Agenda

• High level requirements
• A written program
• A sample structure
• Elements of the program
• Create a program description
WISP

- The law requires organizations to have a formal comprehensive written information security program (WISP)
- The law requires organizations to have two types of controls in place in their security programs
  - Administrative controls (organizational, policy)
  - Computer system security controls (software, administrative processes)
  - There is overlap
- What is a WISP?
  - Full documentation of your security program
  - Documentation of the specific controls required by the law
Administrative Controls

- Establishment of a responsible person or group
- Risk assessment and treatment
- Security policy
- Education and training
- Identity management and access control
- Partner management
Technical Controls

- Secure authentication and identity management
- Access controls on protected information
- Encryption of protected information when transmitted wirelessly
- Monitoring for unauthorized use and monitoring of access to protected data
- Encryption of personal information on laptops or other portable devices
- Reasonably up-to-date versions of system security agent software
- Firewalls protecting systems from the Internet
- Virus protection, patch management
- Education and training on technical controls
A Program: Two Approaches

• A 201 CMR 17 specific program
  • A policy that matches one-to-one the controls required
  • Pros: simple policy, well understood controls
  • Cons: assumes that this regulation establishes all required controls or requires multiple policies to serve multiple regulations

• A general security and compliance program
  • Single policy and governance to support various business, regulatory, technical, and contractual requirements
  • Pro: A single structure for all needs
  • Cons: More complex policy
Program Governance

- Appoint one or more people responsible for program maintenance
  - Assign both business and technical representatives to this function
- Establish security policies to safeguard the information
  - Establish a policy framework that deals with all security
  - Add specific policies for dealing with protected information from various
  - Establish a review and approval process and schedule
- You must establish disciplinary measures for failure to comply with policy
- Breach notification structure
- This structure should allow you to satisfy other regulatory needs (e.g., PCI, HIPAA, Red Flag Rules)
Policy Structure

- Many ways to structure policies and your program
- Policy sets are available online from many sources
- Some specific 201 CMR 17 policies can be as brief as 5 pages
- The most useful approach is a general policy structure that can accommodate multiple standards and regulations
- Policy is derived from policy requirements throughout ISO 27002
- This presentation meets 201 CMR 17 requirements
Sample Policy Structure

- Organization and Policy
- Hard and Information Asset Management
- Risk Assessment
- Information classification and handling
- Human resources and training
- Access control
Policy Structure (cont.)

- Incident response
- Physical security
- Partner management
- Vulnerability management
- System Acquisition and development
- Administration and management
Getting The Program Started

- A security and compliance program requires cooperation from the top to the bottom
- Regulatory compliance is a business issue
  - Needs to be translated into responsibilities, technology, behavior, and budget
  - This means that you need involvement from business, technology, legal, human resources, and management at multiple levels
  - In the end, the program needs to work for every employee and business partnership
- You will need to establish and maintain the program forever
- It can be expensive
Risk Management

• Establish a methodology for assessing, documenting, and managing risk
  • The heart of 201 CMR 17
  • Risk needs to be assessed regularly, on schedule and in response to events
  • Many organizations, even big ones, do not have such a methodology in place
  • Required by PCI and HIPAA
  • Needs to deal specifically with risk of compromise of protected information in any form

• Need to assess the effectiveness of controls in mitigating risk
  • Specifically mentions training, compliance with policy, and means of detecting and preventing security failures
Partner Management

- You need to ensure that 3rd party service providers have the capacity to protect personal information as described in the law.
- This typically means verifying the existence of a WISP and inquiring about the practices the provider has in place.
- Best practice calls for a partner management program including risk assessment and regular reviews of provider risk and practice.
- Responsibility for compromise: in the past, only entities entrusted with the data were responsible, now anyone possessing information is responsible.
Identity & Access Management

- You are required to tightly control access to personal information
- You need to have a policy and a workflow to ensure that only people with a business need have access
  - Ensure that terminations include access disablement
- You should have a documented method for reviewing and recertifying access periodically
- You need to have reasonable authentication and access control
  - Unique usernames
  - Good password practice (complexity, age, lockout)
Incident Management

- The WISP must include a requirement for the documentation of actions taken in response to a breach of security.
- You must also require a post incident review to change business practices or response activities to mitigate the risk of future incidents.
- The law implies the presence of an incident response plan, required by most regulations and standards.
- You should practice the plan regularly.
Vulnerability Management

- You need to ensure that virus protection is up-to-date and active
- You need to ensure that system software is reasonably up-to-date
- Your program / policy needs to include a statement regarding responsibility for vulnerability management and a methodology
- Best practice requires monitoring for updates and maintaining a comprehensive database of versions and vulnerabilities
- The methodology should include a risk assessment weighing deployment versus no deployment
Information Classification & Handling

- Your program needs to require encryption of personal information in three situations
  - Transmission across public networks
  - Transmission on wireless networks
  - When on “laptops and other portable devices”

- Challenges for many organizations will be cryptographic standards and key management
  - Who is responsible for selecting technology
  - Types of acceptable encryption
  - Where keys may be stored
  - When keys must be changed

- See NIST standards for guidance
Security Program Description Document

- All organizations would benefit from a high level document describing their security programs.
- The document should summarize the program’s goals and components without exposing the details.
- Such a document can help in a variety of situations:
  - Customer briefing
  - Partner reviews
  - Security audits
  - Compliance assessments
- Can serve as a starting point for building a security program.
Program Description Contents

- Organizational structure and security goals
- Policy structure and governance
- Risk assessment approach and high level risks
- Approach to management of access and identity
- Method for evaluation of partners
- Policy for data retention and destruction
- Philosophy of monitoring
- High level approach to managing and learning from incidents
- Applicable technical controls
- Training and awareness program
Summary

• You must have a written information security program to comply
• It is likely that this regulation is not your only compliance requirement
• Create a general program
• Ensure that the general program meets the specific regulatory requirements
  • Encryption
  • Partner management
  • Training
• Create a living program with management support that can adapt to changing risk and regulatory requirements