Massachusetts' Data Protection Law- A Proactive Approach

John Moynihan, CGEIT

President

Minuteman Governance

Introduction

Minuteman Governance

- A consultancy providing information security services to public and private sector clients.

- Regulatory Compliance, Program Development, Risk Assessment, IT Audit, Incident Response and Data Breach Investigation.

Clients

- Energy
- Hospitality
- Financial Services
- Media
- Real Estate
- State/Municipal Government
- Professional Services

201 CMR 17

- Overview
- Scope and Critical Definitions
- Distinguishing Aspects
- Common Misconceptions
- Case Studies
- Regulatory Horizon

The Law - MGL Ch 93H

- Passed July 2007
- Original Date - October 31, 2007
- Included Public Sector

Applicability

- Any "person" that collects personal information about a Massachusetts resident
- Electronic and Paper Records
- Customers and Employees

- Intersects all Industries
- Limited Exemptions
- Overshadows existing laws

Contrast and Compare

- "PCI" – Cardholder
- "HIPAA"/HITECH – Health
- "Red Flag" – Financial Institutions
- Only Customers, Patients, Clients

Exemptions

State Agencies

Federal Agencies

Municipalities

Authorities

Key Identifiers

- SSN
- Credit/Debit Card
- Drivers License
- Financial Account
- Passport

California

- First to enact a data breach law in 2003. Requires notification of victims and credit freezes.
- Precedent regulation at the time.

Nevada

- October 1, 2008 - Encryption of transmitted data outside of an entity's "secure system".

- January 1, 2010 - Expanded to include portable devices.

Oregon

- Organizations that collect and handle personal information must develop, implement, and maintain safeguards.
- Administrative, technical and physical controls are required.

Massachusetts

"Control" vs. Notification"

Distinguishing Elements

- Control Based
- Non-technical Focus
- Severe Consequences
- Employee Data

Requirements

- Administrative
- Technical
- Physical

Internal Risk

- Employees
- Vendors
- Business Partners

Misconceptions

- There are many misconceptions regarding the law.
- Misinformation is contributing to non-compliance.

Misconception #1

- "This is an IT law."
- Technology alone will not facilitate compliance.
- Dangerous Approach

Misconception #2

- PCI, HIPAA, HITECH, Red Flag compliance translates into 201 CMR 17 compliance.
- This is inaccurate.

Misconception #3

- "We don't collect customer information, so the law doesn't apply to us."
- The law also applies to employee data.

Misconception #4

- "What are the chances we'll get caught? We will take our chances with the fines."
- Third-Party Requirement is significantly impacting and disrupting relationships.

Misconception #5

- "Encrypt Everything"
- Only required for transmissions and media containing "personal information."

Misconception #6

- "We don't maintain any personal information on our network or in any electronic format."
- Applies to paper records.

Common Exceptions

- Assessments performed within a variety of diverse industries.
- Recurrent exceptions have been identified.
- These areas warrant your attention.

Administrative Issues

- Risk Assessment
- Ambiguous Policies
- Lack of Employee Training
- Nonexistent Third-Party Controls
- Absence of Discipline
- Minimal Compliance Monitoring
- Organizational Disregard
- Password Control

Technical Issues

- Retention and System Back-up
- Mobile and Portable Devices
- Patch Management
- Email
- Virus Protection
- Encryption

Physical Security Issues

- Facility Access Control
- Infrastructure Security
- Data Destruction/Disposal
- Off-Site Document Storage

Consequences

- Third Party Disruptions
- $5000 for each record
- Notification of victims
- Litigation

Regulatory Horizon

HR 2221

- Passed House December 8
- Will Supersede State Laws
- Control Based Approach

Major Requirements

- A) Create a security policy for the collection, use, sale, other dissemination, and maintenance of such personal information.

- (B) Identify an individual as the point of contact with responsibility for the management of information.

Requirements

- C) Implement a process for identifying and assessing any reasonably foreseeable vulnerabilities.
- D) Conduct regular monitoring for a breach of system security.

Sound Familiar?

- If your organization has not fully addressed the law's requirements, I urge you to act now by altering your practices or deploying the necessary administrative, technical and physical security controls.

Summary

- MA 201 CMR 17 is a reality
- Multifaceted approach required
- Non-technical elements
- Employees central to compliance
- Third-parties exposure critical
- Peripheral view necessary

Questions

Contact

- John Moynihan
- (617) 645-4422
- minutemangovernance.com