Technical and Procedural Challenges

Richard E. Mackey, Jr.
Vice president
SystemExperts Corporation

Agenda

- What to *do* versus what to *document*
- Background
- High level challenges
- A living program
- Common procedural weaknesses
- Technical challenges
- Keeping the program going

Background

- The law requires a security program
- The law requires general controls that all companies ***should*** already have in place
  - General security policy
  - Regular maintenance of program
  - Identity management
- It also requires specific controls that are peculiar to this law
  - Encryption
  - Data management
- The WISP captures what you **say** you do, you need to actually **do** it
- Practices based helping other organizations comply with regulations and contracts like HIPAA, GLB, and the Payment Card Data Security Standard (PCIDSS)

High Level Challenges

- Establishing a living security program
- Knowing and tracking where your information is
- Risk assessment
- Partner management
- Formal identity and access management
- Incident response and follow up
- Encryption
- Configuration management
- Vulnerability Management

Establishing A Living Security Program

- Security is a process not a project
- ISO 27001 and COBIT recommend a plan-do-check-act model
  - Identify assets
  - Assess risk
  - Implement controls
  - Monitor and assess effectiveness of controls
  - Improve
- Risk and effectiveness need to be reassessed regularly
- The program needs to be maintained under change control
- The program needs to be visible and high priority
  - Management attention
  - Part of regular training
- This is the cornerstone of good security

Managing Protected Data

- Many organizations never analyze their need for or the location of sensitive data – that has to change
  - Where is it?
  - Do we need it?
  - How long do we need it?
  - How can we securely dispose of it?
  - Is it adequately protected where it is?
  - Do we track its movement?
  - Would we know if it was compromised?
- The first step is understanding what you have

Data Management Guide

- Establish an information asset catalog
  - The type of data (specifically personal information)
  - The owners of the data (who can accept risk)
  - The custodians of the data (who is responsible for implementing controls)
  - Regular review
- Establish a data classification scheme
  - The sensitivity of the data (C, I, or A)
  - The regulatory requirements for the asset
- Establish data handling procedures
  - Where it may be stored
  - When it needs to be encrypted
  - How long it needs to be kept
- Establish destruction procedures
  - Particularly problematic for backups
  - Can also be problematic for service providers

Risk Management

- Unless your organization has been forced to comply with other regulations, it is likely you do not have a formal risk management methodology
- You need to assess the risk of compromise of the protected information
- Your method needs to be repeatable (see ISO 27001)
  - Documented method
  - Assess inherent risk (in absence of controls)
  - Assess residual risk (in presence of controls)
  - Select controls based on effectiveness of risk mitigation
- Must implement controls required by law
- Identify and accept all remaining risk
- Document results of risk assessments (critical for audit)

Partner Management

- Many organizations do a poor job of assessing the adequacy of partner security practices
- You need to have a methodology for management in place
  - Identify data sharing requirements
  - Eliminate unnecessary data sharing
  - Assess and document risk of sharing
  - Review (to the degree commensurate with risk) the practices of the partner
  - Establish contractual terms for data protection and right to audit
  - Establish incident response roles and plan
  - Regularly review practice of partners

Identity & Access Management

- You need to know precisely who has access to protected information
- You can only accomplish this if you have a well defined access granting process
  - You need an auditable request and approval workflow
  - You need to identify who can approve access (data owner, supervisor)
  - You need to recertify access at least annually
- …and a privilege removal process (on termination and job change)
  - Coordinate with HR
  - Notify interested parties

Access Management

- Require tight access controls on the applications, databases, and files that store the data
  - Require authentication
  - Define groups
  - Configure files and databases to only allow access to those groups
  - Check configuration regularly
- Ensure that employees do not circumvent controls
  - Training and awareness
  - Disciplinary process
- Technology help
  - IAM systems – help with workflow, reporting, recertification
  - Data loss prevention – help with preventing and detecting transmission and unauthorized copying

Incident Management

- You need a documented incident management procedure
  - Reporting mechanism and forms
  - Responsibility for review
  - Communications method for discussion
  - Specific role assignments for production decisions, communication with external parties
  - Requirements, responsibility, and procedures for notification of regulators, law enforcement, partners, and customers
  - Feedback to individuals who report incidents
  - Post incident review
  - Documented changes to procedure
- Supplemental requirements
  - Incident reporting policy
  - Training for employees and responders
  - Review and practice

Vulnerability Management

- The complexity of vulnerability management depends on the complexity of your environment
- For simpler environments, you may be able to automate
  - Virus protection
  - Firewall updates
  - System software update
- More complex environments
  - Routers
  - Switches
  - Web servers
  - Web applications
  - Database servers

Vulnerability Management Guide

- General advice: Simplify your environment and isolate your data
  - Use network segregation to reduce the number of systems and networks with personal data on them
  - This reduces the number of systems that need to be managed tightly
- Identify systems with connectivity and manage their state
  - Assign responsibility for vulnerability management
  - Monitor updates – automatically and manually
  - Assess risk
  - Deploy updates
  - Track state
  - Include all systems with access to the data (even remote system)
- Train employees to understand and implement controls
  - Firewalls
  - Virus protection
  - Acceptable use of systems

Encryption

- You need to implement encryption for
  - Internet, wireless networks, "laptops and other portable devices"
- Choices to consider
  - Laptops: Windows file system encryption, TrueCrypt, PGP, other commercial products
  - Thumbdrive encryption – same list w/o Windows
  - PDAs, phones? – best to avoid the problem
  - Internet – SSL, VPN (ipsec, SSL)
  - File transfer - (scp, sftp)
  - Wireless - WPA2
- Establish a method to change keys before you start
  - Backup
  - Partner

Summary

- You need to implement the controls described in your WISP
- The law is not overly prescriptive (unlike PCI), but there is no sense in taking short cuts
- The best approach is to build a living sustainable program
  - Management support
  - Regular formal review
  - Integration into everyday operations
- Your best cost control is isolation and data elimination
- Know your program and be ready to defend your choices