Akerman

Hot Topics and Trends in Cyber Security and Privacy

M. Darren Traub

March 13, 2015

"I'm no expert, but I think it's some kind of cyber attack!"

"Cyber Attacks Ranked Top 5 Most Likely Risks in 2015" - The World Economic Forum

Recent Global Headlines Include:

THE HOME DEPOT

SONY

TARGET

Neiman Marcus

Anthem. BlueCross

Michaels Where Creativity Happens

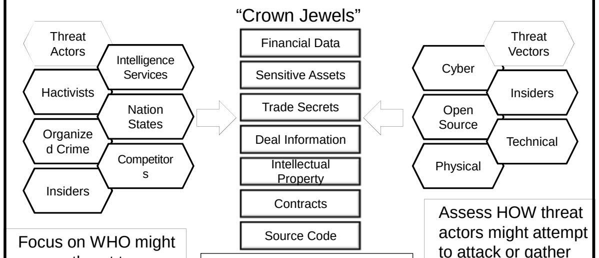
Where Do These Attacks Come From?

- Inside Attacks
- Perimeter Attacks
- Phishing
- Malware & Malvertising
- Social Engineering
- Advanced Persistent Threats

Adversary	Motives	Targets	Impact
Nation State	• Economic, political, and/or military advantage	• Trade secrets • Sensitive business information • Emerging technologies • Critical infrastructure	• Loss of competitive advantage • Disruption to critical infrastructure
Organized Crime	• Immediate financial gain • Collect information for future financial gains	• Financial / Payment Systems • Personally Identifiable Information • Payment Card Information • Protected Health Information	• Costly regulatory inquiries and penalties • Consumer and shareholder lawsuits • Loss of consumer confidence
Hacktivists	• Influence political and / or social change • Pressure business to change their practices	• Corporate secrets • Sensitive business information • Information related to key executives, employees, customers & business partners	• Disruption of business activities • Brand and reputation • Loss of consumer confidence
Insiders	• Personal advantage, monetary gain • Professional revenge • Patriotism	• Sales, deals, market strategies • Corporate secrets, IP, R&D • Business operations	• Trade secret disclosure • Operational disruption • Brand and reputation National security impact

Threat Modeling

Understanding your adversaries and their motivations ensures we are better prepared to defend our "Crown Jewels"



Focus on WHO might pose a threat to your company

Then consider WHAT threat actors are targeting your business ecosystems

Assess HOW threat actors might attempt to attack or gather information on your company

Lessons Learned From Recent Retail and Consumer Events

Attack Method	•Organized and coordinated efforts to exploit a known technical vulnerability in the fundamental infrastructure
Awareness	•Adversaries tested and enhanced their approach over the course of months before executing their campaign; intelligence sources communicated threat elements
Detection	•Technical indicators were undetected during the attack sequence; additionally, third parties, such as law enforcement or banks, detect the compromise, *not* the company
Security Posture	•Known companies compromised were assumed to be compliant with industry standards – compliance does not equal security
Industry Exposure	•Attacks are often not limited to a single company; many companies within an industry sector share the same or similar profile and it is highly like there are other targets and victims

What Are We Talking About?

An individual's ability to control information about him/herself

Personally Identifiable Information ("PII")

- Data that can identify an individual
  - Name
  - Address
  - SSN
  - Driver's license number
  - Location? Triangulated data?

"Sensitive" information

- Medical history, health information
- Bank and Credit Card Account Numbers, Passwords, Financial info.
- Video rental history
- Educational records

Statutory Bases of Information Privacy (Federal)

- HIPAA – health data
- Gramm Leach Bliley – financial data
- COPPA – children's personal information online
- VRPA – video rental history
- TCPA – telemarketing
- FCRA – credit information
- Patriot Act
- Privacy Act – use of data by government

Statutory Bases of Information Privacy (State)

- Data security requirements
- Breach notification
- Document shredding
- Genetic information
- GLB analogues
- Consumer protection laws
- More….

What Can You Do?

Privacy and Security Assessment Checklist

Network security

- ✓ Authentication and firewalls
- ✓ Phishing filters
- ✓ Passwords
- ✓ Access controls
- ✓ Purging accounts of former employees
- ✓ Intrusion detection and prevention
- ✓ Encyption
- ✓ Logging

Privacy and Security Assessment Checklist

Identify and map your data
- What do you have?
- Where is it?

Records retention policy
- If you don't need it, delete it (securely)

Contract with vendors/business partners
- Who has responsibility and liability for data security?
- Audits

Privacy and Security Assessment Checklist

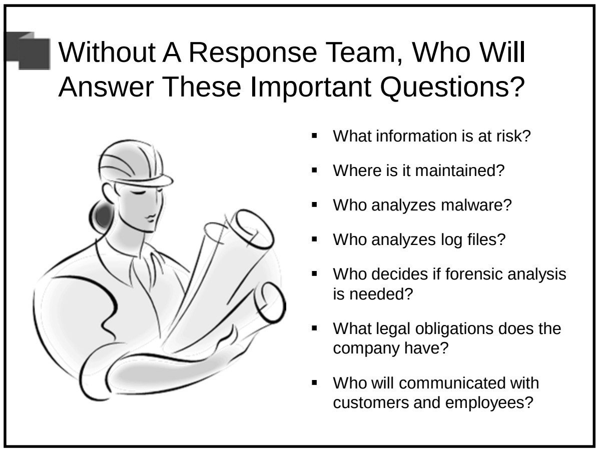
- Employee training
- Privacy notices and practices
  - Do what you say, and say what you do
- Cyber insurance coverage
- Access controls
- Framework cyber checkups

Incident Response Plan

Issue
- Lack of an incident response plan and incident response team

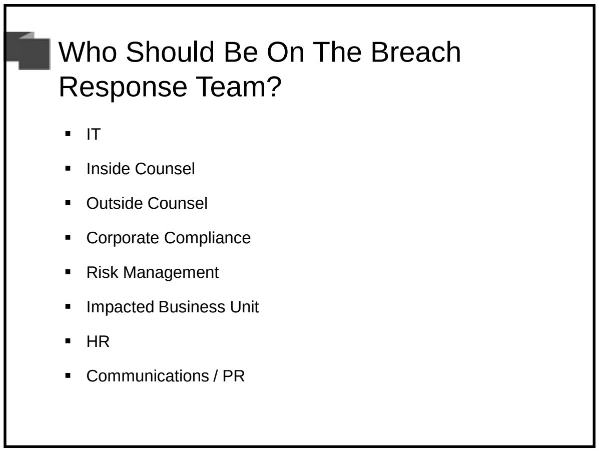
Consequence
- Loss of valuable time, data, and effectiveness because response is not planned or coordinated

Suggested Policy
- Implement plan, assign and train a response team and create a plan



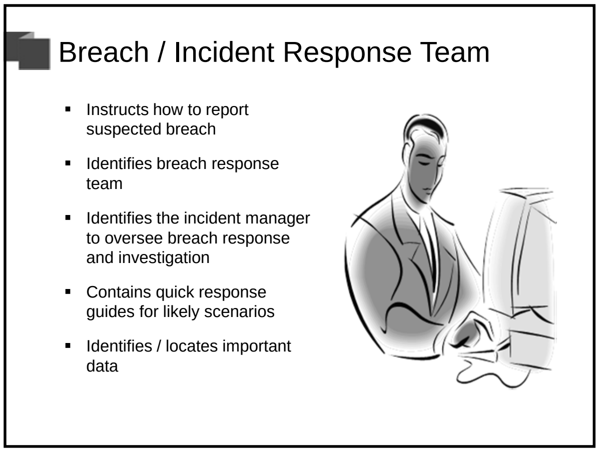
Without A Response Team, Who Will Answer These Important Questions?

- What information is at risk?
- Where is it maintained?
- Who analyzes malware?
- Who analyzes log files?
- Who decides if forensic analysis is needed?
- What legal obligations does the company have?
- Who will communicated with customers and employees?



Who Should Be On The Breach Response Team?

- IT
- Inside Counsel
- Outside Counsel
- Corporate Compliance
- Risk Management
- Impacted Business Unit
- HR
- Communications / PR



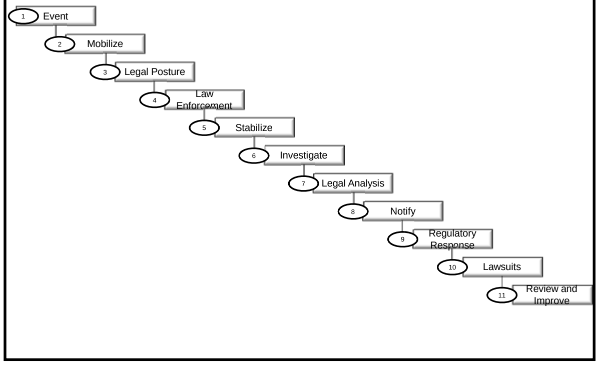
Breach / Incident Response Team

- Instructs how to report suspected breach
- Identifies breach response team
- Identifies the incident manager to oversee breach response and investigation
- Contains quick response guides for likely scenarios
- Identifies / locates important data

Advantages of a Response Team

- Improved decision making process
- Coordination between IT and operations
- Coordination with outside expert
- United efforts with communication
- Damage control
- Basis for preparation exercises
- Efficiency and agility
- Mitigates legal exposure

Data Breach Response Time



1 Event

2 Mobilize

3 Legal Posture

4 Law Enforcement

5 Stabilize

6 Investigate

7 Legal Analysis

8 Notify

9 Regulatory Response

10 Lawsuits

11 Review and Improve

Upon First Notification of a Breach

- Immediately engage outside counsel—so A/C privilege applies
- Notify Chief Privacy Officer
- Gather description of event
- Identify location of event
- Take Immediate Steps To Stop Source Of Breach
  - Employee / Internal
  - Hacker / Virus / Malware
  - Vendor / Third Party

Determine What Information Was Involved

- Does the compromised information meet the definition of personal information or its equivalent under any of the relevant state or federal breach notification rules?
- Certain jurisdictions have adopted expansive definitions of personal information under breach laws
- Was The Information Encrypted?
  - Generally, encryption is available as a safe harbor under existing security breach notification laws
  - Encryption does not include password-protection on equipment such as desktop computers, laptop computers, and portable storage devices

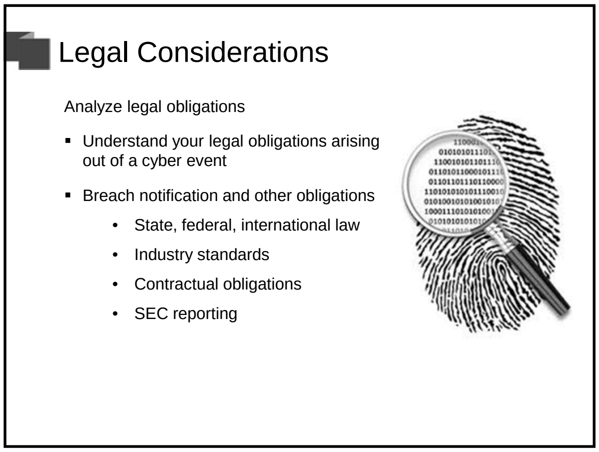
Determine Need To Notify Units Within The Company

- Legal Department
- Information Management (to sequester records)
- Billing (suspend billing process?)
- Human Resources (if a work force member caused the breach)
- Vendors

Conduct an Investigation

Stabilize affected systems and investigate scope

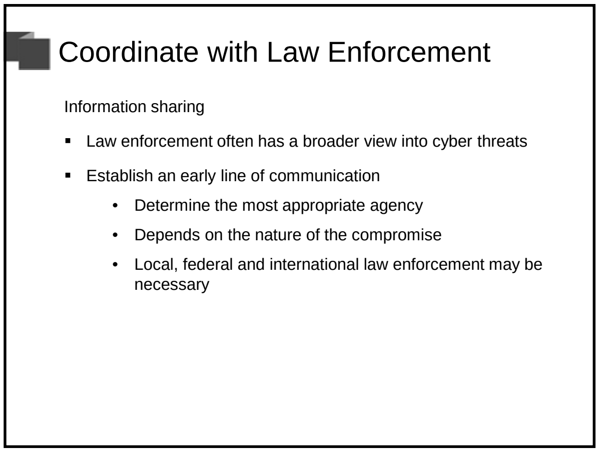
- Contain the attack
- Forensic imaging
- Restore the integrity of the system
- Retain third-party forensic experts?
- Understand:
  - Nature of the compromise
  - Data and systems at issue
  - Whether communications systems are secure
  - Whether insiders are involved



Legal Considerations

Analyze legal obligations

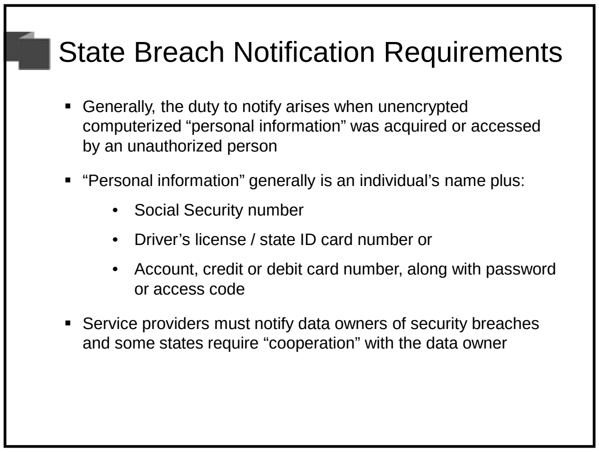
- Understand your legal obligations arising out of a cyber event
- Breach notification and other obligations
  - State, federal, international law
  - Industry standards
  - Contractual obligations
  - SEC reporting



Coordinate with Law Enforcement

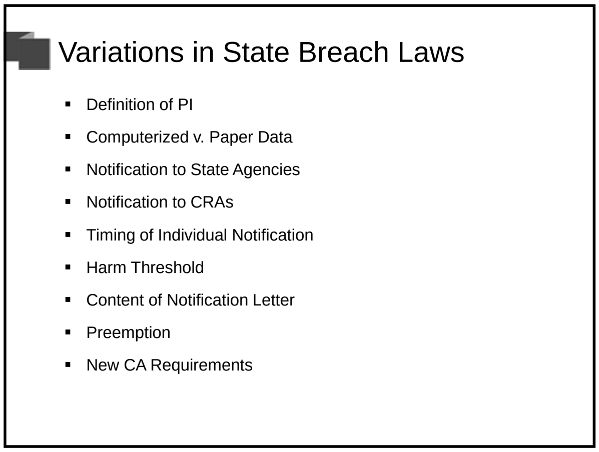
Information sharing

- Law enforcement often has a broader view into cyber threats
- Establish an early line of communication
  - Determine the most appropriate agency
  - Depends on the nature of the compromise
  - Local, federal and international law enforcement may be necessary



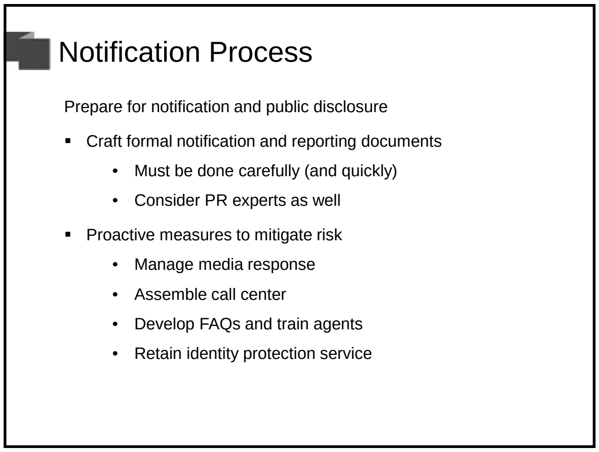
State Breach Notification Requirements

- Generally, the duty to notify arises when unencrypted computerized “personal information” was acquired or accessed by an unauthorized person
- “Personal information” generally is an individual’s name plus:
  - Social Security number
  - Driver’s license / state ID card number or
  - Account, credit or debit card number, along with password or access code
- Service providers must notify data owners of security breaches and some states require “cooperation” with the data owner



Variations in State Breach Laws

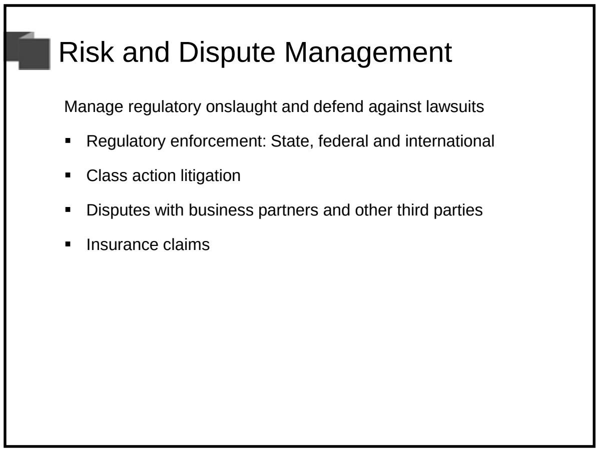
- Definition of PI
- Computerized v. Paper Data
- Notification to State Agencies
- Notification to CRAs
- Timing of Individual Notification
- Harm Threshold
- Content of Notification Letter
- Preemption
- New CA Requirements



Notification Process

Prepare for notification and public disclosure

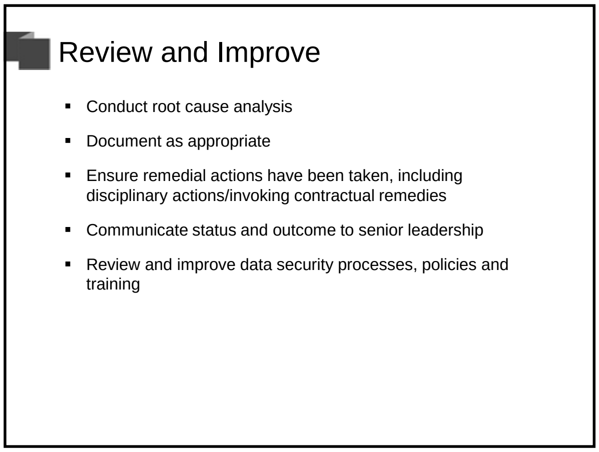
- Craft formal notification and reporting documents
  - Must be done carefully (and quickly)
  - Consider PR experts as well
- Proactive measures to mitigate risk
  - Manage media response
  - Assemble call center
  - Develop FAQs and train agents
  - Retain identity protection service



Risk and Dispute Management

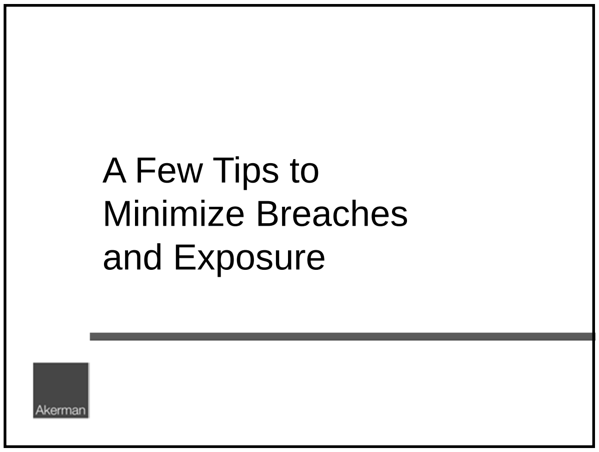
Manage regulatory onslaught and defend against lawsuits

- Regulatory enforcement: State, federal and international
- Class action litigation
- Disputes with business partners and other third parties
- Insurance claims

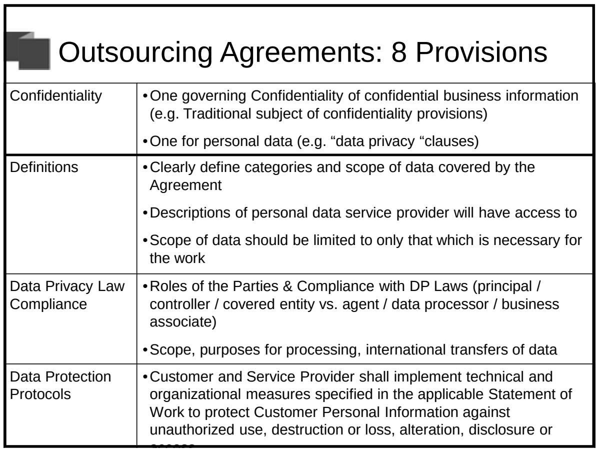


Review and Improve

- Conduct root cause analysis
- Document as appropriate
- Ensure remedial actions have been taken, including disciplinary actions/invoking contractual remedies
- Communicate status and outcome to senior leadership
- Review and improve data security processes, policies and training



A Few Tips to Minimize Breaches and Exposure



Outsourcing Agreements: 8 Provisions

Confidentiality	• One governing Confidentiality of confidential business information (e.g. Traditional subject of confidentiality provisions) • One for personal data (e.g. "data privacy "clauses)
Definitions	• Clearly define categories and scope of data covered by the Agreement • Descriptions of personal data service provider will have access to • Scope of data should be limited to only that which is necessary for the work
Data Privacy Law Compliance	• Roles of the Parties & Compliance with DP Laws (principal / controller / covered entity vs. agent / data processor / business associate) • Scope, purposes for processing, international transfers of data
Data Protection Protocols	• Customer and Service Provider shall implement technical and organizational measures specified in the applicable Statement of Work to protect Customer Personal Information against unauthorized use, destruction or loss, alteration, disclosure or

Security Incidents	• Service provider shall maintain procedures to detect and respond to loss, misuse or unauthorized acquisition of Customer Personal Data while such data is in Service Provider’s custody or control. • Notification requirements in the event of loss, unauthorized acquisition or misuse of unencrypted Customer Personal Data.
Limitations of and Exclusions from Liability	Define and address: • Direct Damages • Indirect Damages
Security Audit Provisions	• A standard set of audits or specific audits required by customer should be included
Customer-Requested Background Checks of Supplier Personnel	• When a customer requests specific background checks, this should be included in the terms, subject to any local legal requirements (some jurisdictions limit what is allowed).

Beware of the Mobile Ecosystem

- 1.4 billion smart phones in use
- Mobile marketing will generate $400 billion in revenues by 2016
- 224 million Americans actively use mobile apps
- 85% of mobile device users prefer apps to mobile sites
- These apps are on the same devices as your company’s confidential information/email

The Mobile Ecosystem

90% of full-time employees use a personal smartphone for work purposes

- 62% of those use it every day
- 39% don’t use password protection
- 52% access unsecured wifi networks
- 69% believe they are expected to access work emails after hours

(Cisco, BYOD Insights in 2013: A Cisco Partner Network Survey, March 2013)

“I thought you said I could bring in my own device.”

The Mobile Ecosystem

BYOD: Bring Your Own Device

- A BYOD program includes:
  - Policies that govern use of personal devices to access corporate services
  - Policies attempt to manage risk associated with storage and transmittal of data using devices that may be outside of the employers control
  - Policies to address impact of mobile devices on existing workplace behavior

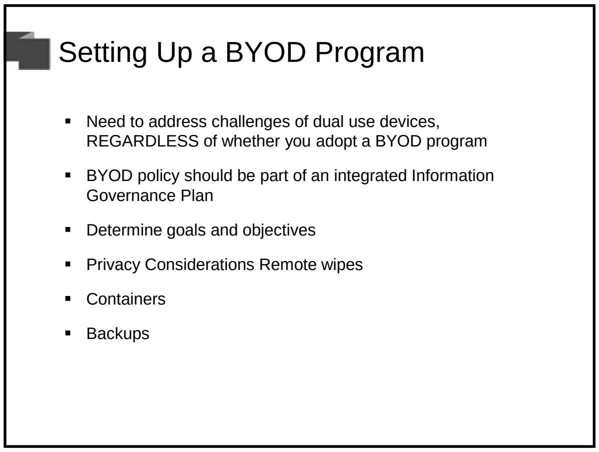
COPE: Corporate Owned, Personally Enabled

Mobile Device Management

- Software that allows corporate IT to manage use of mobile devices. Component of BYOD programs. Features may allow an employer to:
  - Require users to register devices as condition of network access
  - Enable remote locking or wipe of device
  - Implement anti-spam solutions, block specific apps, and prevent users from disabling or altering security settings on devices
  - Monitor employee use and location of user and device

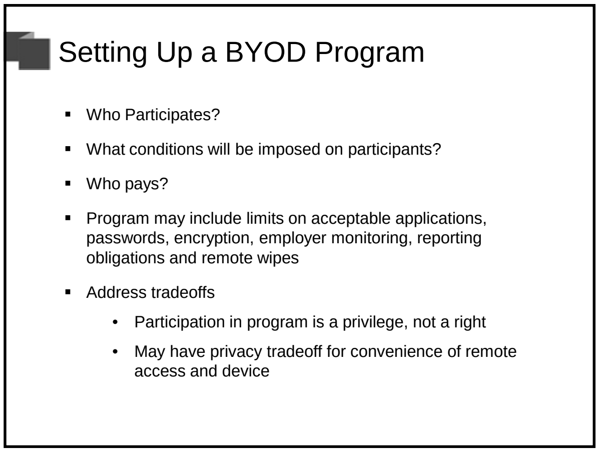
Policies Affected by BYOD: Mobile Devices Have Impact on Policies Throughout Your Business

- Data Privacy & Security
- Harassment, Discrimination & EEO
- Workplace Safety
- Time Recording and Overtime
- Acceptable Use of Technology
- Compliance and Ethics
- Records Management
- Litigation Holds
- Confidentiality & Trade Secret Protection



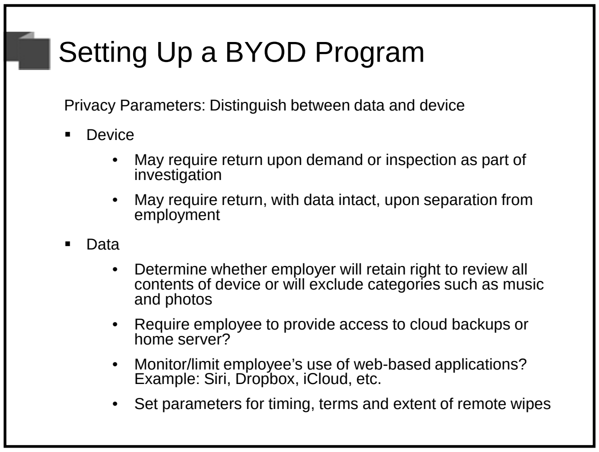
Setting Up a BYOD Program

- Need to address challenges of dual use devices, REGARDLESS of whether you adopt a BYOD program
- BYOD policy should be part of an integrated Information Governance Plan
- Determine goals and objectives
- Privacy Considerations Remote wipes
- Containers
- Backups



Setting Up a BYOD Program

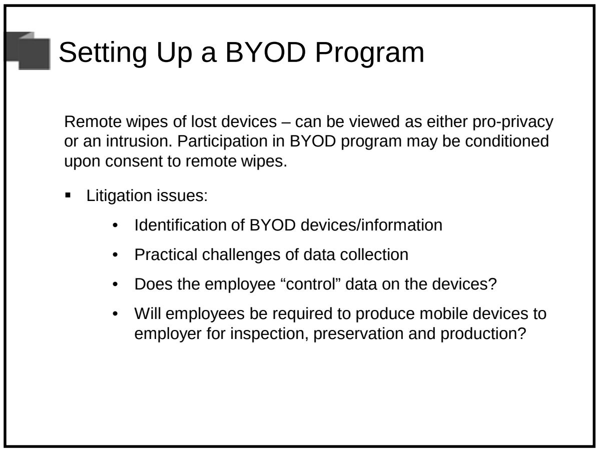
- Who Participates?
- What conditions will be imposed on participants?
- Who pays?
- Program may include limits on acceptable applications, passwords, encryption, employer monitoring, reporting obligations and remote wipes
- Address tradeoffs
  - Participation in program is a privilege, not a right
  - May have privacy tradeoff for convenience of remote access and device



Setting Up a BYOD Program

Privacy Parameters: Distinguish between data and device

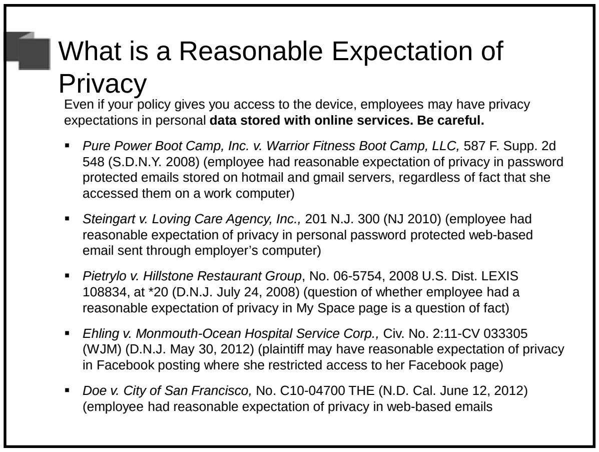
- Device
  - May require return upon demand or inspection as part of investigation
  - May require return, with data intact, upon separation from employment
- Data
  - Determine whether employer will retain right to review all contents of device or will exclude categories such as music and photos
  - Require employee to provide access to cloud backups or home server?
  - Monitor/limit employee’s use of web-based applications? Example: Siri, Dropbox, iCloud, etc.
  - Set parameters for timing, terms and extent of remote wipes



Setting Up a BYOD Program

Remote wipes of lost devices – can be viewed as either pro-privacy or an intrusion. Participation in BYOD program may be conditioned upon consent to remote wipes.

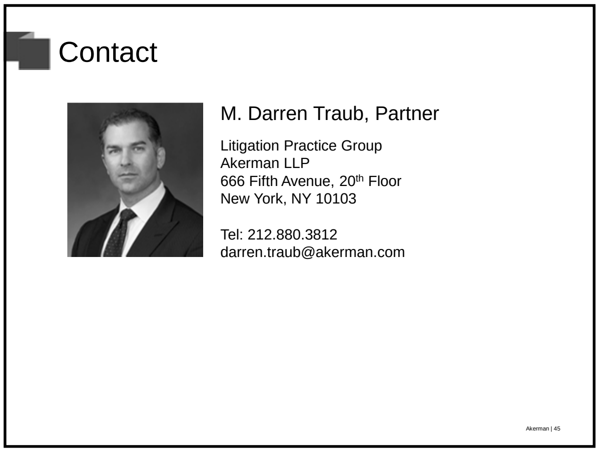
- Litigation issues:
  - Identification of BYOD devices/information
  - Practical challenges of data collection
  - Does the employee “control” data on the devices?
  - Will employees be required to produce mobile devices to employer for inspection, preservation and production?



What is a Reasonable Expectation of Privacy

Even if your policy gives you access to the device, employees may have privacy expectations in personal **data stored with online services. Be careful.**

- *Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC,* 587 F. Supp. 2d 548 (S.D.N.Y. 2008) (employee had reasonable expectation of privacy in password protected emails stored on hotmail and gmail servers, regardless of fact that she accessed them on a work computer)
- *Steingart v. Loving Care Agency, Inc.,* 201 N.J. 300 (NJ 2010) (employee had reasonable expectation of privacy in personal password protected web-based email sent through employer’s computer)
- *Pietrylo v. Hillstone Restaurant Group*, No. 06-5754, 2008 U.S. Dist. LEXIS 108834, at *20 (D.N.J. July 24, 2008) (question of whether employee had a reasonable expectation of privacy in My Space page is a question of fact)
- *Ehling v. Monmouth-Ocean Hospital Service Corp.,* Civ. No. 2:11-CV 033305 (WJM) (D.N.J. May 30, 2012) (plaintiff may have reasonable expectation of privacy in Facebook posting where she restricted access to her Facebook page)
- *Doe v. City of San Francisco,* No. C10-04700 THE (N.D. Cal. June 12, 2012) (employee had reasonable expectation of privacy in web-based emails



Contact

M. Darren Traub, Partner

Litigation Practice Group
Akerman LLP
666 Fifth Avenue, 20th Floor
New York, NY 10103

Tel: 212.880.3812
darren.traub@akerman.com

Akerman | 45

Akerman

Akerman LLP | 600+ lawyers | 20 locations | akerman.com

©2015 Akerman LLP. All rights reserved.