

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

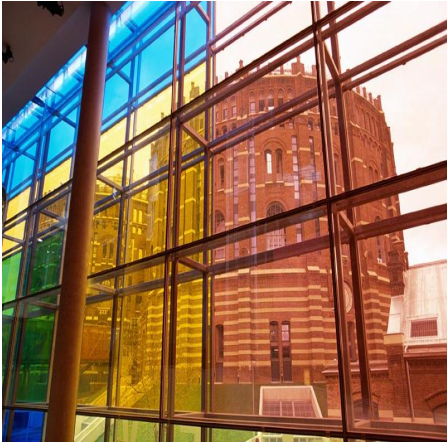
New & Heightened Security Threats

- 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”

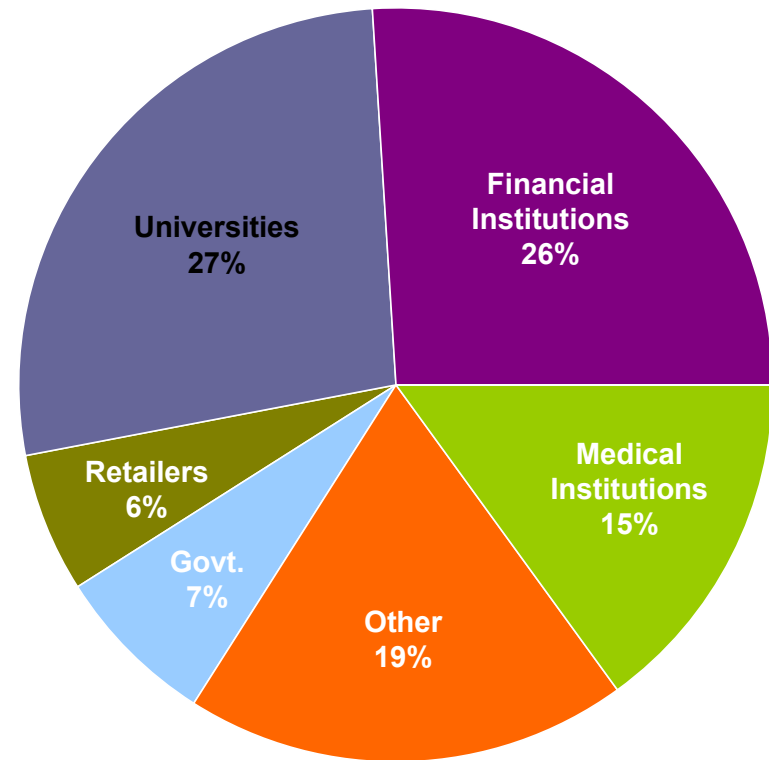
- A privacy sensitive American family may spend between \$200 and \$300 and many hours annually to opt-out
- 100+ million phone numbers have been placed on the Do Not Call Registry

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

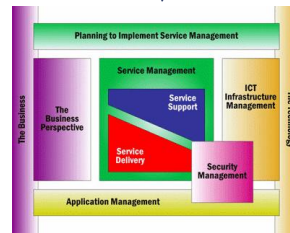
Reductionism

- 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”

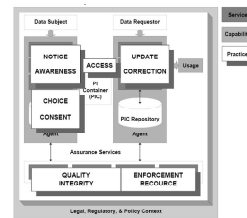
Management

Reference	Criteria	Illustration and Explanation of Criteria	Additional Considerations
1.0	The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.		
1.1	Policies and Communications		
1.1.0	Privacy Policies The entity defines and documents its privacy policies with respect to: • Personal Data (Sec 1.1.0) • Choice and Consent (Sec 1.1.1) • Collection (Sec 1.1.2) • Use and Disclosure (Sec 1.1.3) • Access (Sec 1.1.4) • Opened Transfer and Disclosure (Sec 1.1.5) • Security (Sec 1.1.6) • Monitoring and Enforcement (Sec 1.1.7)	Privacy policies are documented, developed, and made readily available to internal and external parties who need them.	
1.1.1	Communication to Internal Personnel Privacy policies and their consequences of non-compliance with such policies are communicated to those entities to which the entity's external personnel report.	The entity's privacy policies are communicated to internal personnel (for example, to a subject's supervisor) to ensure that the entity's policies are understood.	Privacy policies do not replace security policies or other policies that apply to the protection of personal information.

Generally Accepted Privacy Principles



ITIL

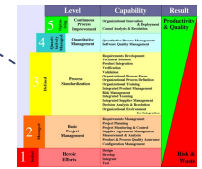


ISTPA Privacy Framework

The PCI DSS national requirements

	Technical	Physical	Personnel	Operational	Information Security	Other
Leadership and high-level objectives (COP 1)	X	X	X	X	X	X
Information security (COP 2)	X	X	X	X	X	X
Access control (COP 3)	X	X	X	X	X	X
Cardholder data security (COP 4)	X	X	X	X	X	X
Encryption (COP 5)	X	X	X	X	X	X
Monitoring and testing (COP 6)	X	X	X	X	X	X
Security policies and procedures (COP 7)	X	X	X	X	X	X
Vendor management (COP 8)	X	X	X	X	X	X
Penetration testing (COP 9)	X	X	X	X	X	X
Incident response (COP 10)	X	X	X	X	X	X
Disaster recovery (COP 11)	X	X	X	X	X	X
Secure development (COP 12)	X	X	X	X	X	X
Supply chain risk management (COP 13)	X	X	X	X	X	X
Information security (COP 14)	X	X	X	X	X	X
Access to cardholder data (COP 15)	X	X	X	X	X	X
Cardholder data security (COP 16)	X	X	X	X	X	X
Cardholder data security (COP 17)	X	X	X	X	X	X
Cardholder data security (COP 18)	X	X	X	X	X	X
Cardholder data security (COP 19)	X	X	X	X	X	X
Cardholder data security (COP 20)	X	X	X	X	X	X
Cardholder data security (COP 21)	X	X	X	X	X	X
Cardholder data security (COP 22)	X	X	X	X	X	X
Cardholder data security (COP 23)	X	X	X	X	X	X
Cardholder data security (COP 24)	X	X	X	X	X	X
Cardholder data security (COP 25)	X	X	X	X	X	X
Cardholder data security (COP 26)	X	X	X	X	X	X
Cardholder data security (COP 27)	X	X	X	X	X	X
Cardholder data security (COP 28)	X	X	X	X	X	X
Cardholder data security (COP 29)	X	X	X	X	X	X
Cardholder data security (COP 30)	X	X	X	X	X	X
Cardholder data security (COP 31)	X	X	X	X	X	X
Cardholder data security (COP 32)	X	X	X	X	X	X
Cardholder data security (COP 33)	X	X	X	X	X	X
Cardholder data security (COP 34)	X	X	X	X	X	X
Cardholder data security (COP 35)	X	X	X	X	X	X
Cardholder data security (COP 36)	X	X	X	X	X	X
Cardholder data security (COP 37)	X	X	X	X	X	X
Cardholder data security (COP 38)	X	X	X	X	X	X
Cardholder data security (COP 39)	X	X	X	X	X	X
Cardholder data security (COP 40)	X	X	X	X	X	X
Cardholder data security (COP 41)	X	X	X	X	X	X
Cardholder data security (COP 42)	X	X	X	X	X	X
Cardholder data security (COP 43)	X	X	X	X	X	X
Cardholder data security (COP 44)	X	X	X	X	X	X
Cardholder data security (COP 45)	X	X	X	X	X	X
Cardholder data security (COP 46)	X	X	X	X	X	X
Cardholder data security (COP 47)	X	X	X	X	X	X
Cardholder data security (COP 48)	X	X	X	X	X	X
Cardholder data security (COP 49)	X	X	X	X	X	X
Cardholder data security (COP 50)	X	X	X	X	X	X

ITCi Unified Compliance

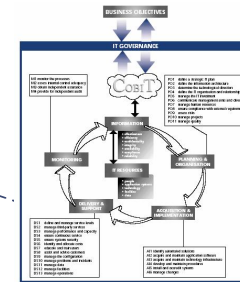


CMMI

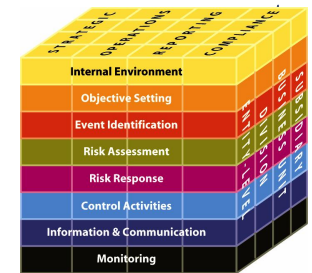
Information Security Regulatory Checklist

Information Security Regulatory Checklist	Regulatory	Industry	Academic	Government	Healthcare	Financial	Energy	Transportation	Manufacturing	Retail	Education	Non-Profit	Other
Compliance Challenge	●	●	●	●	●	●	●	●	●	●	●	●	●
Regulation	●	●	●	●	●	●	●	●	●	●	●	●	●
Standalone Only	●	●	●	●	●	●	●	●	●	●	●	●	●
Security Research Model Art	●	●	●	●	●	●	●	●	●	●	●	●	●
Public	●	●	●	●	●	●	●	●	●	●	●	●	●
Hybrid Level	●	●	●	●	●	●	●	●	●	●	●	●	●

PwC SecurityATLAS



COBIT



COSO ERM

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.