Trends in the Law of Information Security

Thomas J. Smedinghoff
Wildman Harrold
Chicago

Three Factors Driving the Legal Landscape

- Total corporate dependence on information technology and networked information systems, which leads to
  - Tremendous economic benefits, efficiencies, cost savings, and productivity improvements
  - A significant new potential vulnerability
- Recognition that a security compromise affects all corporate stakeholders
  - Shareholders/investors, employees, customers, suppliers, regulators, general public, etc.
- A major shift in public attitude
  - Compare our response to a bank robbery by Jessie James
  - To our response to the digital robberies of today

Legal Response to the Problem of Information Security

Wildman Harrold
Attorneys and Counselors

The law addresses security of corporate information and communications in three ways:

1. Some laws protect the security of corporate information
2. **Some laws impose security obligations on companies to protect their own information**
3. Some laws provide some legal benefits for implementing security

This session focuses on item No. 2 above

Session Approach

Wildman Harrold
Attorneys and Counselors

- Put the focus on corporate security obligations
  - Look at development of the issues
  - Not a case-by-case review
- Take the 50,000 foot view – consider developments broadly
  - Despite narrow application in some cases
- Because developing law in one sector may –
  - Be the only available precedent
  - Apply by analogy
  - Define best practice
  - Indicate a trend

Key Trends
Re Corporate Security Obligations

Wildman Harrold
Attorneys and Counselors

- The general duty to provide security for corporate data is expanding, and becoming more defined
- A legal standard for reasonable security is emerging
- Specific duties are also emerging regarding –
  - Specific data elements
  - Specific security controls
- A new duty to warn has been created

The General Corporate Duty to Provide Data Security

Wildman Harrold | 225 West Wacker Drive | Chicago, IL 60606 | (312) 201-2000 | wildman.com

What Is the Duty to Provide Security?

Wildman Harrold
Attorneys and Counselors

- A general duty to provide–
  - "appropriate" or "reasonable"
  - administrative, technical and physical controls
  - to protect the confidentiality, integrity, availability, and authenticity of corporate data

- But what is "appropriate" or "reasonable"

It Comes From Many Sources

- Many sources; don't always use the word "security"
- Numerous Federal laws and regulations, such as –
  - E-SIGN, Sarbanes-Oxley, GLBA, HIPAA, Safe Harbor, FTC Act, FCRA/FACTA, Federal regulations, etc.
- Numerous State laws and regulations, such as –
  - Laws imposing general duty to provide security, state unfair business practice laws, etc.
- Common law / tort law
- Evidentiary requirements
- Contractual commitments and self-imposed obligations
- Industry standards (e.g., PCI, ISO/IEC 27001, etc.)
- Self-imposed obligations
- International law

It's All About the Stakeholders

Wildman Harrold
Attorneys and Counselors

- Protecting those likely to be hurt by inadequate corporate security
  - Shareholders / investors
  - Employees
  - Customers / prospects
  - Suppliers
  - Individuals
  - Government regulators
  - Others
- Consider the implied negligent misrepresentation theory based on alleged failure of TJX to notify the issuing banks in the TJX cases currently pending

It Applies To All Companies

Wildman Harrold
Attorneys and Counselors

- FTC expanding scope of FI regulations to <u>all companies</u>
  - First deceptive business practices (since 2001)
  - Now unfair business practices (since 2005)
- State laws imposing general duty on <u>all companies</u>
  - Obligation to "implement and maintain reasonable security procedures and practices . . . to protect personal information from unauthorized access, destruction, use, modification, or disclosure"
- Common law duty of <u>all companies</u> to provide security
  - *Wolfe v. MBNA America Bank* (2007)
    - Where injury foreseeable and preventable, defendant had duty to third parties to authenticate identity of applicants for credit card
  - *Bell v. Michigan Council* (2005)
    - "defendant did owe plaintiffs a duty to protect them from identity theft by providing some safeguards to ensure the security of their most essential confidential identifying information"

It Covers All Corporate Data

Wildman Harrold
Attorneys and Counselors

- Personal data is driving many laws
- But the trend is to require security for all data, such as –
  - Financial data – e.g., SOX
  - Tax data – e.g., IRS Regs.
  - Transaction data – e.g., UETA, E-SIGN
  - E-mail records – e.g., SEC regs.
  - Employee Data – e.g., DHS I-9 regs.
- Now it's also an evidentiary issue
  - *American Express v. Vinhnee* (9th Cir, Dec. 2005)

    (Evidence not admissible without showing of adequate information security)

Responsibility Is At the Top

Wildman Harrold
Attorneys and Counselors

- It's not an IT issue – it's a governance issue
- Who?
  - Upper management
  - Board of directors, CEO, CFO
- What?
  - Approve the security program
  - Oversee development, implementation, and maintenance of the security program
  - Require regular reporting

The Legal Standard for Information Security

What Is “Reasonable Security”?

Wildman Harrold | 225 West Wacker Drive | Chicago, IL 60606 | (312) 201-2000 | wildman.com

The General Duty: It's All About the "Process"

Wildman Harrold
Attorneys and Counselors

- The key question – What is required for legally-compliant "reasonable security"?
  - Strong security measures do not, *per se*, provide adequate security
  - Note the TJX case – all the data was encrypted!
    - "But we had locks" – Carol Meyerowitz, CEO, TJX Cos. at Shareholders meeting on June 6, 2007 (apologizing for the company's recent security breach that involved the theft of at least 45.7 million credit and debit card numbers)
- A legal standard is developing
  - Focus is on "process," not specific security measures
  - The laws do not tell you what to do
  - Five (5) key points to the legal standard . . .

The Legal Standard – It's All About the "Process"

Wildman Harrold
Attorneys and Counselors

1. Identify the assets to be protected
   - Both (i) under company control and (ii) outsourced
2. Conduct risk assessment
   - Identify and evaluate threats, vulnerabilities, and damages
   - Consider available options
3. Develop & implement a written security program
   - That is responsive to the risk assessment
   - That addresses the required categories of controls
4. Continually monitor, reassess, and adjust
   - To ensure it is effective
   - To address new threats, vulnerabilities, and options
5. Address third parties

1. Identify Your Information Assets

- "We don't even know what we have"
- Identify the –
  - Systems and networks to be protected
  - Information to be protected
  - Laws that apply to that information
- Consider –
  - Your systems and your records
  - Third party records in your possession
  - Your records and processing that you outsource to others

2. Conduct a Risk Assessment

- What are the foreseeable threats?
  - Internal and external?
- For each foreseeable threat
  - What is the likelihood that it will materialize?
  - What is the potential damage that it would cause?
- What is the sufficiency of the protective measures in place to guard against them?
- What is the additional burden of implementing adequate precautions?

3. Develop and Implement A Responsive Security Program

Wildman Harrold
Attorneys and Counselors

- Program must be in writing
  - "If it's not in writing, it doesn't exist"
- Decide on the specific security controls
- Two legal requirements
  - Focus on responding to the threats identified in the risk assessment
  - Consider the designated categories of security controls
- Controls must respond to risks
  - Armed guards don't protect against Internet access
  - Firewalls don't protect against dishonest employees

3. Controls Must Respond to the Risk Assessment

Wildman Harrold
Attorneys and Counselors

- *Guin v. Brazos Education*
  - No liability for breach caused by unforeseeable event where proper risk assessment done and responsive controls put in place
- *Bell v. Michigan Council* and *Wolfe v. MBNA America Bank*
  - Liability imposed where the harm of someone misusing plaintiffs' personal information was foreseeable, but not addressed
- Federal Financial Institutions Examination Council (FFIEC) Guidance
  - Cannot apply controls without first doing a risk assessment

4. Continual Monitoring and Reevaluation Required

- Constant testing and monitoring to ensure security program is effective
  - Merely rolling out the security program isn't sufficient
  - Need to monitor compliance and effectiveness
- Review, reassess, and adjust program in light of:
  - Changes in threats
  - Changes in technology
  - Changes in business
  - Changes in operations or environment
  - Results of compliance monitoring
  - Changes in customer requirements
- Obtain independent audit

5. Address Security re Third Parties

Wildman Harrold
Attorneys and Counselors

- Who?
  - Third parties that access company systems
    - Contractors, customers, suppliers, business partners, government entities (not all of these treated the same)
  - Providers of outsourced services
    - ITO, HRO, BPO, managed security services, etc.
- What?
  - Due diligence in selection / authorization
  - Contractual imposition of security obligations
  - Monitoring and auditing of performance

The Death of Industry Best Practices?

- May represent minimum requirements
  - Company must "implement standard practices. . . where such standards have gained sufficient industry acceptance and adoption such that . . . adherence to the standards would not unreasonably place [company] at a competitive disadvantage." – *Ziff-Davis AG Consent Decree*
- But may not be sufficient
  - FFIEC Guidance – Challenging so-called industry best practice re online authentication practice
  - Remember the *T.J. Hooper* case – (liability imposed for failure to provide security in excess of industry standard practice)
- New ISO/IEC 27001 int'l standard (Nov. 2005)
  - Allows for certification

Explosion of Specific Duties: A Problem of Compliance Overload

Wildman Harrold
Attorneys and Counselors

- Special rules for selected data elements
  - Sensitive data (EU)
  - Social security numbers
  - Credit card data
  - Health care data
  - I-9 data; W-9 data
- Special rules for selected security controls
  - Online authentication
  - Data destruction
  - Data retention

Duty to Delete Data Coming??

Wildman Harrold
Attorneys and Counselors

- August 9, 2006 -- Rep. Ed Markey (D-Mass.), called for congressional action to impose limits on the retention of Internet data
  - Cited AOL inadvertent release of 20 million keyword searches by more than 600,000 Internet users as evidence that a data retention law is needed to prevent companies from storing consumers' Internet information for indefinite periods of time.
  - Bill (H.R. 4731), would require companies to eliminate Internet data when it is no longer needed for any "legitimate business purpose”

Duty to Retain Data Coming??

Wildman Harrold
Attorneys and Counselors

- March 15, 2006 – European Data Retention Directive (2006/24/EC) adopted to combat terrorism
  - Empowers EU member states to require telecoms and Internet companies to store telephone call and Internet data for up to six months
- June 7, 2006 – Colorado law (H.B. 1011) requires ISPs to preserve and release records of their users to law enforcement agencies in certain cases
- June 16, 2006 – 49 state AGs general urge a national data retention standard to assist in investigations of online sexual predators.

The Duty to Disclose Security Breaches

Wildman Harrold | 225 West Wacker Drive | Chicago, IL 60606 | (312) 201-2000 | wildman.com

Overview of Breach Notification Laws

Wildman Harrold
Attorneys and Counselors

- Not a new concept
  - Appears in IRS regulations for tax data
- Obligation akin to “duty to warn”
- Imposes duty to disclose security breaches to –
  - Data subjects who may be affected/injured
  - Regulators, enforcement agencies – (some laws)
  - Credit agencies – (some laws)
- Started in California in 2003, now 39 states in the U.S.
- Having a major PR impact
- See chronology of breaches at www.privacyrights.org

U.S. Breach Notification Law Requirements

Wildman Harrold
Attorneys and Counselors

- Applies to sensitive personal information –
  - A person's name
  - Plus one of the following data elements:
    - SSN
    - Drivers license number
    - Financial account or credit card number
    - Other (in some states)
- Triggering event (varies by state)
  - Any breach of security, *or*
  - Breach with reasonable likelihood of harm

International Adoption Coming

Wildman Harrold
Attorneys and Counselors

- Japan (2005)
- European Union recommendations for adoption
  - European Commission (Sept. 2006)
  - Article 29 Working Party (Sept. 2006)
  - UK House of Lords Report (July 2007)
- Canada
  - Office of Privacy Commissioner Voluntary Guidelines (Aug. 2007)
- New Zealand
  - Privacy Commissioner Voluntary Guidelines (Aug. 2007)
- Australia
  - Privacy Commissioner recommended legislation (Sept. 2007)

A New Duty to Disclose Inadequate Security?

- Court allowed banks to proceed against TJX
  - On a theory of "*implied negligent misrepresentation*"
    - the negligent misrepresentation claim is based on implied representations that TJX and Fifth Third made to the issuing banks that they took the security measures required by industry practice to safeguard personal and financial information. Even if neither TJX nor Fifth Third had direct contact with the issuing banks, TJX and Fifth Third knew that the issuing banks were part of a financial network that relies on members taking appropriate security measures.
  - Based on alleged failure of TJX to notify the issuing banks that its security was inadequate – i.e., "that TJX and Fifth Third had a duty to disclose that it was taking deficient security measures"

In Re TJX Companies Retail Security Breach Litigation (D. Mass. October 12, 2007)

What Happens When You Breach Your Obligations?

Wildman Harrold
Attorneys and Counselors

- Liability to injured persons
  - Shareholders and investors
  - Data subjects, e.g., employees, borrowers, others
  - Business partners
  - Unrelated third parties -- how far does it extend?
- Compliance liability
  - Liability with or without injury (e.g., fines, injunctions)
- Remediation costs
  - "Estimates Put T.J. Maxx Security Fiasco at $4.5B" *Information Week* 5/2/07
- Reputation risk – the ultimate penalty!
  - Choicepoint – 20% stock price decline
  - Card Systems – out of business

Damages – A Mixed Bag So Far

Wildman Harrold
Attorneys and Counselors

- Courts requiring actual loss or damage
- The threat of future harm, not yet realized, will not satisfy the damage requirement
- Theft of personal data, without more (e.g., evidence that plaintiff's data was targeted or actually accessed by bad guys) is not sufficient to establish injury (i.e., does not establish increased risk of experiencing identity theft over next several years)
  - *Stollenwerk v. Tri-West Healthcare Alliance*
  - *Guin v. Brazos Education*
  - *Forbes v. Wells Fargo Bank*

But Where Losses Are established . . .

Wildman Harrold
Attorneys and Counselors

- Even mental anguish may be recoverable in ID theft cases
- "[Plaintiffs] had spent numerous hours trying to correct the problems created by the identity theft, which left their collective credit in ruins. Plaintiffs produced concrete examples of the aggravation and anguish suffered by detailing their experiences of trying to purchase cars, homes, furniture or phone service and the resultant humiliation of being turned down for credit. Accordingly, plaintiffs presented sufficient evidence to create a question for the jury regarding their mental damages."

Bell v. Michigan Council

Further Information

Wildman Harrold
Attorneys and Counselors

Thomas J. Smedinghoff
Wildman Harrold
225 West Wacker Drive
Chicago, Illinois 60606
312-201-2021
smedinghoff@wildman.com