Liability Risks for Security Breaches

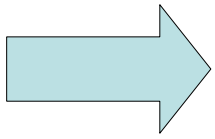
Maury D. Shenk

STEPTOE&JOHNSON

4 November 2004

Why liability? – Answer one

Something Bad Happens



People Fight Over Blame and Financial Responsibility

Why liability? – Answer two

The major reason companies don't worry about the externalities of their security decisions … is that there is no real liability for their actions. Liability will immediately change the cost/benefit equation for companies, because they will have to bear financial risks borne by others as a result of their actions.

Bruce Schneier
Testifying before U.S. House of Representatives in 2003

Statute and regulation – EU

- EU directives implemented by national law in 25 Member States
- Data Protection Directive (95/46/EC)
  - Applies to "personal data"associated with an identifiable living individual
  - Article 17 (Security of processing) – requires "appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access"
  - Article 23 (Liability) – Allows action by "any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive"

Statute and regulation – EU (cont'd)

- Privacy and Electronic Communications Directive (2002/58/EC)
  - Applies data protection principles to providers of electronic communications services
  - Article 4 (security)
    - Similar to Article 17 of Data Protection Directive
    - Also requires that "[i]n case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk"
  - Same liability rules as Data Protection Directive

Statute and regulation – US federal

- Gramm-Leach-Bliley (GLB) Act (1999)
  - Security of financial institution customer information
  - Implementing regulations require banks to "Protect against any anticipated threats or hazards to the security or integrity of [customer] information"
  - Regulatory enforcement; no private right of action
- Health Insurance Portability and Accountability Act (HIPAA) (1996)
  - Security of health information
  - Implementing regulations provide obligations similar to GLB Act
  - Regulatory enforcement; no private right of action

Statute and regulation – California

- Most important of the 50 states because of size, technology industry and legislative activism
- S.B. 1386 (2003)
  - Requires disclosure of security breach that compromises *unencrypted* personal information of California residents
  - Provides a private right of action
- A.B. 1950 (2004)
  - Requires any business (other than financial or health) that "owns or licenses" personal information of a California resident to "implement and maintain reasonable security procedures"
  - Provides a private right of action

Contract and tort

- Contract
  - Responsibility for what is agreed
    - Explicitly
    - Implicitly – statutory duties could be implied
  - Subject to contractual exclusions of liability
- Tort
  - Negligence
    - Duty of care may be implied from statutory standards, industry standards or industry practice
    - Caution required increases with (1) likelihood of injury and (2) severity of harm
  - Intentional tort – less likely

Practical considerations

- Few significant cases so far – almost none in Europe
- Who is at risk?
  - Consumer lawsuits bigger risk than B2B disputes
  - Consumer data riskier than financial data?
- Poor security could eliminate insurance coverage

Best practices

- Following "best practices" may be the best defence
- Don't be a "poster child" for bad security
- Example – best practices for patching
  - Implementation of patches provided by manufacturer
  - Timely implementation schedule, taking into account deployment issues
  - Timely replacement of software, particularly if unsupported
  - Implementation of specific statutory and/or regulatory requirements