

REUTERS/Benoit Tessier

Data Breaches: Readiness and Response

October 3, 2015

Presenters:

Erica Gann Kitaev, Senior Legal Editor, Practical Law

Scott Koller, Counsel, BakerHostetler

Zach Ratzman, Director of Government, Practical Law

This is an informational and educational report distributed by the International Municipal Lawyers Association during its 2015 Annual Conference, held October 3-7, 2015 in Las Vegas, NV. IMLA assumes no responsibility for the policies or positions presented in the report or for the presentation of its contents.

BakerHostetler

Practical Law™ A THOMSON REUTERS LEGAL SOLUTION

© 2015 Thomson Reuters.

Agenda

- Data Breach Readiness
  - Laws Protect “Personal Information”
  - Knowing the Applicable Laws and Standards
  - Understanding the Threats
  - Security Best Practices and Fundamentals
- Data Breach Response
  - Verification
  - Containment and Mitigation
  - Investigation and Analysis
  - Notification
  - Post-incident Review

Data Breach Readiness

Laws Protect "Personal Information"

What is Personal Information? Individual first name or initial + last name, plus the following

- User IDs, passwords, mother's maiden name, answers to security questions
- Government identification numbers (driver's license, SSN, passport)
- Financial account numbers (usually in combination with security codes)
- Employee identification number (not common)
- Biometric data
- Medical and/or health insurance information
- *Increasing trend to not require name under certain circumstances*

Knowing the Applicable Laws and Standards

- State Law
  - General or State Agency Data Breach Statute(s)
  - Medical Privacy (or other information-specific) Laws
- Federal Law
  - HIPAA/HITECH
- Contracts/Industry Standards
  - PCI DSS

Understand the Threats

- Inside Threats
  - Employee negligence
    - Security failures
    - Lost mobile devices
  - Employee ignorance
    - Improper storage and disposal of personal information
    - Lack of education and awareness
  - Malicious employees
- Outside Threats
  - Hackers
  - Malware
  - Phishing
  - Thieves
  - Vendors

Security Best Practices

Employ Technical, Administrative and Physical Safeguards

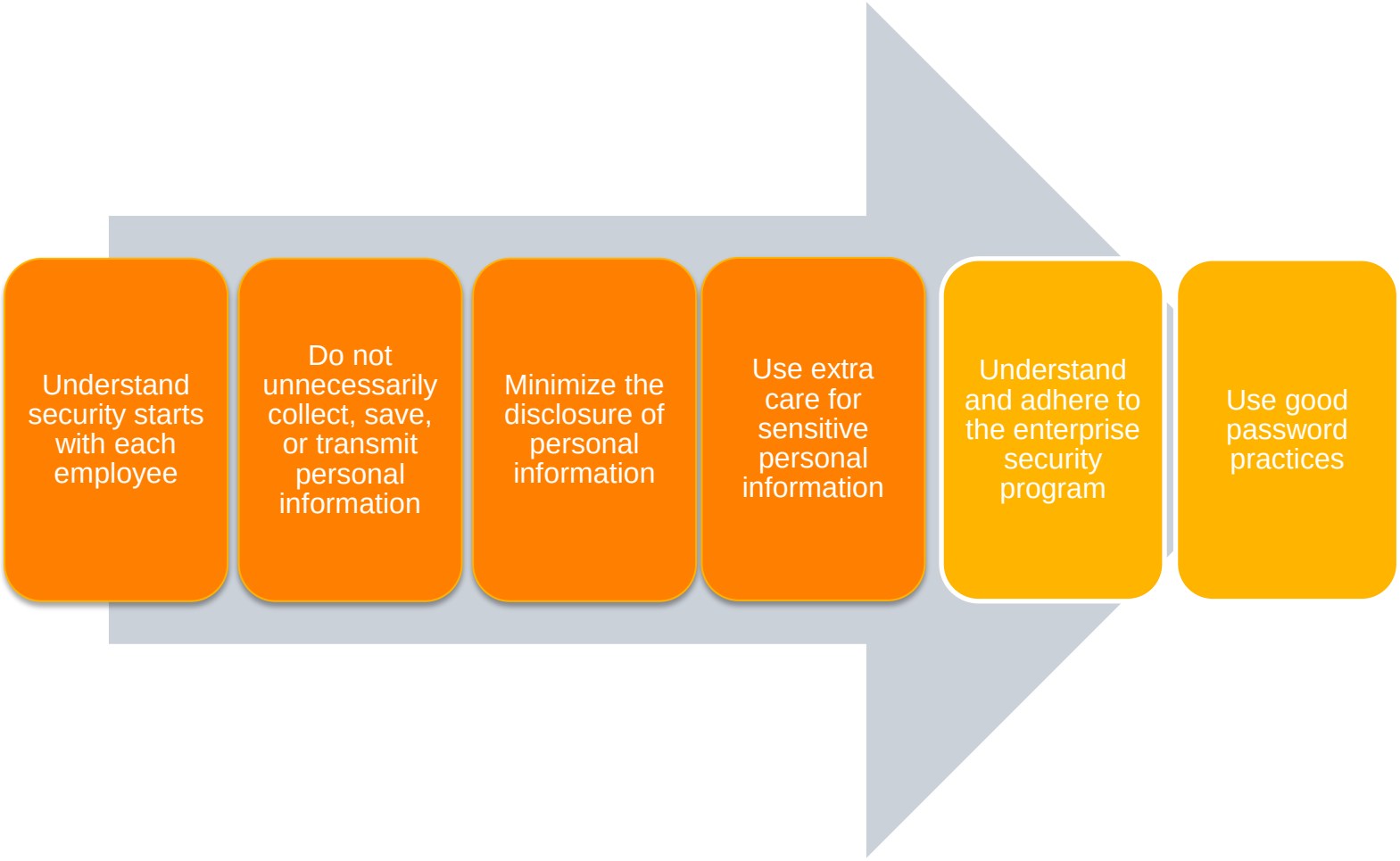
- Key **administrative safeguards** include:
  - Written policies and procedures
    - Privacy policies
    - Information security policies
    - Use policies, such as BYOD, etc.
  - Employee training and awareness
  - Personal information inventories
  - Vendor oversight programs
- Key **physical safeguards** may include:
  - Device and media controls
  - Locking file cabinets
  - Securing hardware with locks
- Key **technical safeguards** may include:
  - Encryption
  - Anti-virus programs
  - Access controls
  - Firewalls

Security Fundamentals*

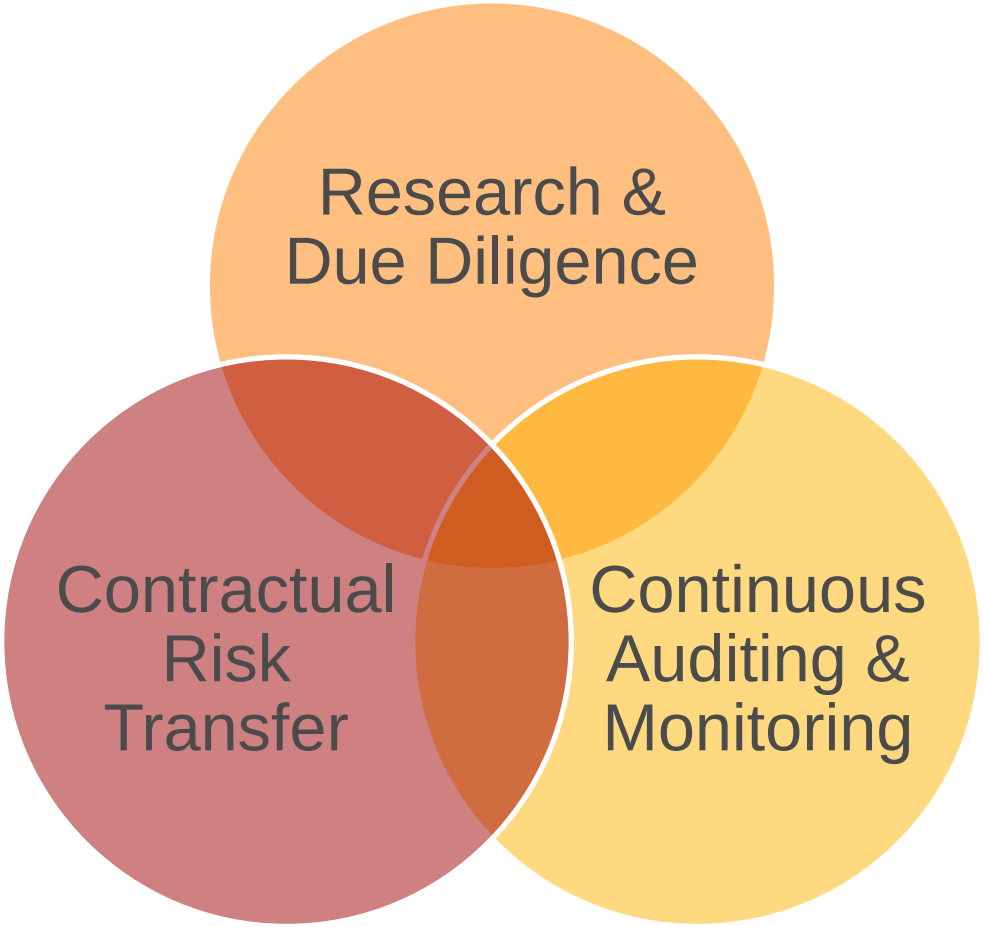
- Do not collect, keep, or use personal information unnecessarily
- Restrict access to sensitive data
- Require secure passwords and authentication
- Store sensitive personal information securely and protect it during transmission:
- Ensure proper configuration by segmenting the network and monitoring who is trying to get in and out
- Secure remote access to the network
- Apply sound security practices when developing new applications
- Make sure service providers implement reasonable security measures – put them in writing and verify compliance
- Put procedures in place to keep security current and address vulnerabilities
- Secure paper, physical media and devices.

** See the FTC's Start with Security: A Guide for Business*

Security Fundamentals / Personal Use Security



Security Fundamentals / Vendor Management



Data Breach Response

Verify that a Breach has Occurred

- Identify the affected system(s) or hardware
  - Lost laptop v. the Network
- Identify the nature of the data affected
  - PII? Encrypted?
- Understand the incident type
  - Malicious v. accidental; internal actor(s) v. external actor(s)
- Determine whether data was exposed
  - Actual exposure v. reasonable likelihood of exposure

Contain and Mitigate the Damage

- Identify systems and information that were compromised
- Take immediate steps to stop the source/responsible entity
  - E.g., Take machines offline, find and remove malware
- Determine whether other systems are threatened
- Implement additional technical measures as needed
  - E.g., Changing locks, passwords, admin rights

Investigate and Analyze the Incident

- Collect and preserve information and evidence
  - Document the who, what, why and when
- Consider attorney-client privilege and Sunshine Laws
  - Analysis of your analysis
- Determine whether outside help is needed
  - Third-party consultants/forensic experts
  - Outside counsel
- Analyze the legal implications
  - Risk of harm to affected persons
  - Encryption (or other readability) safe harbors

Make Necessary Notifications (if any)

- Determine Who
  - Affected individuals
  - Regulatory/law enforcement authorities
  - Third-party vendors/insurance carriers
- Determine How
  - Medium: mail? email? phone?
  - Use a vendor or handle in-house?
- Determine What
  - Look to the relevant laws
- Determine When
  - Statute-specific, but generally 30-45 days (or as soon as practicable)

Conduct a Post-Incident Review

- Review existing security policies and procedures
  - What worked, what did not
  - What could have helped or prevented the incident
- Improve incident response plan
  - Incorporate lessons learned

Relevant Practical Law Resources

- Data Breach Response Checklist (included in CLE materials)
- Practice Note, The NIST Cybersecurity Framework
- Practice Note, Breach Notification
- Data Breach Notification Laws: State Q&A Tool
- Cyber Insurance: Insuring for Data Breach Risk

These resources are available with the free, no-obligation trial password to Practical Law you receive by attending this session.

Practical Law:

What Are You Working On?

http://us.practicallaw.com/about/us-contact-us

Zach Ratzman

Practical Law

zach.ratzman@thomsonreuters.com

Scott Koller, Counsel

BakerHostetler

(mskoller@bakerlaw.com)

Questions

BakerHostetler

Practical Law™ A THOMSON REUTERS LEGAL SOLUTION