

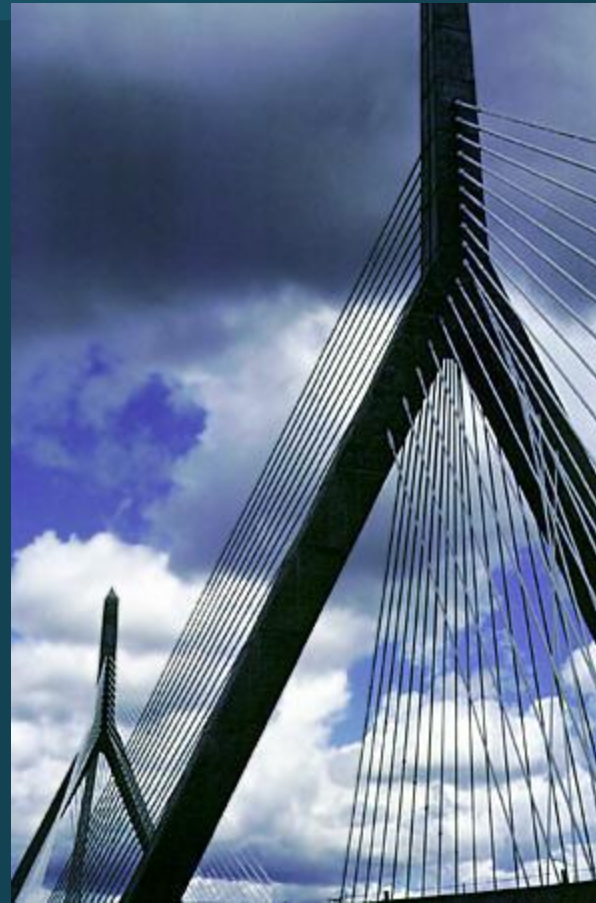
JOHNSON|HALEY

# Massachusetts Data Privacy Regulations



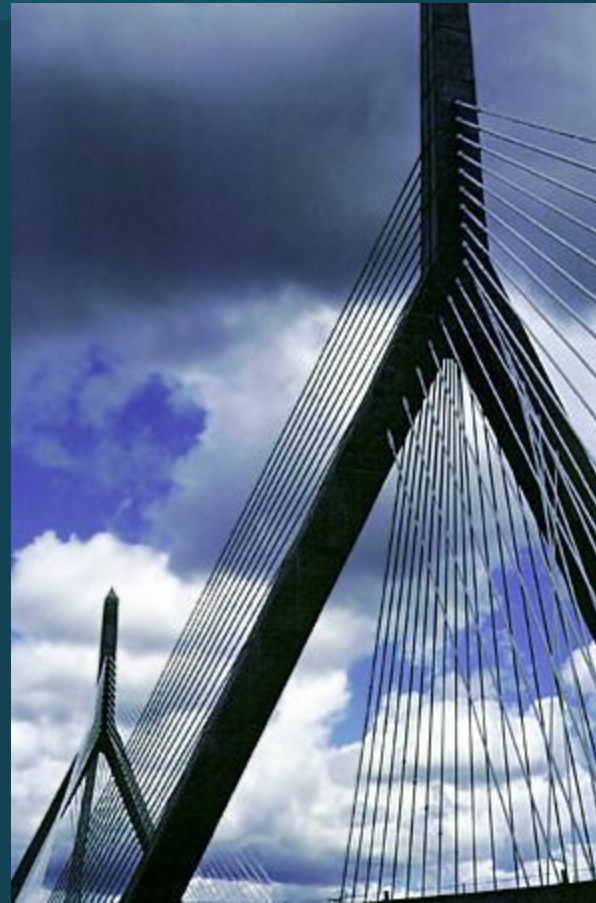
# Agenda

- Context, Basic Facts
- Your Responsibilities
- Key Requirements
- Enforcement
- How we can help
- Summary



# Today's Panel

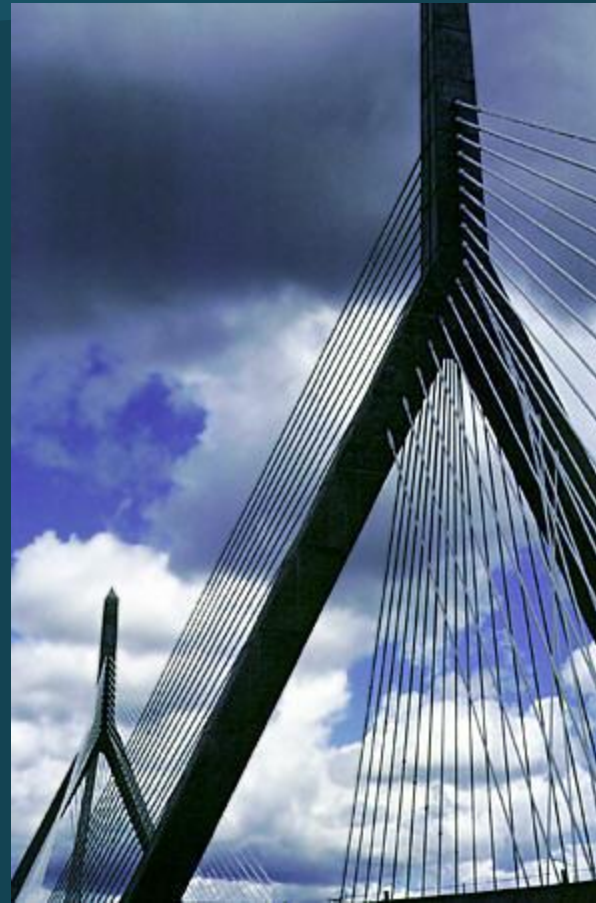
- Pierce Haley, Esq.,  
Johnson Haley LLP
- Peter Radochia,  
KyndL Corporation



# Legal Issues

Pierce J. Haley, Esq.  
[phaley@johnsonhaleyllp.com](mailto:phaley@johnsonhaleyllp.com)

Johnson Haley LLP  
51 Franklin St.  
Boston, MA 02110  
(617) 778-1200



JOHNSON | HALEY

# Big Picture

- Relax

# Big Picture

- Relax
- You don't need extensive knowledge of computers

# Big Picture

- Relax
- You don't need extensive knowledge of computers
- Businesses may already be in compliance

# Big Picture

- Relax
- You don't need extensive knowledge of computers
- Businesses may already be in compliance
- For others, there are simple rules to help bring you into compliance

# Scope

- Who is affected by this new law?
  - Anyone with “data that includes personal information about a resident of the commonwealth”

# Scope

- Who is affected by this new law?
  - Anyone with “data that includes personal information about a resident of the commonwealth”
  - In other words, everyone

# Scope

- Who is affected by this new law?
  - Anyone with “data that includes personal information about a resident of the commonwealth”
  - In other words, everyone
- But you have till March 1, 2010 to comply

# Your Responsibilities

- Audit
- Written Comprehensive Information Security Program (“WISP”)
- Implementation
- Ongoing compliance

Johnson Haley and KyndL will be pleased to assist you with these tasks.

# Audit

- Identify and assess all risks
  - Where do you keep the data
    - Files
    - Computers
    - Other
  - Who has access to it

# The WISP

- Need to draft a plan
  - Written
  - Periodically updated
    - At least annually

# The WISP

- Things to consider within the Plan
  - Designate an employee to be responsible for maintaining data security

# The WISP

- Things to consider within the Plan
  - Designate an employee to be responsible for maintaining data security
  - Identify and assess all risks

# The WISP

- Things to consider within the Plan
  - Designate an employee to be responsible for maintaining data security
  - Identify and assess all risks
  - Develop/implement employee security policies

# The WISP

- Things to consider within the Plan
  - Designate an employee to be responsible for maintaining data security
  - Identify and assess all risks
  - Develop/implement employee security policies
  - Develop/implement contractor and visitor security policies

# The WISP

- Things to consider within the Plan
  - Designate an employee to be responsible for maintaining data security
  - Identify and assess all risks
  - Develop/implement employee security policies
  - Develop/implement contractor and visitor security policies
  - Impose penalties and require signed nondisclosures for everyone

# The WISP

- Prevent physical access to info storage
  - By staff
  - By former employees
  - By all others

# The WISP

- Monitor effectiveness
  - From a personnel point of view
  - From a technical point of view

# The WISP

- Monitor effectiveness
  - From a personnel point of view
  - From a technical point of view
  - Do you need to change the way you do business???

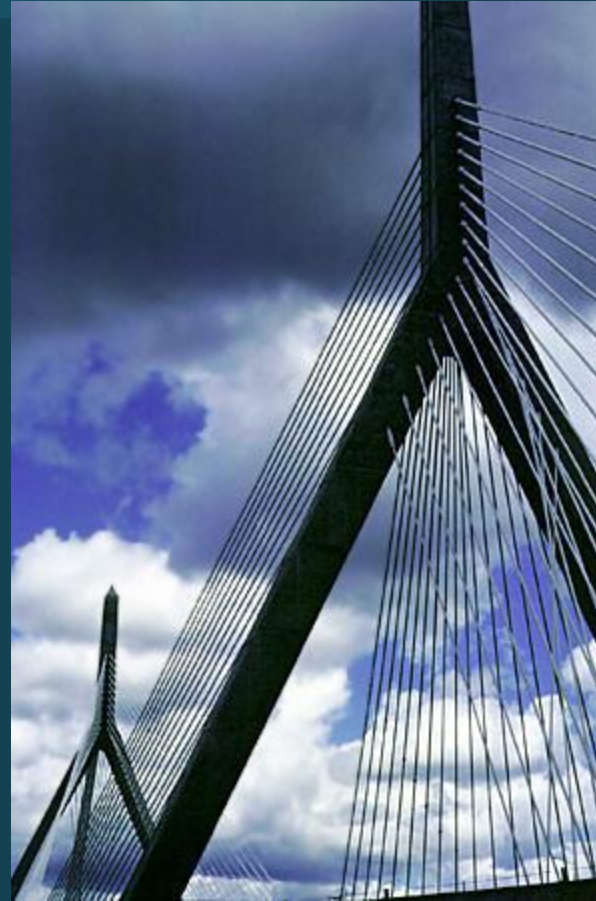
# The WISP

- Review security measures
- Document any breaches

# Technical Issues

Pete Radochia  
[pradochia@kyndl.com](mailto:pradochia@kyndl.com)

KyndL Corp  
40 Salem Street  
Lynnfield, MA 01940  
(781) 463-6006



JOHNSON | HALEY

# IT Requirements

- Based upon the output of the Audit
- What do your business processes dictate you need?
  - Should you change business processes?
  - Should you implement new technology?

# IT Requirements

- Secure user authentication protocols
  - User IDs
  - Passwords or biometric/token devices
  - Safeguarding of passwords, etc.
  - Restricting scope of access
  - Safeguards against “phishing”

# IT Requirements

- Secure Access control measures
  - Access on need-to-know basis
  - Logins and passwords must be unique and universal
    - No default or vendor-supplied passwords

# IT Requirements

- Encryption of personal confidential data
  - a) On public networks
  - b) Transmitted wirelessly
  - c) On laptops
  - d) On other portable devices
    - USB drives
    - CD-ROM, etc.

# IT Requirements

- Operating System security patches

# IT Requirements

- Operating System security patches
- Internet firewall protection

# IT Requirements

- Operating System security patches
- Internet firewall protection
- “Reasonable” monitoring for unauthorized use

# IT Requirements

- Operating System security patches
- Internet firewall protection
- “Reasonable” monitoring for unauthorized use
- Periodic breach testing

# IT Requirements

- Up-to-date “security agent software”
  - “Malware protection”
  - “Reasonably up-to-date” patches and virus definitions
- Employee training on security software
- One Size Does Not Fit ALL

# Enforcement

Chapter 93H – The Attorney General is charged with enforcing the provisions of the law and can file injunctions or take other action to remedy breaches of security.

Violating the terms of an injunction carries a civil penalty of \$10,000 for each violation.

# How Can We Assist You

- Audit
- Written Comprehensive Information Security Program (“WISP”)
- Implementation
- Ongoing compliance

# Summary

- Protecting your data
  - Make a plan and make sure that your Business is in compliance
- Reporting of breaches
  - If a breach occurs at your company, you must notify the appropriate people

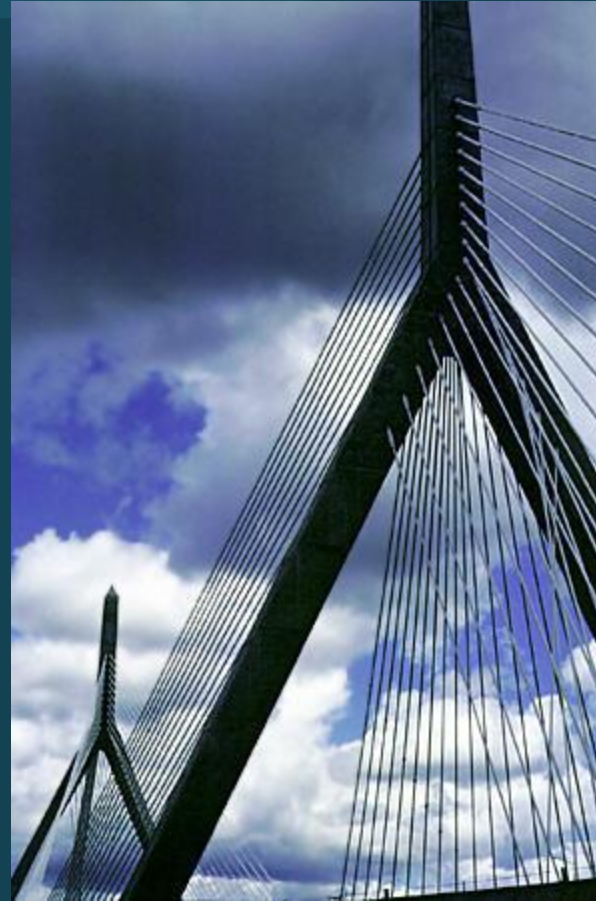
# For More Information

Pierce J. Haley, Esq.  
[phaley@johnsonhaleyllp.com](mailto:phaley@johnsonhaleyllp.com)

Johnson Haley LLP  
51 Franklin St.  
Boston, MA 02110  
(617) 778-1200

Pete Radochia  
[pradochia@kyndl.com](mailto:pradochia@kyndl.com)

KyndL Corp  
40 Salem Street  
Lynnfield, MA 01940  
(781) 463-6006



JOHNSON | HALEY