Locke Lord LLP

Defining Reasonable Security

March2 3, 2015

Thomas J. Smedinghoff
Locke Lord LLP

Atlanta | Austin | Boston | Chicago | Dallas | Hartford | Hong Kong | Houston | Istanbul | London | Los Angeles | Miami | Morristown | New Orleans
New York | Orange County | Providence | Sacramento | San Francisco | Stamford | Tokyo | Washington DC | West Palm Beach

The World Is Rapidly Changing

- In the past, when Jesse James or Butch Cassidy robbed a bank or a train, and stole cash and valuables, we –
  - **Felt sorry for the business** what was victimized, and
  - Hunted down the bad guys (and even made movies about it!)
- Today, when a business is robbed of valuable digital data, we --
  - **Blame the business** for failing to provide adequate security!
  - File lawsuits against the business and its directors, and
  - Initiate government enforcement actions against the business
- And in the process, we have made data security a legal obligation that applies to all companies

These Obligations Come From An Ever-Expanding Patchwork of -

- Statutes and regulations -
  - Data security laws and regulations (e.g., state security laws)
  - Privacy laws (virtually every country)
  - E-transaction laws
  - Corporate governance legislation and regulations (e.g. SOX)
  - Unfair business practice laws and enforcement trends
  - Sector-specific regulations, such as HIPAA, GLB, SEC, COPPA
- Common Law Obligations (i.e., court rulings)
- Rules of Evidence
- Contractual Obligations
- Industry Self-Regulation (e.g., PCI)
- Self-Imposed Obligations

The Basic Legal Standard – "Reasonable Security"

- Must implement "**appropriate**" measures to protect data
  - E.g., GLB, HIPAA, several state data security laws, numerous country privacy laws
- Must implement "**reasonable**" measures to protect data
  - E.g., several state data security laws, numerous country privacy laws
  - E.g., California - "A business that owns, licenses, or maintains personal information about a California resident **shall implement and maintain reasonable security** procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." Cal. Civ. Code § 1798.81.5(b).
- The law views security as a **relative concept!**

But What Is "Reasonable" Security?

- Two leading approaches --
  - Comprehensive written information security program (**WISP**)
    - GLB security regulations (Fed, OTC, FDIC, OCC) – 2001
    - GLB security regulations (FTC) – 2002
    - FISMA (gov't agencies) – 2002
    - HIPAA security regulations (HHS) – 2003
    - FTC enforcement actions – 2002–present
    - Oregon (as a safe harbor) – 2007
    - Massachusetts regulations – 2008
    - AG enforcement actions and developing case law
    - International - EU Data Protection Directive, Argentina, Austria, Iceland, Italy, Netherlands, Norway, Philippines, Poland, Portugal, Spain, and others
  - NIST Cybersecurity Framework
    - Voluntary framework released by NIST February 12, 2014
    - Based on consensus of public-private collaboration
    - May ultimately become a *de facto* legal standard

The Reasonable Security Legal Standard

- Can be summarized in two words -
  - Risk-based “Process”
  - Responsive “Controls”

The Legal Process - Overview

- Identify the information assets to be protected
  - Both (i) under company control and (ii) outsourced
- Conduct risk assessment
  - Identify and evaluate threats, vulnerabilities, and damages
  - Consider available options
- Select and implement appropriate security controls
  - That are responsive to the risk assessment
  - That address the required “categories” of security measures

The Legal Process – Overview cont.

- Regularly monitor and test the controls
  - To ensure they are effective
- Continually review, reassess, and adjust the program
  - To address new threats, vulnerabilities, and available options
- Address third parties
  - Outsource providers / cloud providers
  - Third parties with access

Select and Implement Appropriate Security Controls

- Physical controls (*to protect and restrict access to* -)
  - Facility and equipment
  - Media
- Technical controls
  - Access controls
  - Identification and authentication
  - System configuration and change management
  - System and data integrity
  - Data communications protection
  - System maintenance
  - System activity and intrusion detection monitoring
  - Data destruction
- Administrative Controls
  - Personnel security
  - Employee awareness and training
  - Backup and disaster planning
  - Incident response planning
  - Audits

Factors to Consider in Selecting Security Controls in Each Category

- Probability and criticality of potential risks (i.e., risk assessment results)
- Burden of implementing adequate precautions
- Company's size, complexity, and capabilities
- Nature and scope of company's activities
- Sensitivity of information to be protected
- Company's technical infrastructure, hardware, and software security capabilities
- State of the art re security measures
- Cost of the security measures