Protecting Personal Information: Best Practices for Business

Agenda

August 13, 2008

8:30 - 9:30 Registration

9:30 - 9:45 Opening Remarks

- Welcome and introduction of co-sponsors

9:45 - 10:15 Presentation – Risks & Costs: What's at Stake?

Business and legal reasons to address data security including:

- Federal laws and standards enforced, recent cases, and the costs, penalties, and relief imposed
- California laws and standards enforced, recent cases and the costs, penalties, and relief imposed
- The prospects of private litigation against companies that experience a breach
- Other costs of data breaches – breach response costs, reputational damage, customer relations impact
- Other business rationales for improved data security

Presenters:

Catherine Harrington-McBride, Attorney, Los Angeles Regional Office, Federal Trade Commission

Joanne McNabb, Chief, California Office of Privacy Protection

10:15 - 10:25 Break

10:25 - 11:35 Panel 1 – Protecting Personal Information: Steps & Strategies

Practical guidance and lessons learned from persons engaged in security compliance, addressing basic questions, such as:

- What challenges have you faced in taking and maintaining an inventory of your personal information and equipment?
- How have you gone about determining whether you had adequate network and physical security?
- What data security challenges have you faced in hiring service providers and technical staff?
- How have you worked with outside IT professionals to address security issues posed by electronic information you use, maintain, store, or share?

- What issues have you confronted in determining what information to retain and what information to dispose of?
- What obstacles did you confront in persuading your organization to invest in better information security? How did you get top management involved?
- How did you balance the costs and benefits of compliance? How did resource availability affect your data security planning?

Moderator: Laura Berger, Attorney, Division of Privacy and Identity Protection, Federal Trade Commission

Panelists:

Barbara Lawler, Chief Privacy Officer, Intuit
Eric Nelson, Principal, Secure Privacy Solutions
Jill Phillips, Chief Privacy Officer, Chevron
Shai Samet, President and Founder, Samet Privacy LLC
Andrew Serwin, Partner, Foley & Lardner

11:35 - 11:50 Break

11:50 – 1:00 Panel 2 – When Things Go Wrong: Planning for & Responding to Data Breaches

Breach response and the importance of planning ahead, including:

- Anticipating and planning for a breach
- Responding when a breach occurs
- Breach investigation and maintenance of evidence
- Data and systems recovery
- Working with outsiders – what do law enforcement or technical professionals do when called in to respond to a breach, and what information do they look for and need?
- Notice and assistance to victims and consumers – how do consumers respond when a trusted business suffers a breach, and what is the best way for businesses to notify and communicate with customers in order to protect the relationship?

Moderator: Burke Kappler, Attorney, Division of Privacy and Identity Protection, Federal Trade Commission

Panelists:

James Aquilina, Executive Managing Director and Deputy General Counsel, Stroz Friedberg, LLC
Jonathan Avila, Vice President – Counsel, Chief Privacy Officer, The Walt Disney Co.
Lt. Robert (Rocky) Costa, Los Angeles County Sheriff's Department – Southern California High Tech Crimes Task Force
Reece Hirsch, Partner, Sonnenschein, Nath & Rosenthal LLP
Richard Purcell, Chief Executive Officer, Corporate Privacy Group

1:00 Closing Remarks