Building Blocks of Data Privacy

John P. Tomaszewski
Seyfarth Shaw LLP
The Building Blocks

- Corporate Governance
- COSO Framework
- COBIT Framework
- Privacy Program Components and Structure
Corporate Governance

The Triumvirate
Administrative
Technical
&
Procedural
Safeguards

Policy
(General management statements)

Standards
(How to implement policy)

Processes
(Specific controls)

Procedures
(Step by step instructions)
Corporate Governance

Policy is generally “End State” oriented

Senior Management Endorsement/Approval
• Need a “Responsible Officer”

Alignment Between Business Objectives & Security Needs
• The most secure computer is encased in plastic… and at the bottom of the ocean.

Integration Between Executive & Line Management
• Have to have the folks building stuff know what their obligations are.
Corporate Governance

Technical Standards
• Password length & complexity
• Encryption requirements (at rest & in transit)
• PC configuration standards (e.g. disable USB ports, etc.)
• Network configuration standards

Administrative Standards
• Metrics
• Training
• Audit

Procedural Standards
• Product Requirements
• Development Methodology
• Role-based access controls (both people AND machines)
Corporate Governance

Access credential Provisioning
Identify responsibility for business processes
Accountability (read: Enforcement)
Training
• Onboarding
• Annual
• Other periodic as necessary (e.g. security engineers need more)
Vendor management
• contracts
• due diligence
Event Management
Corporate Governance

**Procedures**
(step by step instructions)

**Technical Procedures**

Standard Operating Procedures ("SOP")
- Standing up new products & services
- Transitioning customers across services
- Personal Device connectivity/monitoring
- Data Loss Prevention policies (monitoring & blocking network traffic)

Configuration Baselines
- Collection Limitations (only collect what you need)
- 3rd Party Vendor Tracking Tech on websites
- Encryption implementation requirements (salting, hash algorithms, etc.)

Database architecture
- Metatagging data for sensitivity classification
**Data Privacy**

**Controlling Data**
Like any other “control.”

Control: a proactive step taken to accomplish an objective

- Controls attain Objectives.
- Objectives address Risks.

Controls are best developed within a framework.

Begin with **COSO** - a general control framework.

Treadway Commission’s **Committee Of Sponsoring Organization**
COSO Internal Control Framework
After establishing general controls (COSO)
Time to get detailed (COBIT)

COBIT Framework
Control Objectives for Information Technology
An IT governance framework
Process-oriented

It starts with your Business Goals.
COBIT Framework

- **Information Criteria**
  - Determines Parameters
- **Governance Drivers**
  - Determines Availability
- **IT Resources**
  - Optimize Use Of
- **Business Goals**
  - Achieve Quality Of
- **The Process**
  - PLAN & ORGANIZE
  - MONITOR & EVALUATE
  - DELIVER & SUPPORT
  - ACQUIRE & IMPLEMENT
Putting it all together
Privacy Program Components

DEFINE

TEST

MANAGE
The Nature of Information

Confidential Information

Internal

Proprietary

Public

Private

Note: overlaps are a function of time
Define Asset

What are we Controlling?

Data → Information → Knowledge → Intelligence

Inventory managed by each division/business unit
• Know what you use and how you use it
• Data flow diagrams
• Data classification standard
Privacy Programs

Privacy Statement/Policy:
• Data storage policy
• Data access policy
• Associate training policy
  • Monitoring and compliance policy
  • Data classification standard
  • Data disclosure standard
    • Access Management Process
    • Data disclosure process
• Associate handbook policy
  • Confidential information and trade secret policy
Privacy Programs

Privacy Policy Structure

• Clear & Conspicuous
• Content:
  • How you collect data
  • What you do with the data (be specific if possible)
  • Data disclosure statement
    • When you disclose to third parties
    • What categories of data you disclose to third parties
    • Who you disclose data to
    • Disclosure processes
  • What kind of security is in place
• Review (periodically – business models change)
Privacy Programs

Privacy Policy Delivery
• At time of relationship formation
• Annually
• By paper or electronically
  • Reasonable expectation of “actual notice”
  • Watch out for E-SIGN/UETA

Consent
• Include language in Terms & Conditions/Consumer Agreement
• Opt-in: easier to manage
• Opt-out: preferred by businesses
  • General opt-out hard to manage
  • The more specific the options, the easier to manage in the long run
• Unsubscribe processes for email
• Be SURE you get the language right
• Permissions follow data
Privacy Programs

Infrastructure

• Continuing Education
  • Awareness Training
  • Classes for security applications

• Effective tools
  • Easy to understand policies, definitions, and standards
  • Management support for privacy related decisions (even if deployment is delayed)

• Privacy Assessments
  • What is the risk? Is it Data, Information, Knowledge, or Intelligence that needs to be protected?

• Product design & review
  • Make sure the product has privacy as a business requirement
Privacy Programs

Data Flow and Gap Analysis
Annual privacy assessment (has the gap changed)
Internal Audit
3d Party Audits
Certification Programs
Privacy Programs

Designate responsible party in senior management
Track risks as identified in testing
Quarterly reporting to executive management
Privacy Programs

Incident Response

• Establish security protocol and escalation process
  • What constitutes a triggering event?
  • Who, what, when, and how to notify?

• Include multiple parties
  • Legal
  • PR
  • Media Relations
  • Investor Relations
  • Operations
  • Technical Teams
Incident Response

• Security Breach Notice Requirements (in 20+ states)
  • Unauthorized access/acquisition
  • Computerized data (some states don’t require)
  • Compromising the security, confidentiality or integrity
  • Data “owners” must notify consumers in the “most expedient time possible.”
  • “Processors” must notify “Owners” immediately
  • Many times, no harm is necessary to trigger notice requirements
Employee’s Role

• In order to prevent accidental or intentional loss or disclosure of confidential information, companies must be committed to providing a secure environment.
• Managers are responsible for ensuring employees are aware of what information is considered especially sensitive and how confidential information is to be handled.
• Confidential information is secured when not in use.
• Confidential information if shredded when disposed of.
Question & Answer

John Tomaszewski
Seyfarth Shaw
jptomaszewski@seyfarth.com
(713) 860-0088