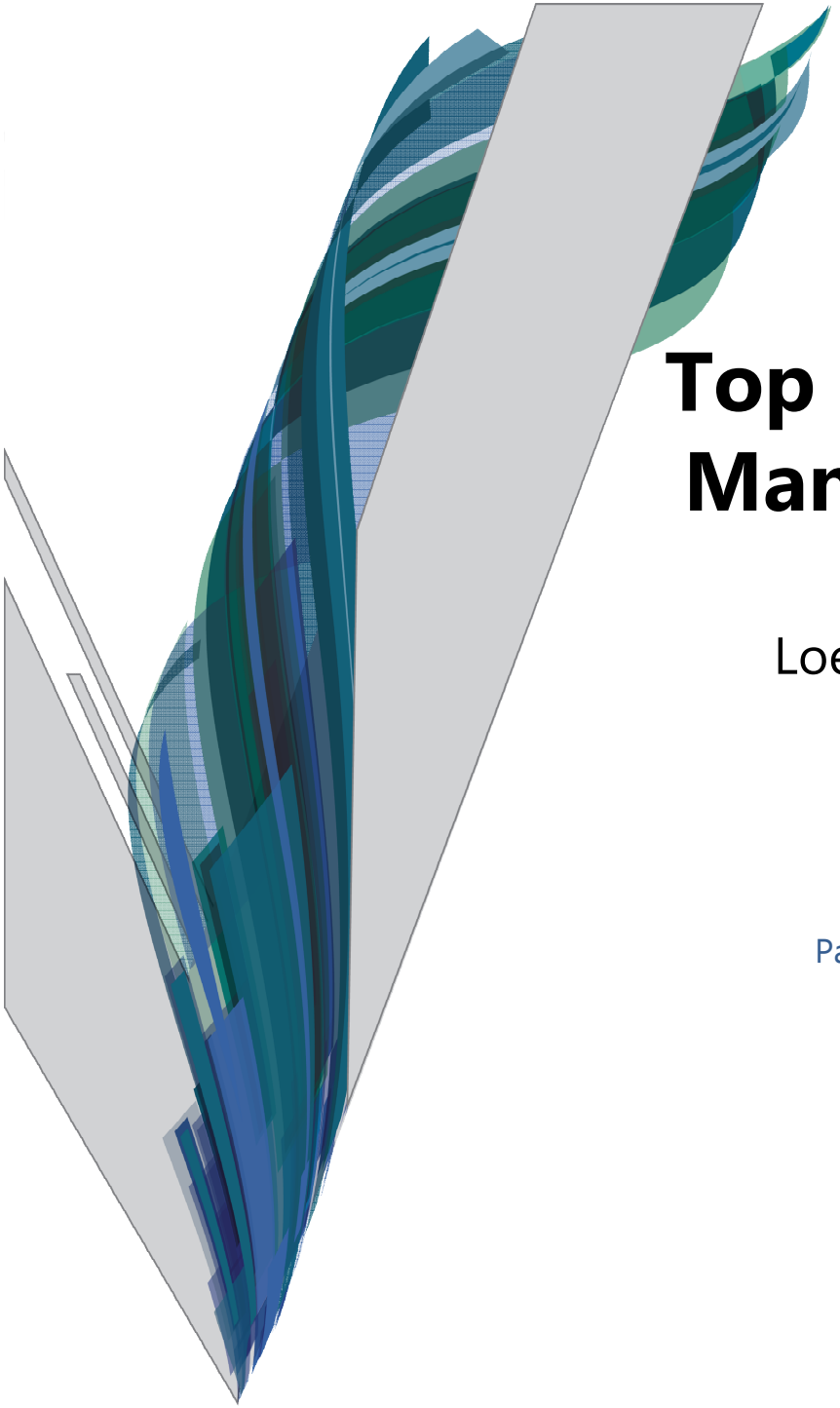


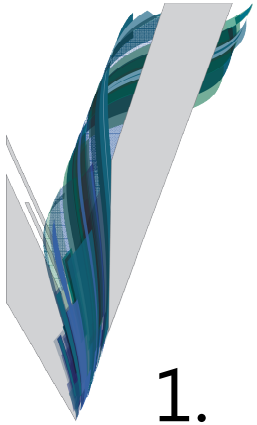
VENABLE

Top Five Cybersecurity Tips: Managing Your Legal Risks

Legal Council Meeting
Loews Madison Hotel, Washington, DC

July 17, 2017
4:00 PM ET

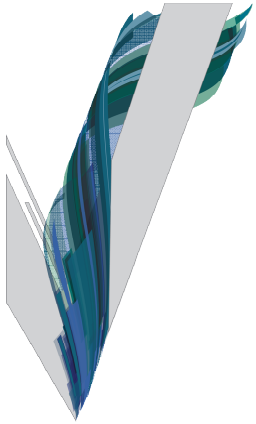
Julia Kernochan Tama, Esq.
Partner, Privacy and Data Security Practice, Venable LLP



Cybersecurity Tips for Lawyers

1. Know the Legal Rules
2. Assess Your Risks
3. Know Your Vendors
4. Prepare for the Worst
5. Stay Up-to-Date

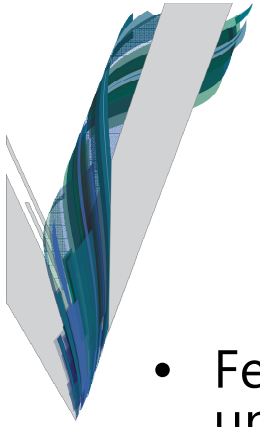
VENABLE



Cybersecurity and Data Security

- Cybersecurity and data security are related concepts
- Cybersecurity focuses on protecting networks and infrastructure from attacks and bad actors and can include personal information
  - Networks, communications backbone, financial systems, etc.
- Data security focuses on securing personal information (*e.g.*, names, payment card numbers, Social Security numbers, etc.) from being accessed and/or acquired by unauthorized individuals
  - Consumer data breaches, lost laptops, etc.
- Different agencies and laws regulate different types of incidents, often with overlapping interests

VENABLE



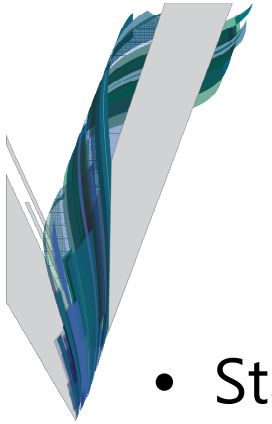
1. Know the Legal Rules

- Federal Trade Commission (FTC) enforces federal law prohibiting unfair or deceptive acts or practices. The FTC interprets the law to require reasonable security for personal information.

- Practices that the FTC has identified as factors in reasonable security:

  - Minimizing the collection of personal information;
  - Failure to implement and enforce appropriate password policies;
  - Failure to use encryption to protect consumer information in storage and in transit;
  - Failure to perform due diligence of and oversight of service providers' cybersecurity practices;
  - Failure to provide employees with adequate cybersecurity training;
  - Failure to implement policies and procedures to detect and respond to a breach.

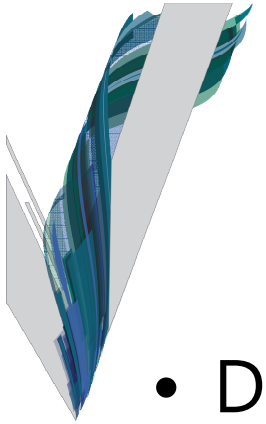
VENABLE



1. Know the Legal Rules

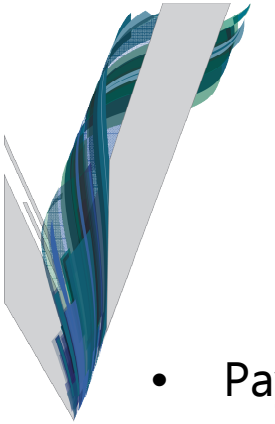
- State Data Security Laws
  - Nine states require that companies implement sufficient policies and procedures to maintain reasonable data security.
  - Typically apply based on individuals' residence, not the entity's location.
  - AR, CA, FL, CT, IN, MD, OR, TX, UT
- Massachusetts Standards for the Protection of Personal Information
  - MA has implemented detailed data security requirements that apply to associations and other legal entities.
  - Requires a written comprehensive information security program, with specific components and technical requirements.

VENABLE



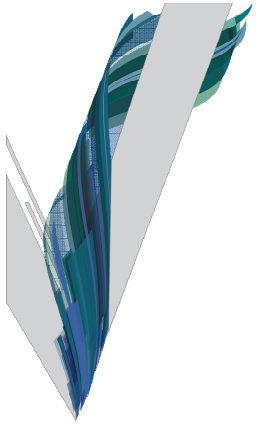
1. Know the Legal Rules

- Data Disposal
  - About 30 states impose legal obligations on companies to properly dispose of records that contain personal, financial, or health information.
  - Laws vary by state and specific methods of disposal are not specified, but a common formulation is that the data must be made "*unreadable or indecipherable through any means*." Kans. Stat. Ann. § 50-7a03.
  - Federal secure disposal rules apply to specific types of data, such as nonpublic personal information held by financial institutions.



1. Know the Legal Rules

- Payment Card Industry Data Security Standards (PCI DSS)
  - Regularly updated security standards created by the credit card industry
  - Practices and policies to protect accountholder data
- Implementation
  - Compliance steps for merchants depend on card processing volume
  - Qualified Security Assessors (QSAs) can assist
  - Information security policy is required
  - Service providers should be PCI DSS compliant
- Enforcement
  - Credit card brands require merchant banks to enforce compliance by their clients
    - Fines imposed on banks can be passed on to companies
  - States have enacted statutory requirements similar to PCI DSS



2. Assess Your Risks

Legal Risk

- Sector-Specific Enforcement (*e.g.,* energy, financial services, health care, advertising, retail, etc.)
- FTC Enforcement
- State Attorney General Enforcement
- Congressional Investigations
- Class Action Lawsuits

Legal Assessment

- Policies/Procedures
- Governance
- Incident Response Plan
- Vendor Selection and Contracts
- Training
- Data Mapping

Legal Risk Management

- Reporting and Decision Making
- Legal and Regulatory Compliance Framework

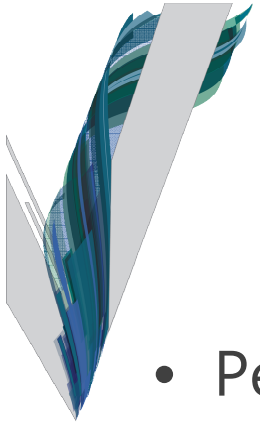
VENABLE

2. Assess Your Risks

- Security program should be proportional to:
  - Data handled
  - Size and nature of business

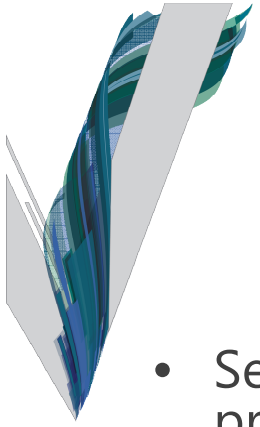
- Administration began to focus on cybersecurity in earnest beginning in 2013
  - Executive Order 13636 directed the National Institute of Standards and Technology ("NIST") to develop a baseline cybersecurity framework
- NIST released the Cybersecurity Framework in February 2014
  - **Voluntary** methodology and process for assessing and reducing cybersecurity risks in critical infrastructure sectors
  - Draft updated v. 1.1 released for comment on January 10, 2017; comments were due in April.

VENABLE



2. Assess Your Risks

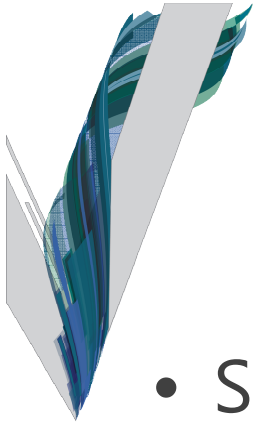
- Perform an enterprise-wide vulnerability assessment
- Implement a comprehensive information security program that addresses any identified vulnerabilities
  - Periodically review and update the information security program
- Implement appropriate data security policies, such as:
  - Data Classification Policy
  - Password Strength Policy
  - Access Control Policy
  - Encryption Policy
  - Data Disposal Policy
  - Patch Management Policy
- Implement an Incident Response Plan



3. Know Your Vendors

- Select and oversee service providers with reasonable security programs (or you may be a service provider)
- Adequate cyber insurance coverage
- Consistent contract provisions related to security and breach response
  - Audits and audit reports
  - Insurance and indemnification
  - Notifying data owner of breach
  - External notifications / credit monitoring / responding to investigations
  - Restrictions on use/disclosure of data
  - Reps and warranties of compliance with privacy and security obligations
  - Data return and disposal

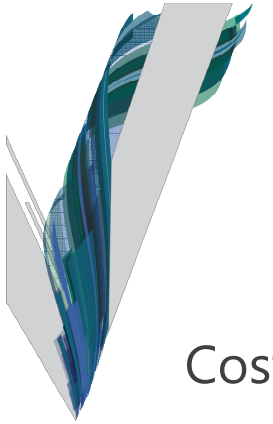
VENABLE



3. Know Your Vendors

- Specific concerns for vendors hired to help with security assessment and services for your business
- Security findings can be sensitive, and may create liability risks for the organization
- Consider structuring the engagement to ensure products are protected by attorney-client privilege to the extent possible

VENABLE



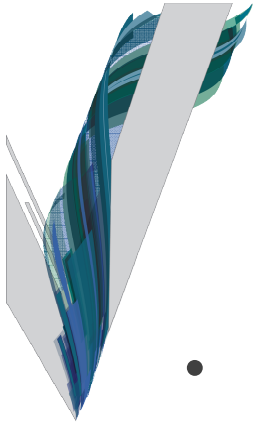
4. Prepare for the Worst

Cost of a data breach

- Many factors contribute to total costs:
  - Breach response efforts
    - Delivering notices, credit monitoring, legal costs, etc.
  - Reputational Costs
    - Customer and employee goodwill, media scrutiny
  - Litigation and/or Regulatory Defense

- Projected average cost of a breach:
  - 1,000 records: $52,000 - $87,000
  - 100,000 records: $366,500 - $614,600
  - 10 Million records: $2,100,000 - $5,200,000
  - Source: 2015 Data Breach Investigations Report, Verizon (2015), available at http://www.verizonenterprise.com/DBIR/2015/

VENABLE



4. Prepare for the Worst

- Service providers face pressure or contract obligations to shoulder costs and/or tasks for data owners

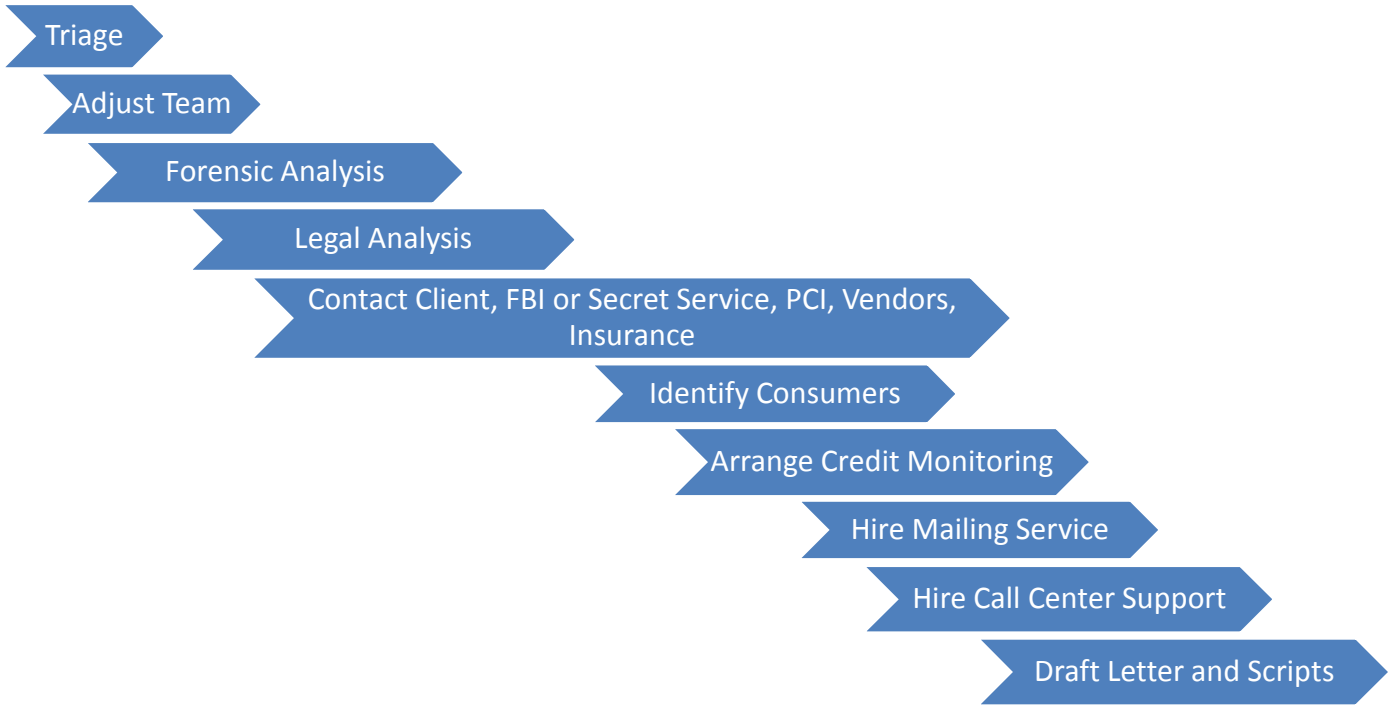
- An effective incident response plan will facilitate:

  - Prompt detection, investigation, recovery;
  - Notification of and cooperation with law enforcement officials, if deemed necessary;
  - Notification to external parties affected by the incident, if any, such as customers, associates, or credit card companies;
  - Notification to cyber insurance provider, if necessary;
  - Notification to affected individuals, if required;
  - Notification to state or federal regulatory agencies, if required;
  - Review of security policies and procedures to prevent a reoccurrence.

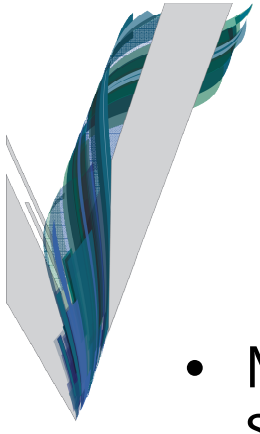
VENABLE

4. Prepare for the Worst

Breach Response Timeline: "Sprinting a Marathon"



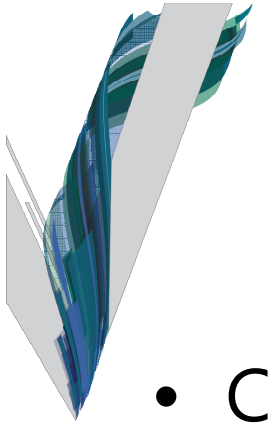
VENABLE



4. Prepare for the Worst

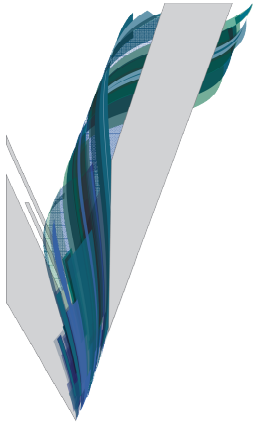
- Most states have implemented a data breach notification statute; federal legislation is being considered
- The requirements for notification can vary widely by state; many states require notice to state authorities and individuals
- Not all security incidents require notification
  - where a "breach" did not occur
  - where the information involved was not "personal information"
  - where there is no risk of harm to affected individuals
- Data owner typically has legal duty to notify affected individuals and government agencies; service provider notifies data owner

VENABLE



5. Stay Up-To-Date

- Cybersecurity risk management is not a "one-time" effort
- Legal standards and security threats are constantly evolving
- Consider periodic review and reassessment, particularly following a breach



Questions?

Julia Kernochan Tama
Partner
Privacy and Data Security Practice
Venable LLP
jktama@Venable.com
202.344.4738

VENABLE