

# Cybersecurity Law



Andrew Vollmar, Esq.  
Shawn Waldman

# Introduction

- Liability of business owners and C-level execs. resulting from cyber incidents is on the rise.
  - Includes non-profits
- Various U.S. companies reported over \$40 billion in losses from unauthorized use of computers in 2014 (Experian second annual report, 2015)
  - Primary cause: Employees
- In the latest study by the Ponemon Institute and IBM , the average total cost of a data breach for participating companies is \$3.79 million. (350 companies in 11 countries)
  - Healthcare industry breaches growing rapidly and are among the most costly of all breaches
- Small businesses particularly at risk.
  - Lack of resources
  - Owners believe hackers would not target their business

# Model ABA Rule 1.1(8)

- To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes... with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.

# ABA Model Rule 1.6(c)

- “[M]ake reasonable efforts to prevent the inadvertent disclosure of, or unauthorized access to, information relating to the representation of a client.”



# Factors to be Considered

- Sensitivity of information
- Likelihood of disclosure without safeguards
- Cost of Safeguards
- Cost of Employing Safeguards
- Do safeguards adversely affect lawyer's ability to represent other clients

# ABA Rule 1.6, Comment 18

- A client may require lawyer to implement additional safeguards not required by the rule
- The client may give informed consent to forego additional safety measures required by this rule.

# Cybersecurity Risks

- Phishing
- SPAM
- Cyber extortion/ransomware
- Data breaches
- Inadequate security measures  
(passwords, encryption, back-ups, etc.)
- Poorly trained employees

# Liability

- **Private consumer actions**
  - Negligence: failing to adhere to latest industry standards to safeguard private consumer data
  - Breach of contract
- **Government regulation**
  - Steep fines—FTCA, HIPPA, GLBA
  - FCC, FTC, State attorneys general
    - E.g., Wyndham (Third Circuit decision permits FTC regulation of “unfair or deceptive business practices.”)
    - Violation of notification laws
- **Derivative suits**
  - D & O liability



# Liability Example

- *FTC v. Wyndham Worldwide Corp.*, 10 F.Supp3d 602.
- FTC brought suit for “unfair trade practices”
- Wyndham argued cyber legislation indicated Congress’ intent to limit the FTC’s authority.

# FTC Guidelines for Cyber Defense

- Assess the security in place
- Minimize the data collected and retained
- Testing and retesting cyber security



# Guidelines (Continued)

- Training personnel on best practices
- Retain competent service providers
- Employ a “defense in depth” system
- Implement access control

# What do we do now ?



# Risk Assessment

- Identify vulnerabilities in current security infrastructure.
  - Encryption of private data
  - Data storage techniques
  - Policies and procedures
  - Basic measures—password updates, antivirus
  - Third-party vendors
  - Cloud computing

# Policies and Procedures

- Employee training
  - Employees are the primary facilitators of data breaches
- BYOD
  - Must have policy to regulate use
- Third-party vendors
  - Review all contracts
  - Safeguard provisions
  - Assessment and audit structure
- Cyber Insurance
  - First and third-party coverage
  - Extortion/ransomware
  - Determine need for supplemental coverage (D&O)

# Response Plan

- Plan to promptly and fluidly respond to a data breach.
  - Manage and coordinate company's response team
  - Act as an intermediary between C-levels and team members
  - Identify key tasks (notification), manage timelines, and documented response efforts.
  - Assess scope of breach
  - Team member readiness
  - Practice, practice, practice
  - Constant review and update

# Response Team

- Executive leaders (CISOs)
- In-house IT and security personnel
- Legal
- External relations/PR
- Customer care specialists
- Law enforcement



# Thank you



Andrew Vollmar, Esq.

[avollmar@ffalaw.com](mailto:avollmar@ffalaw.com)

(937) 913-0173



Shawn Waldman

[Shawn.Waldman@securecyberdefense.com](mailto:Shawn.Waldman@securecyberdefense.com)

(937) 802-7521