Citation Key

for more information see: http://open.umich.edu/wiki/CitationPolicy

Use + Share + Adapt

{ Content the copyright holder, author, or law permits you to use, share and adapt. }

Public Domain – Government: Works that are produced by the U.S. Government. (USC 17 § 105)

Public Domain – Expired: Works that are no longer protected due to an expired copyright term.

Public Domain – Self Dedicated: Works that a copyright holder has dedicated to the public domain.

Creative Commons – Zero Waiver

Creative Commons – Attribution License

Creative Commons – Attribution Share Alike License

Creative Commons – Attribution Noncommercial License

Creative Commons – Attribution Noncommercial Share Alike License

GNU – Free Documentation License

Make Your Own Assessment

{ Content Open.Michigan believes can be used, shared, and adapted because it is ineligible for copyright. }

Public Domain – Ineligible: Works that are ineligible for copyright protection in the U.S. (USC 17 § 102(b)) *laws in your jurisdiction may differ

{ Content Open.Michigan has used under a Fair Use determination. }

Fair Use: Use of works that is determined to be Fair consistent with the U.S. Copyright Act. (USC 17 § 107) *laws in your jurisdiction may differ

Our determination **DOES NOT** mean that all uses of this 3rd-party content are Fair Uses and we **DO NOT** guarantee that your use of the content is Fair.

To use this content you should **do your own independent analysis** to determine whether or not your use will be Fair.

Self-Regulation and Privacy

510 - Data Security and Privacy: Legal, Policy, and Enterprise Issues
University of Michigan School of Information
Week 7

New Business Roles

- Chief Privacy Officer
- Chief Security Officer
- Actual titles vary
- Can be same person in small company
- May hold other jobs
- CPO typically more in line of business role or came from that background; CSO in tech role

Privacy Programs

Homonyms in Privacy

- Two meanings for “Privacy Policy”
- Internal structures
- External statements

Common Element

- Personal information
- Personally Identifiable Information (PII)
- Elements of PII vary
- Some can be disputed
  - IP number
    - See EU Article 29 proceedings

Internal Privacy Policy

Privacy Plan Norms

- Must be consistent with
  - Business operations
  - Legal compliance framework
  - Management goals
  - Organizational culture
  - Systems architecture
- Programs, Policies, Procedures

Privacy Plan Organization

- Boards of Directors
- Senior management
- Internal management
- Operational staff

Looking Familiar So Far?

- Internal privacy policies, programs, procedures track security ppp

Differences

- Privacy narrower; often within security
- Privacy focuses more on issues surrounding specific types of information
- Privacy and security may have own specific statutory definitions to consider
- Statutes/regulations generally more detailed with security

Link Privacy and Security PPP

- Avoids duplication of effort
- PII does affect considerations; *e.g.*,
  - Add tracking of whether PII
  - Add consumer preferences

External Privacy Policy

Public Statements

- Statements of protections given to personal data
- Reasons
  - Statutory requirement
  - Customer service
- Formats
  - Print
  - Web sites

Customer Service

- Statements of how will treat data
- No broad law requiring but must follow if posted
- Changing policy may create problems

Consumer Issues

- Readable
- Understandable
- Mechanism to force/encourage acknowledgment
- Notice mechanism - Platform for Privacy Preferences (P3P)
  - Standard format
  - Retrieved and interpreted by browsers (IE)
  - Automate decisions
  - Avoids having to read notices at every site

Private Sector Programs

Seal Programs

- To confer level of trust on the part of consumers and businesses
- BBB
- TRUSTe
- Chamber of Commerce

Self-Regulation Standards

- Individual seal programs
- Joint effort
  -

Self-Regulatory Principles for Online Behavioral Advertising, July 2009.

http://www.ana.net/advocacy/getfile/15279

Developed by:

- American Association of Advertising Agencies
- Association of National Advertisers
- Council of Better Business Bureaus
- Direct Marketing Association
- Interactive Advertising Bureau

Joint Effort

- Education
- Transparency
- Consumer control
- Data security
- Material changes
- Sensitive data
- Accountability

Professional Certifications

- International Association of Privacy Professionals
  - Certified Information Privacy Professional (CIPP)
  - CIPP/G – Government
  - /C –Canada
  - /IT – Information

Public-Private Program

COPPA

- 15 USC 6501 *et seq*; 16 CFR 312
- Operate website or online service that gathers PII and is aimed at children or have actual notice of use by children
- Prominent privacy notice with operators, kinds of info, how will use and disclose
- Reasonable for activity
- Parental choice and review; sliding scale
- Safe Harbor

COPPA Safe Harbor

- Industry group guidelines
- Submit for FTC approval
  - Must track COPPA requirements
  - Must have enforcement mechanism
- Approved organizations
  - Children's Advertising Review Unit of BBB
  - Entertainment Safety Rating Board
  - TRUSTe
  - Privo
- No actions for failure to enforce

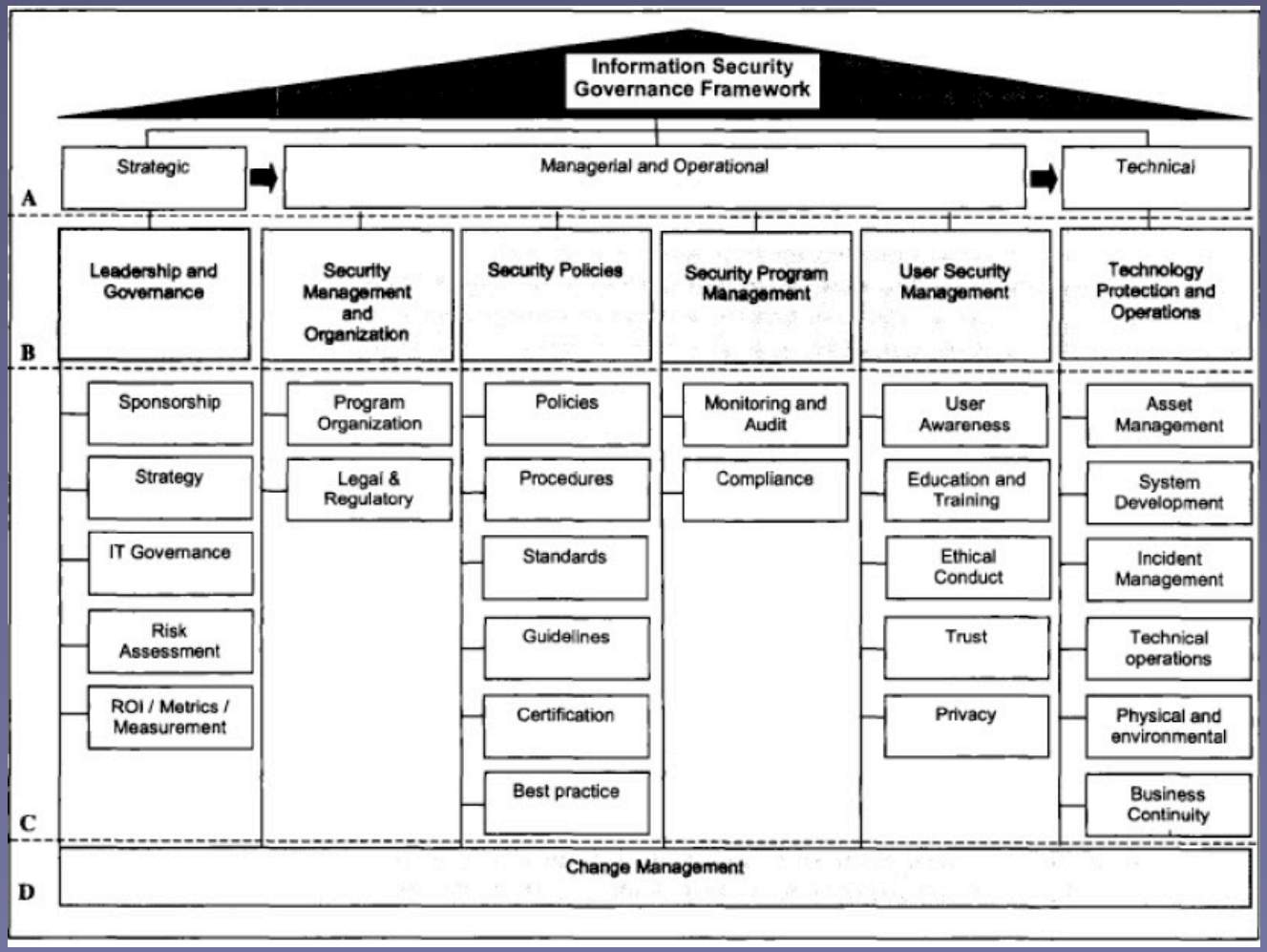
COPPA Enforcement

- Ohio Art
  - “Get your parents’ consent” with nothing more
- Hershey Foods
  - Form for parents but no enforcement
- Xanga.com
  - General interest site but actual knowledge; 1.7 million accounts had birthdates showing less than 13
- Imbee.com
  - Information gathered before parental notice and kept if parent did not respond
- Sony BMG
  - Multiple violations related to music fan site

Links

- http://www.youtube.com/watch?v=MxG2J3bf1BQ
- http://www.wired.com/threatlevel/2009/12/heartland-guilty-plea/

Infosec Governance



PD-INEL

A de Veiga and J. Eliot, An Information Security Governance Framework, Information Systems Management, Fall 2007 24:361-72, p, 363