



EVERYTHING MATTERS

**Information Governance – The Next  
Wave Of Good Corporate Governance:  
*What The Office Of General Counsel  
Should Know About Managing The Risk  
Of The Corporation's Information Assets***

**Vinny Sanchez**

**Partner and Chair, Technology and Sourcing Practice,  
DLA Piper**

**PWC General Counsel Forum  
March 20-21, 2008**

# Overview

EVERYTHING MATTERS

- Fact or Fiction
- Why Should We Care?
- Expanding Legal Duty to Provide Security
- Framework for Legal Claims
- Comprehensive Compliance Program
- Contracting Approach
- Legal Battle Plans

# Fact or Fiction

EVERYTHING MATTERS

- No fiduciary duty to protect data of a company
- Corporate governance is for public companies and Sarbox
- Information security is just an IT issue
- My auditor says we are Sarbox compliant so we're fine
- We are not public and we don't fall under HIPAA or GLB – so no worries
- We have a CIO and a CPO – we're covered
- Not a Board issue
- To the extent it is a Board issue, Board's audit committee takes care of this

# Why Should We Care?

EVERYTHING MATTERS

- It's a Daily Headline Issue – Reputational Risk
- Hacking attempts and successes are increasing
- Lack of uniform security standards
- Lack of “sufficient” corporate standards and policies governing security despite promises or representations to the contrary
- Vulnerability of critical infrastructure and software
- Increasing # of Regulations/Legislation
  - Alphabet soup of regulations and impractical legislative solutions
  - 42 state notification laws; 17 FTC orders

# Expanding Legal Duty

EVERYTHING MATTERS

- Legal Framework Requiring Security
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Gramm-Leach-Bliley Act of 1999 (“GLBA”)
  - FTC Safeguards Rule
  - FTC Disposal Rule
- Sarbanes-Oxley Act of 2002
- USA Patriot Act
- E-SIGN and UETA
- Basel Committee

# Expanding Legal Duty

EVERYTHING MATTERS

- FTC Enforcement Actions
- State Statutes
- Common Law to Provide Security
- Encryption of Social Security Numbers
- Destroying Data in a Secure Manner
- Admissibility of Electronic Business Records

# Expanding Legal Duty - Payment Card Industry Data Security Standard

EVERYTHING MATTERS

- Build and Maintain a Secure Network
- Protect Cardholder Data
- Maintain a Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor and Test Network
- Maintain an Information Security Policy

# Expanding Legal Duty - FTC Consent Orders

EVERYTHING MATTERS

- Must establish and maintain a “comprehensive information security program”.
- Containing “administrative, technical and physical safeguards appropriate to the respondents’ size and complexity, the nature and scope of respondents’ activities and the sensitivity of the personal information collected from or about consumers”.
- Adequate security means that companies maintain effective security that is commensurate with risk.

# Framework for Legal Claims

EVERYTHING MATTERS

- FTC and State Actions/Consent Decrees
  - Deceptive and Unfair Practices – Far Reaching
- Tort Claims (duty per state statute; fraud; neg. misrep., unfair practices, etc.)
- Breach of Contract Claims
- Shareholder Derivative Suits – Did you misrepresent in your SEC filings?
- Violation of Fed/State Licenses/Certifications

# Framework for Legal Claims - Insufficient Practices

EVERYTHING MATTERS

- Inadequate Risk Assessments
- Failure to Encrypt in Storage and Transmission
- Failure to Implement Detection Measures and Response Plans
- Failure to Provide Audit and Monitoring Procedures
- Failure to Oversee and Manage Contractors
- Failure to Install Firewalls
- Failure to Use Virus Detection Software
- Failure to Provide Access Controls

# Comprehensive Compliance Program – Board Responsibilities

EVERYTHING MATTERS

- Board has a duty of care to secure the company's assets
- Board Responsibilities
  - Approve the company's written information security program
  - Oversee the development, implementation and maintenance of the program
  - Review reports from management
- Board committee – Technology and Information Governance ?

# Comprehensive Compliance Program – Board Responsibilities

EVERYTHING MATTERS

- ***NYSE Euronext***

“The Technology Committee is appointed by the Board and charged with assisting the Board in: (i) reviewing technology developments and strategic opportunities, (ii) providing guidance in the prioritization and implementation of technology initiatives, and (iii) *reviewing system security and contingency measures.*”

- ***Eli Lilly – Science and Technology Committee***

“Assist the board with its oversight responsibility for enterprise risk management in areas affecting the company's research and development.

# Comprehensive Compliance Program – Board Responsibilities

EVERYTHING MATTERS

- ***Fannie Mae***

“The function of the Technology and Operations committee is to provide oversight of the corporation's technology and operations environment.”

- ***Freddie Mac***

“The Mission, Sourcing and Technology Committee's primary functions are . . . To review the management of risks associated with the mortgage purchase activities; To review the implementation of OFHEO's Mortgage Fraud Policy Guidance; To review enterprise-wide technology . . .

# Comprehensive Compliance Program – Board Responsibilities

EVERYTHING MATTERS

- ***Bank of New York Mellon***

“The purpose of the Risk Committee (the "Committee") is to assist the Board of Directors in fulfilling its oversight responsibilities with regard to (a) the risks inherent in the business of the Corporation and the control processes with respect to such risks, (b) the assessment and review of credit, market, fiduciary, liquidity, reputational, operational, fraud, strategic, technology, **data-security** and business-continuity risks, (c) the risk management activities of the Corporation and its subsidiaries, and (d) fiduciary activities of the Corporation's subsidiaries. .”

# Comprehensive Compliance Program - Management

EVERYTHING MATTERS

- Management
  - Evaluate impact on company's security program of changing business arrangements and changes to information systems
  - Document compliance with company's security program
  - Keep Board informed as to overall status of security program
  
- Holding Company Structures

# Comprehensive Compliance Program - Management

EVERYTHING MATTERS

## Information Governance Committee – who?

- CIO
- Legal/Compliance
- Finance
- HR
- Risk Management
- Contract/Vendor Management
- Business Unit Owners – But Who to Invite?

# Comprehensive Compliance Program – What is Covered?

EVERYTHING MATTERS

- What are we protecting?
  - Customer information
  - Employee information
  - Competitive Business Information
  - Financial Information
  - Third Party Information
- Physical vs Digital
- Conventional vs Electronic Breaches

# Comprehensive Compliance Program – Components of Program

EVERYTHING MATTERS

- The comprehensive program
  - information security policy (covers various aspects including how to deal with breaches of information)
  - use of information assets/resources
  - record retention policy
  - employee policies/handbook to the extent they address confidentiality
  - disaster recovery/business continuity plans
  - outsourcing

# Comprehensive Compliance Program – Components of Program

EVERYTHING MATTERS

- Risk Assessments
- Due Diligence
- Continuous Monitoring, Detection, Adjustment and Updating
- Incident Response Plans and Documentation
- Training
- Oversee Service Providers (Outsourcing)
- Special Considerations for Franchise Systems

# Contracting Approach

EVERYTHING MATTERS

- Approach is evolving
- Reasonable standard vs. strict liability
- Scope of employment vs. mere possession
- Detection/penetration testing

# Contracting Approach

EVERYTHING MATTERS

- Incident response obligations
  - Who notifies - independent vs. coordinated response
  - Managing different views on obligations
  - Indemnification
  - Remediation costs
  - Have you built the contractual obligations into your overall incident response plan?

# Legal Battle Plans

EVERYTHING MATTERS

- Board Education and Oversight
- Management Education, Oversight and Implementation
- Comprehensive Plan Approved by Legal
- Incident Response Plans
- Multilayer Defense – Legal Component
- Defenses and Counterattacks
- Flexible and Adaptable
- Maintain Public Trust
- Test Legal Battle Plans

# Questions

EVERYTHING MATTERS



# Contact Information

EVERYTHING MATTERS

- If you have any questions, please contact us at:

Vincent A. Sanchez

Chair, Technology and Sourcing Group

DLA Piper US LLP

203 N. LaSalle Suite 1900

Chicago, Illinois 60601

312-368-4000

[vincent.sanchez@dlapiper.com](mailto:vincent.sanchez@dlapiper.com)

