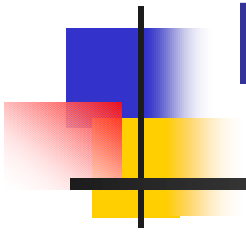


Privacy & Security Laws

Kate Wakefield, CISSP/MLS/MPA

Information Security Analyst

Kwakefield@costco.com

Roadmap

- Privacy & Data Security
  - Legal landscape in United States
  - Key Issues
  - International standards
  - Best Practices
- Next hour: HIPAA Security Regulations
  - Who is impacted – not just health care entities.
  - Specific requirements of the regulations.

About Your Presentor

- Those pesky initials (CISSP, MPA, MLS).
- Currently focused on Privacy and Information Security compliance at Costco Wholesale.
- Costco is a Covered Entity for the Pharmacy, as well as in the 'Employer Context'.
- Member of IAPP, IEEE, ABA, Board member for ISSA Puget Sound Chapter.
- Teach in Information Security BA program at ITT Technical College, sometimes at Bellevue Community College, previously at ESU – KS.

Standard Disclaimers

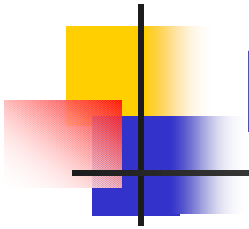
- As they say in Internetish “IANAL” – to obtain legal advice please consult a lawyer who specializes in privacy law.
- My opinions are my own -- not my employers’.
- To do HIPAA Security right, you must do a risk assessment of your organization and assess its risk tolerance, technical expertise, and sensitivity of the data you handle daily.

Legal Landscape for Privacy

- No single overarching Privacy Law in the United States *(yet – 108th Congress has some proposed legislation).*
- Sector-specific regulation:
  - Finance: Gramm-Leach-Bliley
  - Healthcare: HIPAA
- State laws ...
  - Several states have their own Privacy Laws.
  - California SB 1386 – Disclosures.

Key Issues

- Internet data collection.
- Data combination.
- Protection of Personally Identifiable Information (both online & offline).
- Protecting children's privacy (COPPA).
- Preventing identity theft.



Early legislation

- Freedom of Information Act (1966).
- Fair Credit Reporting Act (1970)
  - First legislation to refer to “the consumer’s right to privacy.”
  - Scope limited to consumer reporting agencies.
  - See also Consumer Credit Reporting Reform Act (1996)

Code of Fair Info Practices

- 1970 study of computerized record-keeping practices commissioned by Elliot Richardson of HEW.
- Established a “Code of Fair Information Practice” comprised of five principles:

1. There must be no personal data record-keeping systems whose very existence is secret.
2. There must be a way for a person to find out what information about the person is in a record and how it is used.

Code of Fair Info Practices

3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.
4. There must be a way for a person to correct or amend a record of identifiable information about the person.
5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.

Privacy Act of 1974

- Embodied the Principles from the HEW report into law, guaranteeing three rights (for goverment records):
  - Right to review your own records.
  - Right to amend that record if it is inaccurate, irrelevent, untimely, or incomplete.
  - The right to sue the government for violations of the statute including permitting others to see your records unless specifically permitted by the Act.

FTC Fair Information Practice

- “Privacy Online: a Report to Congress” published in 1998 by the FTC.
- Represents a distillation of “model codes that represent widely-accepted principles concerning fair information practices.”
- Outlines Five Fair Information Practice Principles.

Fair Info Practice Principles

- Notice / Awareness
- Choice / Consent
- Access / Participation
- Integrity / Security
- Enforcement / Redress

Internet Privacy

- Consumer privacy is governed by the Privacy Policy posted on a company's website.
- The Privacy enforcement agency is the FTC.
- High profile cases:
  - Doubleclick
  - Amazon.com
  - Eli Lilly
  - The Gap

COPPA

- Requires website operators which collect personal info from children under 13 to follow six guidelines:
  - Provide clear notice of info collected & disclosure practices.
  - Obtain ‘verifiable consent’ from parents prior to collection.
  - Provide a means for parents to review info collected from their child.
  - Allow parents to refuse to permit use of their child’s info.
  - Not to condition participation or access upon provision of more info than is necessary.
  - Setup and maintain procedures to protect the confidentiality, security, and integrity of personal info collected from kids.

COPPA Implications

- Minimum Necessary principle applies to collection of children's info.
- Even if your site is not primarily aimed at children, if it may gather their info, you must comply with law.
- Several 'Safe Harbor' programs have been approved: TRUSTe Seal, Entertainment Software Rating Board, and Children's Advertising Review Unit of the Council of Better Business Bureaus.
- For more info, including a compliance kit, check: http://www.ftc.gov/bcp/conline/edcams/coppa/intro.htm

Gramm-Leach-Bliley

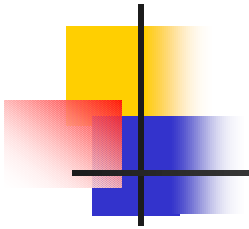
- Applies to financial institutions (banks, securities, and insurance companies) with direct consumer relations.
- Key characteristics:
  - Allows sharing of info among affiliates.
  - Requires notice of privacy practices to consumers.
  - Limit sharing of ‘nonpublic’ personal info with non-affiliated third parties, unless ‘opt out’ is offered.
  - Limit reuse and redisclosure by third parties.
  - Limit disclosure of account numbers for marketing.

GLB Requirements

- GLB specifically requires three types of privacy notices: initial, annual, and revised. Guidance on wording is given.
- Prior to disclosing nonpublic personal info, opt-out notices must be provided.
- Development of a comprehensive written info security program with administrative, technical, and procedural safeguards.
- Also required to exercise due diligence in selecting service providers.

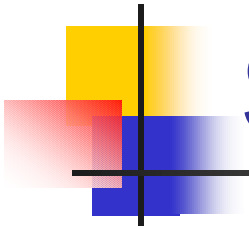
HIPAA Privacy

- Finalized on 8/14/2002 (guidance 12/3/2002). Compliance date 4/14/2003.
- Requires permission to disclose ‘Personally Identifiable Health Information’ except in limited treatment/payment situations.
- Notice of Privacy Practices to consumer.
- Business Associate agreements w/partners.
- Detailed tracking of any disclosures.



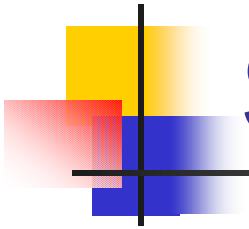
HIPAA Security

- Finalized 2/20/2003, compliance 4/15/2005.
- Detailed specifications for protecting the integrity and confidentiality of data.
- Lists administrative, technical, and physical safeguards which must be implemented.
- Softened requirements in some areas by making some specifications “addressable”.
- Key requirement is a risk assessment to determine how best to comply with the rules.



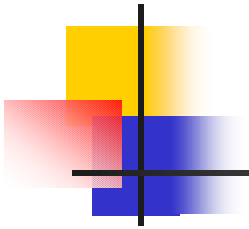
Sarbanes-Oxley

- Additional reporting requirements for publicly traded companies.
- Separation of duties performed by audit firm vs other companies.
- Distinct audit responsibilities.
- Audit of financial systems security and integrity is implied.



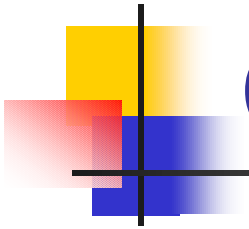
State Laws

- Calif. SB-1386 Database Disclosures
  - Requires companies which do business in California to report incidents where databases are compromised.
- States with their own Privacy Laws: CA, MA, NY, TX, VA, and WA.
- http://www.epic.org/privacy/bill_track.html



International Standards

- OECD Guidelines (1980)
- European Union Directive
- Canada's PIPEDA



OECD Guidelines (1980)

- Collection Limitation Principle
- Data Quality Principle
- Purpose Specification Principle
- Use Limitation Principle
- Security Safeguards Principle
- Openness Principle
- Individual Participation Principle
- Accountability Principle

EU Directive 95/46/EC

- Effective date 10/24/1998.
- Protects personal data by requiring data to be:
  - Processed fairly and lawfully,
  - Collected for specified, explicit, and legitimate purposes,
  - Adequate, relevant, and not excessive in relation to the purposes for which they are collected.
  - Accurate and, where necessary, kept up-to-date.
  - Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data was collected or for which they are further processed.

Data Protection Directive

- Protects individual data to a much higher degree than U.S. legislation.
- Bars transfer of personal data to countries with less stringent safeguards (such as the United States).
- Led to Safe Harbor agreement.
- Can also be handled through contract language promising adequate safeguards or by having the individual agree to transfer.

Safe Harbor Principles

- Notice
- Choice
- Onward Transfer
- Security
- Data Integrity
- Access
- Enforcement

Best Practices for Privacy

- Privacy Policy
- Privacy Officer
- Risk Assessment
- Security Policy
- Security Awareness
- Website ‘Seal’ Programs

Privacy Policy

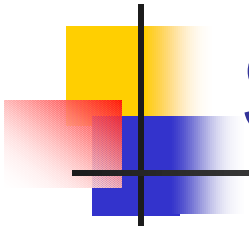
- Develop an organization-specific Privacy Policy, accounting for applicable laws.
- Appropriate legal review of Policy.
- Post the policy on the corporate website and at customer contact points.
- Translate policy to specific procedures.
- Review points of data collection, add acknowledgements where necessary.

Privacy Officer

- Important to have an individual who is accountable for privacy practices.
- Combination of expertise in legal, business, marketing/PR, and security.
- Can spearhead development of a privacy & data security committee.

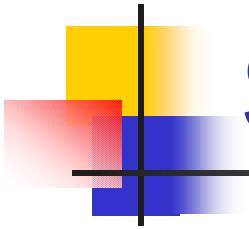
Risk Assessment

- Many of the laws (particularly GLB & HIPAA) judge compliance on what is appropriate for the size and complexity of the organization, and the nature and scope of its activities.
- No “one-size-fits-all” solutions.
- External audit can help identify compliance shortcomings.



Security Policy

- Develop written security policy which outlines specific measure to protect consumer data.
- Example – encryption of data files sent over the Internet.
- Security policy needs to be translated into specific procedures and standards.
- Several resources for sample policies.



Security Policy Resources

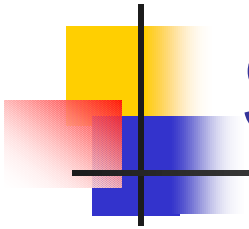
- Information Security Policies Made Easy by Charles Cresson Wood.
- Julia Allen: The CERT Guide to System and Network Security Practices, 2001. ISBN 0-201-73723-X
- Scott Barman: Writing Information Security Policies, 2001. ISBN 1-57870-264-X.

Security Awareness

- Must communicate your policies to the affected employees.
- HIPAA requires privacy training and a security awareness program for all staff.
- FTC cases which enforce privacy policy require staff training.
- Minimum standard for due diligence?

Website ‘Seal’ Programs

- Participation in website ‘Seal’ programs
  - TRUSTe (www.truste.com)
  - BBBOnline (www.bbbonline.org)
  - WebTrust (www.cpawebtrust.org)
- Involve your legal department in review of these agreements and your policies.
- P3P standard – World Wide Web Consortium ‘Platform for Privacy Preferences’ v.1.0 now incorporated in Internet Explorer.



Security Best Practices

- ISO 17799 / BS 7799 provide guidelines – must purchase standard or hire audit firm which will use it for comparison.
- GASSP (being updated by ISSA to GAISP)

  http://web.mit.edu/security/www/gassp1.html
- NIST Special Publication 800-14

  "Generally Accepted Principles and Practices for Securing Information Technology Systems"

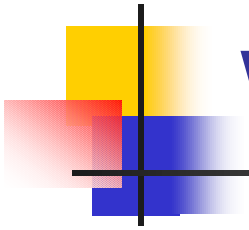
  http://csrc.nist.gov/publications/nistpubs/index.html

Additional Resources - Books

- Julia Allen: The CERT Guide to System and Network Security Practices, 2001. ISBN 0-201-73723-X
- Scott Barman: Writing Information Security Policies, 2001. ISBN 1-57870-264-X.
- Stephen Cobb: Privacy for Business: Web Sites and Email, 2002. ISBN 0-972-48190-7
- Andrew Frackman (et al): Internet and Online Privacy: a Legal & Business Guide, 2002. ISBN 0-9705970-7X

Web Resources – Privacy

- Center for Democracy & Technology
  http://www.cdt.org
- Electronic Frontier Foundation
  http://www.eff.org
- Electronic Privacy Information Center
  http://www.epic.org
- Privacy Rights Clearinghouse
  http://privacyrights.org/index.htm



Web Resources – Security

- System Admin & Network Security
  http://www.sans.org
- Open Web Application Security Program
  http://www.owasp.org
- Security Focus (portal & mailing lists)
  http://www.securityfocus.com
- Security Wire Digest (e-news)

http://infosecuritymag.techtarget.com/currentdaily.shtml