CALIFORNIA DEPARTMENT OF CONSUMER AFFAIRS

OFFICE OF Privacy Protection

Security Breaches Lessons Learned in California

Joanne McNabb, Chief

California Office of Privacy Protection

CA Office of Privacy Protection (COPP)

- CA 1st state with such an agency, started in 2001
- Mission: Protect the privacy of individuals' personal information … by identifying consumer problems in the privacy area and facilitating the development of fair information practices.
  - CA Business & Professions Code § 350

COPP Functions

- Consumer assistance
- Education and information
- Coordination with law enforcement
- Best practice recommendations

Recommending Privacy Practices

- COPP's *Recommended Practices* usually related to new laws
  - Not regulations or legal interpretations
  - "Best practices" guidance
  - Developed with advisory group of stakeholders

COPP's Recommended Practices

- Security Breach Notification (2003, rev. 2005 – law took effect 7/1/03)
  - Prevention
  - Preparation
  - Notification

COPP and Security Breaches

- How COPP learns of breaches
- COPP's assistance on breaches
  - *Recommended Practices*, with sample notice letters
  - One-page flyer on SSN breach
  - FAQs for call centers
  - Information sharing on lessons learned

Lessons Learned from Breaches

Data Is Portable

- More than half of breach notifications on incidents of lost or stolen laptops, disks, tapes, etc.
- Workers are on the move, taking sensitive data with them.
  - Management often not aware.

Data Is Retained Too Long

- Universities, for example, had breaches of data – including SSNs – of students, faculty, applicants not admitted from 10-15 years ago.
  - Discovered no business need to retain that data so long.

Unneeded Data Still Collected

- Forms contain fields for SSNs when no longer needed – old forms persist.

Paper Records Sought by Thieves

- Stolen mail and Confidential Destruction boxes, and lost express mail packages create risk of identity theft.

The Human Factor

- Many workers not aware of value of data – worth more than the laptop.
- Many not aware of incident reporting procedures – results in delays.

Steps Taken by State Government

- Data Classification System revised to call out “notice-triggering” personal information.
  - BL 05-08
- Encryption Policy re personal information on portable computing and storage devices.
  - BL 05-32
- Both available online
  - At www.dof.ca.gov/FISA/BudgetLetters/BudgetLetters.asp

Steps Taken by State Government

- Policy on Information Security Program Expanded to Include Privacy Component
  - Protect personal, sensitive, confidential info *in any medium*
  - Monitor compliance with privacy/security program
  - Report and prepare to notify on breaches *in any medium*
  - Annual privacy/security training and certification for all employees
- See MM 06-12
  - At www.osp.dgs.ca.gov/On-Line+Publications/SAM+Management+Memos.htm

COPP Resources for State Gov't

- Basic Privacy Training Presentation
- *Recommended Practices on Notice of Security Breach* with sample notice letters
- Security Breach First Steps (1-page flyer for use in SSN breach)
- Breach Call Center FAQs
- All available online
  - At www.privacy.ca.gov/state_gov/index.html

Contact Information

Joanne McNabb, Chief
California Office of Privacy Protection
Department of Consumer Affairs
1625 North Market Blvd., Suite N324
Sacramento, CA 95834
866-785-9663
www.privacy.ca.gov