Bill Cook

» Partner, Wildman Harrold, Chicago
» Intellectual Property, Internet and Web law (Business Continuity and Security)
» 90 trials
» Expert presentations on Internet liability before U.S. House Judiciary Comm., GAO, FCC
» Extensive experience representing retailers on CPP, PCI & ADCR matters

» Chicago IMNA Board Member, Immediate Past President
» Former Head of US DOJ Computer Crime Task Force; Counter-Espionage Coordinator and Counter-Terrorist Coordinator; DOJ FEMA Coordinator (Chicago)
» NRC Committee on Critical Infrastructure Protection and the Law
Update

» Privacy Drive Security
» Security is no longer about best practices
» Security is now a duty owed
Key Trend
Duty to Provide Security for Information

» Major trend driven by expansion of privacy law
  » Expanding across all industries
    » Not just financial and healthcare sectors
    » Impact on range of corporate deals
  » Applies to most corporate data
    » Not just personal data
    » Also financial, transactional, tax, confidential, etc.

» It is all about protecting the stakeholders
  » Shareholders / investors, employees, customers and prospects, interests of regulatory agencies, unrelated third parties, national interests
Where Do the Legal Obligations Come From?

- Many sources, no single law or regulation
- **U.S. Federal laws and regulations**
  - Electronic records generally – E-SIGN
  - Financial records – Sarbanes-Oxley
  - Tax records – IRS
  - Other records – SEC, FDA, HHS, etc.
- Personal information
  - GLBA (financial industry)
  - HIPAA (healthcare records)
  - COPPA (children)
  - Safe Harbor (EU source data)
  - FTC Section 5 (all industries)
Where Do the Legal Obligations Come From? (cont.)

» **State laws** and regulations
  » Electronic records generally – UETA
  » General security laws
    » Obligations to implement security
    » Data destruction laws
  » Other specific laws, e.g., EFT, insurance, etc.

» **Evidentiary requirements**
  » e.g., *AmEx* case

» **Contractual commitments**
Where Do the Legal Obligations Come From? (cont.)

» Tort law
  » *Bell v. Michigan Council* – failure to provide security for employee data
  » *In re Verizon* – failure to apply patches

» FTC and State AG enforcement actions
  » False representations and promises
  » Unfair business practices

» International Laws
  » EU Data Protection Directive
  » EU country implementing laws and regulations
  » Argentina, Australia, Canada, Japan, and others
The Legal Standard for Maintaining Information Security

» Because security is a legal obligation, what do you have to do?
  » Do you have to encrypt this data?
  » Are passwords sufficient or do you need a token?
  » Is it OK to allow Wi-Fi access?

» A “legal” standard for “reasonable security” is developing in the U.S.

» It is focused on a “process” rather than specific technical requirements
Key Trend
Executive Responsibility for Information Security

» Who?
  » Not just CIO and risk management functions
  » CEO, CFO, GC, Senior Management
  » Board of Directors

» What?
  » Approve the security program
  » Oversee development, implementation, and maintenance of the security program
  » Require regular reporting
Key Trend
Duty to Disclose Security Breaches

» Duty to disclose security breaches to:
  » Those who may be affected/injured
  » Regulators, enforcement agencies, etc.

» Obligation akin to “duty to warn”

» Started in California in 2003, now 34 states impose some obligation

» Laws differ, but all based on California model

» Having a major PR impact
States Imposing Legal Obligations

States with breach notification laws

States with breach notification laws and with laws imposing obligations to provide security

1 Applies to information brokers only.
2 Applies to state agencies only.

Northwestern University: Internet Update 2007
Breach Notification
Legal Requirements

» Covered information – “name” plus one of:
  » SSN
  » Drivers license number
  » Financial account or credit card number
  » Other

» Triggering event
  » Any breach of security, or
  » Breach with reasonable likelihood of harm

» Obligation on breach
  » Notify persons whose information compromised
  » Notify state enforcement agencies – (some states)
  » Notify credit agencies – (some states)
Breach Notification
Legal Requirements (cont.)

» Timing of the notice
  » In the “most expedient time possible and without unreasonable delay”
  » Delay OK for law enforcement investigation or to take necessary measures to determine the scope of the breach and restore system integrity

» Form of notice
  » In writing
  » Electronic form (but must comply with E-SIGN)
  » Substitute notice
  » Alt – follow company incident response plan

» Penalties
  » State enforcement (e.g., A.G. office)
  » Some private right of action
Privacy violations in credit card situation leads to bank enforcement & regulation
Honor the threat

» Continued growth in Russian & Ukrainian activity for next 5 to 6 years
» Legitimate security technology companies failing in Russia due to employment by hostile technologies
» $100,000 per day profit maximum due to handling issues
» Hostile technology specialists now attacks at POS, processor & banking levels
TJX

» Evolving problem since 2005
» $107 M liability reserve
» Settlement with consumers
» Still pending
  » Class action litigation brought by banks
  » Government actions for negligent protection of consumer information
Merchants and Charge Card Fraud Allegations

» 20% of all retail charges are fraudulent

» Banks point to retailers as source of intrusion due to poor security practices

» Actions taken:
  » Worked with clients to show that PCI security standards were followed or compensating controls put in place
  » Worked with forensic auditors
  » Consumer notification issues handled
  » Represented clients to banks and credit card associations
  » Counterclaims against vendors
Scope of PCI Data Security Standard
“Broader than you think”

» Applies to all entities that “transmit, process, or store cardholder data”
» Not just e-commerce and brick-and-mortar, but…
  » Healthcare
  » Higher education
  » Utilities
  » State and Local Government
  » Insurance
  » Banking
Merchant Levels

- Level 1
  - Over 6 million transactions per year or compromised

- Level 2
  - From 1 million to 6 million transactions per year

- Level 3
  - From 20,000 to 1 million transactions per year

- Level 4
  - Up to 20,000 transactions per year
“Bill Would Punish Retailers for Leaks of Personal Data, WSJ 2/22/07

- Mass. State law
  - Requires retailers, processors or banks to pay for losses when hackers breach their security systems and steal credit card information and financial information
    - Emphasis on retailers
  - $2 billion fraud losses a year currently being paid by the banks
- Barney Frank predicts federal law to follow
CPP (CPC) Designation

» Case against merchant begins with designation as a common point of purchase (CPP) or a common point of compromise (CPC)

» CPP is determined by reverse analysis of credit card or debit card activity

» Credit card association or agent makes contact

» Date of alleged fraud may be remote

» Forensic Audit triggered
ADCR
Account Data Compromise Recovery Process

» CPP on steroids
» Virtually instant money for the issuing banks
» Visa determines CPP
» Calculates potential ADCR based on accounts and time period
» Directed to Acquiring Bank, not to Retailer
» Acquiring Bank debits Retailer accounts
» Issuing bank not foreclosed from bringing separate action
Moving Parts

- Visa, MC, AmEx, Discovery
- Issuing banks
- Acquiring banks
- Franchisees
- Merchants that accept fraudulent credit cards, increasingly located in Europe
- POS software vendors
- Insurance companies and brokers
- Public relations
- Stockholder issues
- Board of Director issues
- Consumer disclosure issues and Secret Service non-disclosure request
Hot Issues in Data Security Cases

» Former or Current Employees
» Company officers
» Vendors
» Agents
» Competitors
Liability From Stolen Computers

» Theft from global telecommunications client’s healthcare vendor included computers with personal data on the hard drives

» Client’s employee database of health information, personal credit cards and other personal information missing

» Actions taken:
  » HIPAA exposure identified
  » Potential employee legal action(s) identified
  » Vendor forced to meet ISO 17799 and corporate standards
    » Prepared and oversaw E&Y ISO 17799 security audit and evaluated compensating controls
  » Negotiated vendor contract changes and remediation
  » Rewrote security provisions for vendor contracts
Trade Secret Theft by Defecting CEO

» CEO and 5 key employees left ecommerce client with trade secret information to start up competing company

» Actions taken:
  » Immediately walled off data at new employer
  » Checked client’s records for data transfers
  » Forced forensic analysis of departed hard drives to locate stolen information
  » Evaluated Economic Espionage Act referral
  » Opponents clearly understood liability and embarrassment if they did not cooperate
  » Used threat of litigation to achieve client’s business strategy without actually having to go to court
  » Negotiated return of all data and essentially shut down potential competitor
Justifying Competitive Intelligence Gathering

- Client’s President accessed competitor’s FTP site and obtained customer lists, vendor price lists, source code.
- Criminal and civil actions filed against Client at the same time as FBI search of corporate offices.
- Actions taken:
  - Conducted internal investigation.
  - Represented Company to FBI and DOJ.
    - All charges dropped and declination letter received.
  - Successfully countered civil action by analysis of competitor’s security practices, FTP site permissions and actual practices.
  - Assisted in PR response.
Puddingmedia

» Service provides eavesdropping on Internet calls.
» Caller talking about dinner who have restaurant ads pop up on browser.
» Similar to Google Inc.’s Gmail where scans of email by system
  » Privacy concerns passed with time and user concerns abated
Identity Theft

» Now possible for consumers to strike back on banks and credit card companies

» Wolfe case
Organizations Required to Protect Employee Information

» Michigan union found negligent in failing to protect membership information from identity theft