CIPM Privacy Summary*

Richard C. Hsu
Shearman & Sterling
rhsu@shearman.com

Governance **Life Cycle**

Mission Statement

- "Communicates to stakeholders"…
- "Across all your different business lines" ….
- "where the organization stands on privacy"

Privacy Strategy

- Achieve Business Alignment
- Identify Stakeholders (IT, IS, Internal Audit, Comms, Procurement, Learning & Development)
- Structure Privacy Team
- Rationalize Data Protection

Governance Models

- Centralized
- Decentralized
- Hybrid

Privacy Framework

- Develop Business Case
- Perform Gap Analysis
- Review and Monitor
- Communicate

Assess

5 Maturity Levels

1. Optimized
2. Managed
3. Defined
4. Repeatable
5. Ad Hoc

Privacy Office

- Understand internal policy of organization including formal written policy

9 Elements of Data Inventory

1. Nature of Repository
2. Owner of Repository
3. Location of Repository
4. Volume of Information
5. Format of Information
6. Use of Information
7. Type of Information
8. Where Data is Stored
9. International Transfers

Privacy Players

- Human Resources
- Marketing
- Finance
- Legal and Compliance
- Info Technology
- Info Security
- Internal Audits
- Third Party Vendors

Internal Audit and Risk Management

- Privacy Impact Assessments (PIA)
- CobiT
- Independent of Management

Protect

Privacy by Design

1. Proactive, not Reactive
2. Privacy as Default Setting
3. Privacy Embedded into Design
4. Positive Sum, not Zero Sum
5. End-to-End Security
6. Visibility and Transparency
7. Respect for User Privacy

Technical / Physical Controls

- ISO 27001 and 27002
- PCI DSS
- Layered Approach

Info Security Practices

- US-CERT IT Security Essential Body of Knowledge (EBK)

Data Life Cycle Management (DLM)

1. Enterprise Objectives
2. Minimalism
3. Simplicity
4. Adequacy of Infrastructure
5. Information Security
6. Authenticity and Accuracy
7. Retrievability
8. Distribution Tools
9. Auditability
10. Consistency of Policies
11. Enforcement

Respond

Steps in a Data Breach

1. Isolate
2. Contain
3. Preserve
4. Establish
5. Document

Key Roles

- Information Services
- Legal
- Human Resources
- Marketing
- Business Development
- Communications/PR
- Union Leaders
- Finance
- CEO
- Customer Care

Response Team

1. Internal Announcement
2. External Announcement
3. Regular Notification
4. Letter Drops
5. Call Center Launches
6. Remediation Offers
7. Progress Reporting
8. Response Evals and Mods

Whether to Notify

- Nature of Data Breach
- Number of Individuals Affected
- Likelihood info is accessible and usable
- Likelihood breach may lead to harm
- Ability to mitigate risk of harm

Sustain

Metrics Life Cycle (*Six Sigma*)

Stage 1: Identify Audience

- Primary
- Secondary
- Tertiary

Stage 2: Define Metric Owner

Stage 3: Select Metrics Criteria

- Objective / Subjective
- Qualitative / Quantitative
- IT Metrics + Quantitative Measurement
- Static / Dynamic
- Absolute / Relative
- Direct / Indirect

Stage 4: Collect Data

Stage 5. Analyze

- Business Resilience
- Trends
- ROI

Monitor

- Regulatory and Legal Changes
- Compliance and Risk
- Environment (external attacks + internal threats)

Audit

- 1st Party Audit
- 2nd Party Audit
- 3rd Party Audit

Communicate

- Internal / External
- Education vs. Awareness

*Adapted from IAPP CIPM Privacy Certification