Employee Use of Information Technology

Implications for Corporate Legal Obligations to Provide Security

Thomas J. Smedinghoff

Baker & McKenzie

smedinghoff@bakernet.com

The Fundamental Premise

Your company is now *totally dependant* on information technology

Corollary No. 1

Your company has a legal obligation to provide adequate security for its computer systems, networks, and information

Legal Obligations Include:

- Duty to provide information security
  - To prevent breaches
  - To detect breaches
  - To respond to breaches
  - To protect transactions
  - To preserve records
- Duty to warn
  - To disclose breaches to those who may be affected
- Duty to disclose state of security readiness?

The Goals of Security

- **Ensure information –**
  - **Availability**
  - **Access control**
  - **Authentication**
  - **Integrity**
  - **Confidentiality**
- **Protect against unauthorized –**
  - **Access**
  - **Copying**
  - **Disclosure or transfer**
  - **Alteration**
  - **Destruction**
  - **Processing**

Corollary No. 2

Your employees are your greatest asset … and your *weakest link*

- ***The most likely threat to data security is not the outsider, but rather negligent, incompetent, or malicious corporate insiders.***

- ***Remember – these are the people***
  - ***you trust***
  - ***you allow to have access to your systems***

Understanding the Role of Employees

Consider the security at your own house

Leading Causes of Information Security Breaches

- 39% -- Non-malicious employee error
- 30% -- Malicious employee activities
- 16% -- Hackers / external penetration
- 15% -- Other / unsure

Ponemon Institute, January 2005

What Is Likely Happening in Your Company?

- Employee use of IT is pervasive
  - There is more of it
  - By more of your employees
  - Using many new tools
  - Providing access to ever more corporate information
- It is an integral part of most jobs
- It is the primary vehicle for delivery of corporate information
- It's the lifeblood of the company

Lots of New Tools (and Toys)

- Corporate networks
- Corporate databases
- Corporate intranet
- E-mail
- Internet access
- Remote terminals, laptops, home computers
- Voice mail
- Metadata
- Chat rooms
- USB drives
- Instant messaging
- Blackberries/PDAs
- Wireless
- Blogs
- Cell phone cameras
- Peer-to-peer file sharing
- Federated identities
- iPods
- Listservs

An Expanded Ability to Affect Corporate Information By:

- Creating it
- Accessing it
- Downloading it
- Copying it
- Altering it
- Disclosing it
- Forwarding it
- Distributing it
- Destroying it
- Losing it (e.g., laptop, USB drive)
- Letting others do the foregoing

Data Portability Is A Business Necessity

- Employees need the ability to easily transport data into or out of of the organization
  - Electronically – e.g. via E-mail or IM or Internet
  - Physically – e.g., via USB drives or Laptops
- But this allows unauthorized –
  - Sending of confidential corporate data out
  - Bringing viruses, infringing material, etc. in

Remote Access
Is A Business Necessity

- Employees often require remote access
  - While traveling / working from home
  - Laptops / home computers / PDAs
- But who are you letting in? Consider –
  - Shared/compromised passwords
  - Phishing / social engineering
  - Federated identity
  - Computers left logged in

Top Data Security Breaches

- 39% -- Confidential business information
- 27% -- Personal customer/prospect information
- 14% -- Intellectual property
- 10% -- Personal employee information
- 16% -- Other / unknown

Ponemon Institute, January 2005

Possible Legal Impact of Employee Activity

- **Breach of legal obligation –**
  - **To provide security for corporate data**
  - **To protect privacy of personal information**
- **Loss of trade secrets or disclosure of confidential information**
- **Corporate fraud**
- **Failure to comply with Sarbanes-Oxley**
- **Inability to enforce rights (evidentiary)**
- **Potential liabilities to stakeholders**

Managing the Legal Risks

Develop a comprehensive, written, legally compliant, security program

Requirements for "Legally" Compliant Security

- Conduct asset assessment
  - Identify what needs to be protected?
- Conduct risk assessment
  - Identify and evaluate threats, vulnerabilities, and damages
  - Consider available options
- Develop and implement security measures
  - That is responsive to the risk assessment
- Address third parties
- Continually monitor, reassess, and adjust the program
  - To ensure it's effective
  - To address new threats, vulnerabilities, and available options
  - Obtain independent audit

Employees and Legally Compliant Security

- Identify employee risks
- Administrative/organizational/procedural security measures
  - required by most laws
- Access control
  - required by most laws
- Education and training requirements
  - Employees don't understand the risks
- Monitoring and enforcement requirements
  - Employees know best how to circumvent security

Two Key Trends

- **Information security is a corporate legal obligation**
  - **Employees are a key component**
- **Most companies that suffer information security beaches**
  - **are viewed as the culprits (for failure to implement appropriate security),**
  - **rather than the victims of a crime**