What Is A WISP?

... and how do I make one?

Richard E. Mackey, Jr.
Vice president
SystemExperts Corporation

Agenda

- Background
- Contents of the WISP
- Documentation of each component
- Create a framework
- Create a program description

Background

- The law is designed to prevent identity theft
- Requires all holders of personal information to implement procedural and technical safeguards to protect the data
- Requires many controls that are foreign to smaller companies
- Is consistent with controls required by industry standards (ISO 27000) and other regulations (HIPAA, Red Flag Rules)
- Companies' programs will be judged taking into account
  - The size, scope, and type of business
  - The resources available
  - The amount of stored data
  - The need for security and confidentiality of the both consumer and employee information

WISP

- The law requires organizations to have a formal comprehensive **w**ritten **i**nformation **s**ecurity **p**rogram (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

- Governance
- Risk assessment and treatment
- Security policy
- Education and training
- Identity management and access control
- Partner management
- Data lifecycle management

Technical Controls

- The law also requires policy and procedures for specific technical controls (some duplicated, some unique)
- Secure authentication and identity management
- Tight 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

Program Governance

- You must appoint one or more people responsible for program maintenance
  - Typically this falls to a multi-disciplinary team that understands business and technical risk
- You must establish security policies regarding the safeguarding of sensitive information
  - These policies may be part of your overall policy set, but must deal explicitly with how to protect confidential data
  - Policies should be managed by a responsible body, reviewed, and approved
- You must establish disciplinary measures for failure to comply with policy

Risk Management

- You must establish a methodology for assessing, documenting, and managing risk
  - Again, a multidisciplinary team should be involved
  - Risk needs to be assessed regularly, based on time and need
  - Many organizations, even big ones, do not have such a methodology in place
  - Required by PCI and HIPAA
  - Described in ISO 27001
  - 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

Data Lifecycle Management

- You need to limit the data you collect to the minimum necessary
  - This requires analysis of information assets and documentation of this policy
  - The most effective method is to never store it (when possible)
- You need to identify and locate all personal information
  - Paper, electronic, files, databases
- You need to retain information for the minimum time necessary
  - Policy needs to reflect the fact that the organization reviews information and destroys unnecessary personal information
- Best accomplished with 3 policies
  - Asset identification and cataloging
  - Data classification
  - Data handling and destruction

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)

Monitoring

- You need to monitor user access
- You need to monitor security controls to ensure they are effective
  - Inspect configurations
  - Test connections
- You need to detect unauthorized access
- Establish requirements for these activities and responsibility for these activities in policy

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 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

Encryption

- Your program needs to require encryption of personal information in three situations
  - Transmission across the Internet
  - 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
  - Relationship of encryption to particular types of data
  - Where keys may be stored
  - When keys must be changed

Build A WISP

- Follow this presentation as an outline of sections
- Check the regulation for specific requirements
- Analyze your policies for treatment of each of these areas
- Use ISO27002 as a guide in selecting and documenting controls
- Use this framework to build up your program over time

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 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

- The WISP is a requirement for the law
- Your existing security policies are a good starting point
- You need to ensure that your policies address unique requirements from the law
  - Data lifecycle
  - Encryption
- Make sure that your program includes regular risk assessment and review of control effectiveness
- Optional: Create a program description
- Wait for requirements for validation/audit