PwC Advisory

March 23, 2007

How privacy affects the IT auditor and security manager: Beyond reductionism.*

ISACA/IAPP 2007 Privacy Panel, San Francisco, CA

Alex Fowler, Director
PricewaterhouseCoopers

*connectedthinking

Utilize information.
Just what you need.
Mostly non-identifying.
Focus on people.

Marketplace Realities

New Laws

- Since 1998, 80+ privacy laws in over 50+ countries were passed in areas of financial privacy, data protection, telemarketing/fax, spam/web, and security breaches

New Business Demands

- Consumer expectation of privacy with Financial Institutions has dramatically changed; more opt-outs
- Loss of Trust & Privacy: 33.4M Americans have been victims of identity theft since 1990; 50M+ received security breach notices in 2005

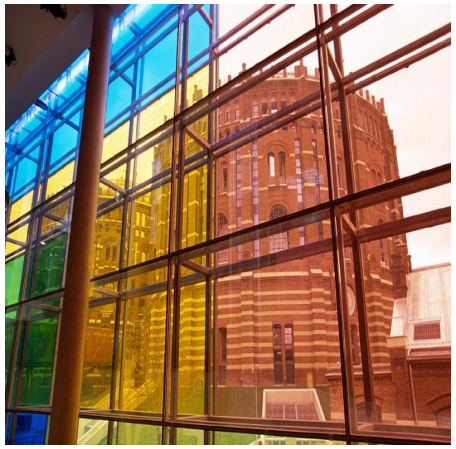
New & Heightened Security Threats

- Number of security-related incidents and sophistication of attacks are increasing
- Public awareness is heightened by new breach notification requirements

New Regulator & Industry Focus on Privacy & Data Protection

- Regulators are active globally and asking tougher questions of data management, information security and control environments
- Companies are developing long-term strategies and frameworks to address privacy and data protections

Privacy Landscape: Looking Out



20-30% of Global 1000 will suffer exposure due to privacy mis-management.

(Gartner)

- Complex cross-jurisdictional regulatory environment
- Privacy is one of many of laws impacting organizational trust and brand
- Cultural and ethical differences shape concepts of privacy for customers, partners, employees, and competitors
- Rapid technological change
- Intense media pressure on privacy breaches / missteps
- Disproportionate legislative pressure compared with market pressure

Privacy Landscape: Looking In

Costs to recover from privacy mistakes will range from $5 - $20 million.

(Gartner)

- Decentralized business structures
- Rapid technological change
- Uncertainty associated with data handling practices
- Limited resources available for non-revenue-generating activities
- Pressure to achieve cost-savings across the board
- Tendency to confuse security as privacy efforts
- Undefined ROI for privacy
- Complexity in measuring performance associated with privacy

2004: The Year American's Opted Out

"Don't Call. Don't Write. Let Me Be"

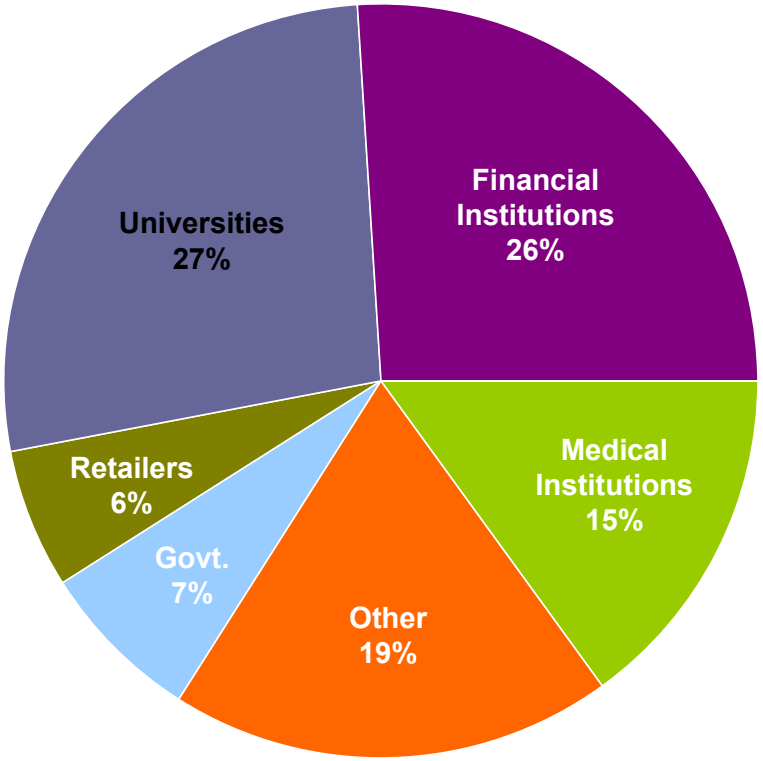
- A privacy sensitive American family may spend between $200 and $300 and many hours annually to opt-out
- 100+ million phone numbers have been placed on the Do Not Call Registry

Opting Out Options

- Phone Solicitations
- Direct Mail Solicitations
- Unsolicited E-mail
- Credit Card Solicitations / Credit Freeze
- Web-based Ad Serving
- What's next? Real Estate Filings, Birth Certificates, DMV Databases

2005-2007: An Era of Security Breach Notifications

- Public bombarded with reports of data breaches (i.e., ChoicePoint, UCLA, t.j.maxx, etc.)
- Nearly 150 million records containing PII have been exposed in breaches since February ‘05
- 20% of consumers who received notices reported severing ties with organization
- 35 state laws introduced, Congress expected to pass Federal legislation in ‘07



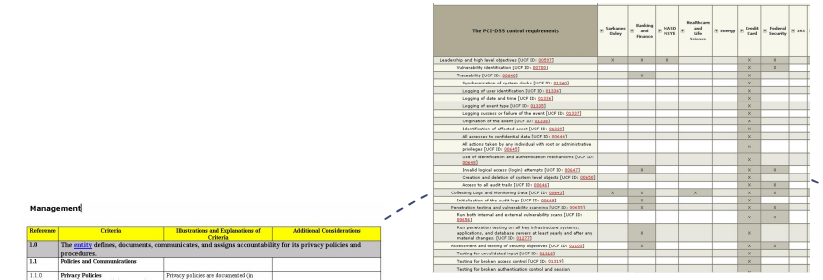
Security Breach Notices by Types of Institution

Source: California Office of Privacy Protection, 2005

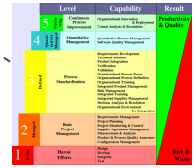
Organizational Response: Reductionism

Reductionism

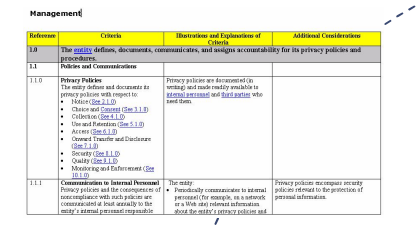
- Privacy reduced and addressed one part at a time
  - -- principles
  - -- compliance requirements
  - -- business processes
- Explosion in IT focus on frameworks, guidelines, standards, taxonomies, etc.
- Unified theories of compliance and “cross walking”



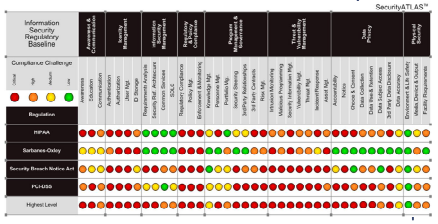
ITCi Unified Compliance



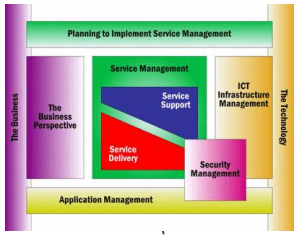
CMMI



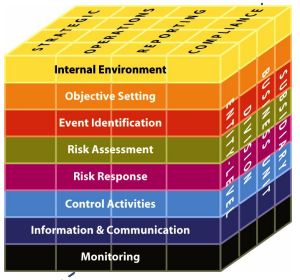
Generally Accepted Privacy Principles



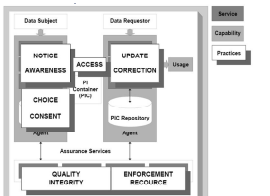
PwC SecurityATLAS



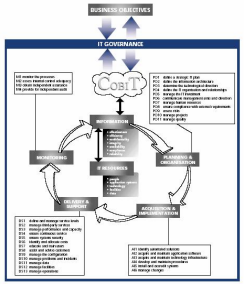
ITIL



COSO ERM



ISTPA Privacy Framework



CobiT

Disconnected Privacy and Compliance

HHS

- HIPAA Privacy Rule
- HHS only acts on complaints
- 25,000 complaints filed to date; no action taken

Healthcare Institution

- Organizations spend $ millions to comply
- Required extensive change management
- Reacts to events

Patient

- Patient signs a notice form
- Patient has to decide whether rights have been violated

What's the point of a compliance effort if it doesn't reduce the chance of an enforcement action or build trust with your customer?

Utilize information.
Just what you need.
Mostly non-identifying.
Focus on people.