INFORMATION SECURITY: THE NEW FRONTIER OF CORPORATE LIABILTY

SCOTT W. PINK
GRAY CARY WARE & FREIDENRICH
spink@graycary.com
(916) 930-3271

February 5, 2004
Open Security Forum

Agenda

- Why cybersecurity matters?
- Emerging Theories of Liability
- Scenarios
- Compliance
- Future Trends.

Gray Cary

- National law firm with over 350 attorneys.
- Full service firm representing leading technology companies.
- Privacy services group provides counseling and advice on privacy and security issues.
- Commercial and technology transactions group assist companies in negotiating and documenting technology deals.

Why Cybersecurity Matters

- Preventing damage and loss.
- Maintaining employee and customer confidence.
- Meeting contractual requirements.
- Ensuring legal compliance.
- Avoiding potential legal liability.

Cybersecurity Law Overview Consumer Protection

- Privacy ➠Security.
- Existing U.S. information security requirements focus on regulated industries:
  - Gramm Leach Bliley
  - HIPAA
- FTC enforcement ➠security requirements imposed under unfair trade practice law.

California's New Security Breach Disclosure Requirements

- SB 1386 – Effective July 1, 2003
- Creates new disclosure requirements for security breaches for government agencies and businesses.
- Applies to:
  - Any person or business that conducts business in California and
  - Owns or licenses computerized data that contains personal information or maintains such computerized data for another

What information is covered?

- Personal information:
  - Individual's first name or initial and last name **in combination** with one or more of the following "data elements", when either of them is not encrypted:
    - Social security number
    - Driver's license number or California ID number
    - Account number, credit or debit card number in combination with required security code, access code or password that would permit access to account

Disclosure Obligations

- Covered businesses must disclose:
  - Any breach of the security of the system following discovery or notification of the breach.
  - Breach = unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of PI of a **California resident**.
  - Good faith acquisition by employee or agent is not breach, provided not used for further unauthorized use or disclosure.

Notice Requirements

- Owners of computerized data must disclose to affected California residents; maintainers of such information must disclose to owners (who in turn must disclose to affected persons).
- Notice must be given to any resident of California whose PI is or is reasonably believed to have been acquired by unauthorized person.
- Notice must be given in "most expedient time possible" and "without unreasonable delay" consistent with:
  - Needs of law enforcement.
  - Necessary measures to determine scope of breach and restore reasonable integrity of system.

Notice Requirements

- **Notice can be provided**:
  - Written notice
  - Electronic notice consistent with E-Sign Act.
  - Substitute notice if cost exceeds $250,000 or affected class exceeds 500,000 or do not have sufficient contact information. Must do all of the following
    - Email to those for which it has addresses
    - Conspicuous notice on web site
    - Notice to major statewide media
- **Can follow existing internal procedures if consistent with time requirements of the law**

Protecting Business Assets

- New SEC Rules under Section 404 of the Sarbanes-Oxley Act might impose cybersecurity requirements:
  - "Internal control over financial reporting" = process that provides reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the registrant's assets that could have a material effect on the financial statements."
- Obligation arise from fiduciary duties of corporate officers and directors?
- Obligations can arise from contracts.

Emerging Standards of Care

- NIST, OECD, Internet Security Alliance.
- Potential impact:
  - Creating standard of care for negligence claims.
  - Creating standards of care for regulators.
  - Creating standards of care for contracts.

National Security Debate

- 9/11 raised national security issues:
  - Passage of Patriot Act increased investigative powers of law enforcement for cybersecurity and other threats.
  - National Strategy to Secure Cyberspace.
  - Critical Infrastructure Information Protection Act encourages sharing of information with Department of Homeland Security.

Scenarios

- CFO loses laptop.
- Former employee accesses payroll files using stolen password.
- Intrusion incident, but accessed data is encrypted.
- Company based in Indiana has servers in South Dakota hacked into with PI of California residents.

Compliance

- Risk Assessment.
- Conduct privacy and security audit.
  - Assess what laws apply to business and whether company is in compliance.
  - Identify data, where located and who has access.
  - Assess whether Personal Information is encrypted and if not, determine if encryption can be applied.
- Revise procedures or create new procedures for Implementing Security.

Compliance

- Revise/review contracts in light of security issues.
  - Representations/warranties.
  - Indemnification.
- Review insurance policies.
- Create crisis response team.
- Continua reassessment.

Trends?

- Proposed federal law – Notification of Risk to Personal Data Act (S. 1350)
  - Modeled after California law.
  - Applies to any company engaged in interstate commerce.
  - Anti-fraud and notification procedures under GLB may suffice.
  - Civil penalties, but no private right of action – enforced by FTC or state attorneys general.
  - Preempts state laws except California's.

THE END

THANK YOU FOR YOUR ATTENTION

About the Speaker

Scott W. Pink is Special Counsel in the Intellectual Property and Transactions Group of Gray Cary, a national law firm based in Silicon Valley that represents leading technology companies. Before joining Gray Cary, Scott was Vice President, General Counsel and Secretary for Prima Communications, Inc., an international publishing company that was sold to Random House. Scott served on the company's executive committee and was responsible for the contractual and legal affairs of the company. Scott has also been a partner in a major San Francisco law firm and a law clerk to the U.S. Court of Appeals for the Ninth Circuit.

Scott is a recognized expert on internet and cybersecurity law. He is currently deputy chair of the American Bar Association Business Law Section's "Cybersecurity Task Force". He has spoken on cybersecurity and specifically on California's new security breach disclosure requirements to the American Bar Association, the Information Technology Association of America, the SDForum, and many other groups. He has published several articles on the subject, including "The New Cybersecurity Paradigm: California Law Now Requires Disclosure of Security Breaches" published in the June 30, 2003 issue of BNA's Privacy & Security Law Report.

Scott is also an expert in intellectual property law and transactions. He has served as chair of local, state and national intellectual property organizations and has spoken to many organizations on the subject of intellectual property law, licensing, distribution and outsourcing transactions, and strategic alliances. He is the author of many publications, including *The Internet and E-Commerce Legal Handbook* published by a division of Random House, *Protecting Trademarks in Cyberspace*, Cover Story for January 2002 issue of the ACCA Docket, *Electronic Filing of Trademark and Patent Applications*, July/August 2002 issue of the ACCA Docket, *State Spam Laws Survive Constitutional Scrutiny, but Should Congress Enact a Federal Law*, April 2002 Journal of Internet Law, and *Publishing in the Digital Age*, The Transnational Lawyer, Spring 2002. He also served as an adjunct Professor of Law at UC Davis Law School. Scott is a graduate *cum laude* of Harvard Law School and *magna cum laude* of Harvard University, where he was a starter on the lacrosse team that finished in the top ten nationally.