email address for the subject persons;
  - Conspicuous posting of the notice on the Entity's Web site if the Entity maintains one; and
  - Notification to major statewide media
  - – <u>Exceptions</u>
    - An Entity may follow the procedures in its own notification policy if it is consistent with the timing requirements of the statute
    - The provisions of this statute do not apply to any Entity that is subject to the provisions of Title V of the Gramm-Leach-Bliley Act

State Legislation

- Massachusetts
  - Data Breach Notification
    - Applies to any entity maintaining information on MA residents
    - Must notify state Attorney General, the Office of Consumer Affairs and Business Regulation, and the MA resident
    - Specific provisions for cooperation with third party owners of data
    - Specifies information requirements for notice to Attorney General and to MA residents

State Legislation

- Massachusetts
  - Data Security Regulation (Mass. Regs. Code tit. 201 § 17.00)
    - Stringent and detailed data security requirements
    - Applies to any person (legal entity or natural person), wherever located, that owns or licenses personal information about a MA resident
      - Includes any organization that receives, stores, maintains, processes or otherwise has access to personal information either for the provision of goods or services or employment

State Legislation

- Massachusetts
  - Data Security Regulation (cont.)
    - Must develop, implement and maintain a comprehensive written information security program ("WISP") that contains administrative, technical and physical safeguards that are appropriate to the size, scope and type of the person's business, the person's available resources, the amount of stored data, and the need for security and confidentiality of both consumer and employee information
    - Specific WISP requirements
    - Computer system security requirements for organizations that electronically store or transmit personal information
    - `

Recent Cases / Breach Notifications

- Amedisys, Inc.
  - Loss of 142 laptop computers containing medical information on approximately 6,900 patients
  - Notified federal and state agencies, as well as affected individuals
  - No evidence of hacking, fraud or identity theft
  - Notifications sent “out of an abundance of caution”
  - Missing laptops were used by employees who left the company between 2011 and 2014
  - Missing laptops equipped with 256-bit disk encryption, administrator restrictions and additional security measures designed to protect the patient data
  - Not a data breach, but can’t be certain of low risk of breach

Recent Cases / Breach Notifications

- Marriott International, Inc. (FCC Enforcement Advisory No. 2015-01)
  - Marriott was blocking personal Wi-Fi hot spots in their hotels
    - Deployed a Wi-Fi deauthentication protocol
    - Resulted in a Consent Decree ($600,000 civil penalty)
  - Willful or malicious interference with Wi-Fi hot spots is illegal
  - Violates Section 333 of the Communications Act
  - What is prohibited?
    - No hotel, convention center, or other commercial establishment or the network operator providing services at such establishments may intentionally block or disrupt personal Wi-Fi hot spots on such premises, including as part of an effort to force consumers to purchase access to the property owner's Wi-Fi network

Recent Cases / Breach Notifications

- Marriott International, Inc. (cont.)
  - Many network devices implement a Wi-Fi deauthentication protocol as a security feature
    - Block unknown wireless network devices from gaining access to the network
    - If this feature is enabled, depending on the circumstances, an argument can be made that the FCC advisory may apply

Recent Cases / Breach Notifications

- Tierney et al. v. Advocate Health and Hospitals Corp. (Seventh Circuit, Case No. 14-3168)
  - Seventh Circuit asked to revive a proposed class action accusing Advocate Health and Hospitals Corp. of violating the Fair Credit Reporting Act by failing to safeguard health data stolen from its offices
  - Alleged that the hospital's inability to adopt, implement or maintain adequate procedures to protect their personal and medical data led to the dissemination of the information for purposes that are not permissible under the FCRA
  - Lower court threw out the FCRA claims, ruling that the hospital can’t be considered a “credit reporting agency” under the FCRA

Recent Cases / Breach Notifications

- Tierney et al. v. Advocate Health and Hospitals Corp. (cont.)
  - Consumer Reporting Agency
    - Assemble credit information for a fee
    - Provide reports to third parties
  - Advocate uses the information to secure payment from insurance companies
  - Why the FCRA?
    - Penalties – range from $100 to $1,000 per willful violation

Insider Threat Detection

- Using big data analytics and software to identify potential insider threats in the workplace
- High risk, high reward
- Rewards
  - Preventing fraud, intellectual property theft and workplace violence
- Risks
  - Data is discoverable in litigation
  - Discrimination claims against employer
- Best Practices
  - Transparency
  - Clearly stated policies that are consistently enforced

Insider Threat Detection

- Best Practices (cont.)
  - Systematic logging, monitoring and auditing of employee network activity
  - Blocking unauthorized emailing or uploading of company data outside the company network
  - Comprehensive employee termination procedures

Website Privacy Notices

- Google Analytics
  - Implicates behavioral tracking and/or collection of personally identifiable information (depending upon settings)
  - If used, include link to how Google uses the data it collects (https://www.google.com/policies/privacy/partners/)
- Behavioral Tracking
  - Collecting information about users' online behavior and using this information to serve ads aimed to be relevant to particular users
  - Include disclosures about behavioral advertising, with links to information about how to opt out of various providers' behavioral advertising
- Do Not Track Technology
  - Allows web browsers, browser add-ons, etc. to request that a web application disable its tracking of an individual user

Website Privacy Notices

- California
  - California Online Privacy Protection Act (CalOPPA) (amendments effective January 1, 2014)
    - Website operators must disclose how they respond to web browser “do not track” signals or to similar technologies that provide users with an ability to exercise choice regarding tracking
    - Must disclose whether third parties conduct tracking of personally identifiable information on the website

Website Privacy Notices

- California
  - Shine the Light Act
    - Gives consumers the right to obtain an accounting of how, and to whom, their personal information has been disclosed for direct marketing purposes during the past year
    - Add a section or link that describes this right and provide contact information for obtaining an accounting
    - Alternative to providing an accounting
      - Published policy that you will obtain opt-in consent before sharing personal information or provide a cost-free method to opt-out
      - Comply with Gramm-Leach Bliley Act disclosure requirements (if applicable)

Website Privacy Notices

- California
  - Privacy Rights for California Minors in the Digital World (Effective January 1, 2015)
    - Prevents operators of websites, online services or mobile apps directed to minors from marketing and advertising of certain products and services to minors residing in California
    - Prevents operator from disclosing personal information about a minor if the purpose is for marketing or advertising such products

Website Privacy Notices

- California
  - Privacy Rights for California Minors in the Digital World (cont.)
    - Operators of websites (including online services and mobile apps) that have actual knowledge that a minor is using its website must permit the minor to remove, or request and obtain removal of, content posted on the website by the minor
      - Must provide notice of this right to minors
      - Must provide clear instructions on how to remove, or request removal of, posted content
      - Must provide notice that removal of posted content does not ensure complete or comprehensive removal of such content

Top 10 for Employers

1. Wearable Tech
2. Data Access Points
3. BYOD
4. Telecommuting
5. CFAA Section 1030
6. Passwords
7. Discipline Policies
8. Data Retention
9. Updated Training
10. Data Mining/Analytics

PRESENTATION

The Matrix Reloaded: Cybersecurity and Data Protection for Employers

Zachary Busey & Bill O'Connor