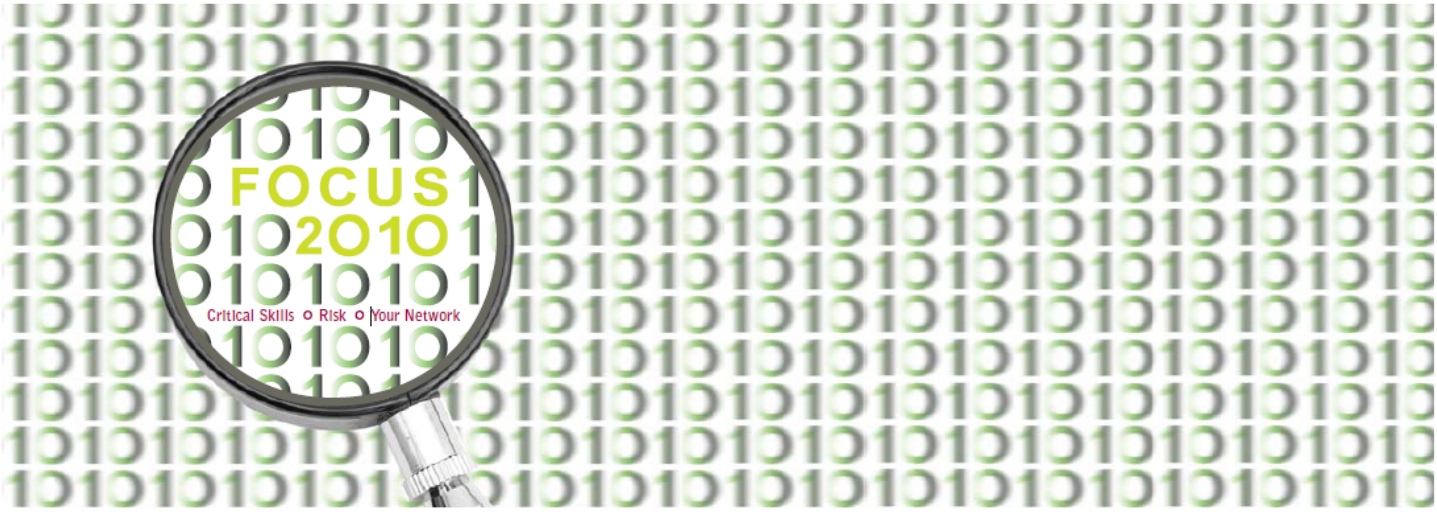
10th Annual SF ISACA Fall Conference

October 4 – 6, 2010



G12: Putting Teeth Into Your Privacy Compliance Program

Ann Geyer, Tunitas Group

ISACA®

Trust in, and value from, information systems

San Francisco Chapter

ISACA
Trust in, and value from, information systems
San Francisco Chapter

Information Security—the New Corporate Governance Requirement

-- Putting Teeth Into Your Privacy Compliance Program

Ann Geyer, Esq.
Tunitas Group

Key Points

- Infosec challenges are not solved by relegating them to regulators or CIOs
- Strengthening security means
  - Including it under corporate governance
  - Resisting boilerplate security
  - Insisting security be aligned with the business requirements
  - Keeping the focus on risk management, reporting and accountability
- Corporate and personal liability starting to drive security governance

ISACA
San Francisco Chapter

Governance

- Corporate Directors
  - Duty to oversee the enterprise
  - Legally required to authorize extraordinary business decisions
  - Not personally liable if use “reasonably prudent business judgment”

Duties of Directors

- Duty of Care
  - Violated by acts of gross negligence
- Duty of Loyalty
  - Violated by acts that go against the organization’s best interests
- Duty of Good Faith (subset of Loyalty)
  - Violated by acts in conscious disregard of the director’s duties to the organization
- Directors incur personal liability for breaching these duties
  - Be informed
  - Avoid conflicts of interest
  - Make prudent decision
  - Apply oversight

Director Liability Cases Relevant to InfoSec

- Graham v. Allis-Chalmers Mfg Co. (1963)
- In re Caremark Int'l Deriv. Litigation (1996)
- In re Walt Disney Co. Deriv. Litigation (2006)
- Stone v. Ritter (2006)

Graham v. Allis-Chalmers Mfg Co.

- Claim
  - Failure to prevent violations of federal antitrust law
  - Directors *should have known* of the violations
- Suit dismissed
  - No duty of directors to "ferret out wrongdoing" if there is no reason to suspect

In re Caremark

- Stockholder suit against directors
- Court held
  - Directors *should have known* Caremark personnel were violating the federal Law
  - Directors allowed a "situation to develop" that led to the violations
  - Directors violated a duty to be "active monitors" of corporate performance
    - Must ensure that information and reporting systems exist
    - Must provide timely, accurate information to reach informed judgments re the organization's compliance with law.
- Failure to act in good faith is a NEC condition for imposing "oversight" liability.

In re Walt Disney

- Further clarified the Caremark standard for "oversight" liability
- To show a director failed to act in **Good Faith**
  - "acts with the intent to violate an applicable law"
  - "intentionally fails to act when duty to act is known, evidencing a conscious disregard"

Take Away Message From These Cases

- If red flags exist,
  Directors must provide appropriate oversight and see that the org takes action
- Directors must have a means
  to reasonably know if red flags exist
- Failing knowledge of red flags,
  directors are not liable for bad outcomes

Director Liability

- Personal liability if found at fault
- May not qualify for indemnification
- May be covered under D& O insurance
- Nonetheless—not a situation any director wants to be in

Governance of Information Security

- Align security program to corporate strategy
- Assess risk }
- Allocate resources } Duty to Monitor
- Measure performance }
- Unified security program based on above considerations

Stone v. Ritter

- Duty to Monitor
  - Director duty includes **Risk and Compliance Oversight**: Directors should assess whether the corporation has established and implemented programs to address:
  - **Risk Management**: The board or a committee receives reports on programs to protect assets and reputation of the corporation. Typical risk management programs include information security, crisis management, plant security, compliance, IP protection
  - **Compliance** with laws and regulations: Oversee management responsibilities, review written policies, establish audit committee, monitor programs for effectiveness

Shames-Yeakel v. Citizens Financial Bank

- Plaintiff Claim
  - Bank failed to implement security protections
  - Bank has a common law duty to prevent identify theft of customer accounts (negligence)
- Court held

  "If the duty not to disclose customer information is to have any weight in the age of online banking, then banks must certainly employ sufficient security measures to protect their customers' online accounts."

Shames-Yeakel v. Citizens Financial Bank

- Bank argued it had good security
  - Used a reputable service firm
  - Required account authorization and authentication (passwords)
  - Restricted access to need-to-know employees
- Plaintiffs argued security not "state of art"
  - Industry report claims single factor not adequate; recommended multi-factor
- Take-away
  - Failure to expeditiously implement state-of-the art security procedures can constitute a breach of the standard of care

Re-enforces the Role of Governance

- Provide oversight
- Ensure processes, controls,
- Have a report back mechanism
- Understand and react appropriately

Recent Emphasis on Director & Executives

- Corporate wrongdoing by high-level actors at large publicly held organizations went undetected
- Increased attention on
  - Organizational culture
  - Improved internal reporting
  - Adequate training
  - Auditing and monitoring
  - Periodic risk assessments

Federal Sentencing Guidelines for Org Defendants

- Sentences can be mitigated if 7 elements are satisfied
  - Designated Director/Office to oversee compliance
  - Restricted delegation
  - Org S&P to reduce the prospect of wrongdoing
  - Standards and procedures known through org
  - Monitoring, auditing, & reporting system
  - Consistent enforcement including sanctions
  - Appropriate response to wrongdoing with emphasis on preventive measures
- And by self-reporting, cooperation, and acceptance of responsibility

Fraud and Gross Negligence

- Most common charges against org under federal law
- Often the result of manipulating information, gross inattention to security, or willful violation of law
  - Insider trading
  - Unreliable or misleading financial records
  - Failure to get informed consent
  - Failure to apply security protections
- Penalties worst
  - Intentional misconduct, repeated misconduct, obstructing investigations

Other Mitigating Factors

- Severity and extent of the underlying misconduct
- Provider's existing compliance infrastructure and supporting resources
- Ability to identify and respond to potential misconduct

Summary

- Courts getting educated about security related harm
- Expectations for corporate oversight (duty to monitor) rising
- Federal sentencing guidelines are more lenient where governance and compliance programs are well established and integrated throughout the org
- Governance and compliance principles mirror basic security practices
  - Alignment
  - Risk Assessment
  - Monitoring
  - Executive reporting

Questions

- Contact:
  - Ann Geyer
  - www.tunitas.com