

Data Security

Preventing and Controlling Employee-Caused Breaches

Robert M. Jaworski, Esq.
(rjaworski@reedsmith.com/609.520.6003)

ReedSmith

The business of relationships.™

May 5, 2010

Introduction

- Employees cause data security breaches, prompting notification letters and resulting in class action lawsuits and government attention
- Proper administrative safeguards and monitoring can reduce the risks posed by employee misconduct
- This oversight must be balanced with the privacy expectations of applicants, borrowers and employees

What Privacy Risks Do Employees Create?

Rise of Breach Notice, Class Actions
and Government Enforcement

Breach Notices

- 45+ States and jurisdictions have letters requiring notice of data security breaches
- GLBA and now HIPAA have the same
- May have to send letters when personal information is lost or stolen
- Tens of millions of such letters sent, bringing bad press, lawsuits, and government investigations

Employees Cause Breaches

- Employees identified as a prime source of identity theft risk in two studies:
 - Kroll Global Fraud Report - Annual Edition 2009/2010
 - Verizon Business RISK Team, 2009 Data Breach Investigations Report
 - ReedSmith has advised on over 150 data breach incidents over the past 5 years and employees were actors and/or victims in most incidents

When Insiders are The Cause, Breaches are Bigger

- Shows that more than 20%+ of breaches were caused by employees
- About half were IT administrators, half were end-users
- When the cause of a breach is internal, median number of records compromised almost triples (100,000 vs. 37,847)
- Time and opportunity to avoid detection

Employees Have a Variety of Means to Cause Breaches

- About 2/3 of such breaches were deliberate, and the remainder were accidents
 - Abuse of system access/privileges
 - Violation of PC/e-mail/web-use policies
 - Violation of other security policies
 - Embezzlement

Employee Breaches are a Major Source of Class Action Litigation

- More than 300 class action suits arising from data security breaches have been filed in the U.S., fueled by tens of millions of data security breach notification letters sent
- Reed Smith has defended dozens of such class actions – 50+ arose from employees stealing valuable personal information from their workplace
- Most privacy class actions seek millions or billions in statutory penalties, even absent any out-of-pocket harm to consumers
- Securities and derivative cases have followed security incidents
- No jackpot recovery for plaintiffs yet, but settlements involving tens of millions of consumers have been brokered

Allegations Against Employers in Private Class Actions

- Negligent hiring and retention
- Negligent supervision
- Breach of contract or implied promise to safeguard information
- FCRA and other federal statutory claims
- Violations of state breach notification and other state privacy laws
- Federal Computer Fraud and Abuse Act (FCFAA)
- Violations of industry or type-of-information specific laws
- Infringement of supposed property or constitutional rights

Employee Breaches are a Major Source of Government Investigation

- The FTC has brought more than a dozen privacy-related enforcement actions
 - Imposing civil penalties and fines of up to a combined \$15,000,000
 - Includes a \$2.25 million consent resolution amount from CVS/Caremark for alleged improper disposal of pharmacy and credit card records (resolution also imposed a 20 year corrective action plan)
- HIPAA-related investigations on the rise
- State Attorneys General are newly-empowered

WHAT CAN COMPANIES DO?

Reducing Risk of Employee Misconduct
and Enterprise-Wide Liability

Data Security: Know and Assess What You Have and What You Need

- Take stock of what personal information your business maintains, and what laws apply to the information
- “Sensitive data” includes social security numbers, credit card or financial information, medical information, drivers license numbers, and, in some states (e.g., CT, NY), passport numbers, mother’s maiden name, personal e-mail addresses, and more
- Check everywhere sensitive data might be stored - both on-site and off-site
- Assess the type of information you collect at each entry point
- Scale down information – Keep only what you need

Data Security: Trace The Flow of Sensitive Information

- Who sends personal information to your company?
 - Applicants/Borrowers
 - Credit bureaus
 - Financial institutions
 - Other businesses
- How does the business receive personal information?
 - Websites, call centers, vendors/service providers
 - By mail or email

Data Security: Protect The Information You Keep

- Determine who has access and who should have access
- Limit access to those with a legitimate business need
- Lock Up Information – and train your employees to do so too!
- Develop written policies and procedures for administrative, physical and technical safeguards of sensitive information.
- Assure your business has in place effective security measures for networks, devices, laptops and PDAs
- Place controls on outflow
- Work with Tech Team to monitor access and detect unauthorized entry into systems and information

Data Security: Properly Dispose of the Information You Don't Need

- Only collect and maintain data for which you have a legitimate business necessity
- Develop a written records retention policy to identify what information must be kept, how to secure it, and how long to keep it
- Dispose of information properly and securely when no longer needed

Reducing Enterprise Risk: Insurance for Privacy "Losses"

- Good news is that many of the potential losses discussed may be subject to mitigation through insurance
- Specialized market developing with respect to cyber- and privacy risk
- Traditional policies may also be responsive
- Timeliness of carrier notice is key

Data Security: Background Screening

- Background checks required for certain government-related work and in certain industries (mortgage bankers/brokers/originators)
- When conducting background checks, be uniform for everyone applying for the same position
- Be aware of privacy restrictions on background screening (FCRA and state law consent and adverse action rules, restrictions on employer reference checking, fingerprinting restrictions)
- Before taking action on results of screening, consider job-relatedness and discrimination concerns

Data Security: Train, Train, Train

- GLBA, HIPAA, and Massachusetts data security regulation require ongoing training of employees
 - During orientation and periodically – don't simply parrot policies
 - On the importance of data privacy and security
 - On computer security systems
 - On storing and transporting personal information offsite
 - Save training materials, get signed certification, consider testing and surveys to reinforce training (www.onguardonline.gov)
 - Require sign-off on policies and/or Data Security Agreements and maintain certificates in personnel files
 - Don't forget temporary workers and contractors

Data Security: Train on Breach Response

- Of the companies suffering breaches in the *Verizon* report:
 - Only 32% had an incident response team in place
 - Only 28% had a written incident response plan
 - Only 25% had incident awareness and response training
 - And only 2% had regular mock incident response training
- Delay in breach response one of the biggest problems, especially with drop-dead deadlines like those imposed by HIPAA or under some state statutes (e.g., Florida's 45 days)
- Designate a Response Plan Coordinator and plan ahead in the event of a data breach
- Train personnel beyond legal and compliance, including IT, facilities, operations, HR, etc. to recognize and respond to data breaches

Data Security: Discipline Employees for Misuse of Personal Information

- Required by GLBA, HIPAA, and the Massachusetts regulation
- In breach situations, may complicate the ability of the company to obtain information needed to comply with notice obligations
- Criminal prosecution of employees sometimes pursued
 - Computer Fraud and Abuse Act (CFAA)
 - But see N.J. v. Riley – State computer crime law not intended to criminalize employee access gained in ordinary course of business, even if that access violated internal workplace policy

Data Security: Cut Off Access at Termination

- Identified as crucial window during which misconduct can occur
 - In February 2009, Washington Post reported a study by the Ponemon Institute, a Tucson-based research group, that revealed nearly 60% of employees who quit or are asked to leave a job are stealing company data
- Especially in a down economy, failure to immediately terminate access to confidential and proprietary business and other sensitive information is the most common problem

Data Security: Cut Off Access at Termination

- Even in voluntary termination situations, employees may take information assets (e.g., contact lists with personal information about clients)
 - Ponemon Institute credits cavalier attitudes toward data theft, including a lack of employee loyalty and telecommuting; increased mobility blurring the line on who really controls the information
 - Most common information taken include email lists (65%), non-financial business information (45%), customer contact lists (39%) and financial information (16%)

Data Security: Post-Termination Measures

- May be obvious, but access needs to be turned off, badges handed in, passwords changed, remote access doors closed, etc.
- As to IT administrators, prospects for remote access should be double-checked – was a backdoor left open?

How Can Companies Reduce Privacy Risks Without Creating New Privacy Problems?

Additional Tips for Balancing
Employee Rights with Best Practices

Personnel and Medical Files – Heightened Sensitivity

- Collect only what you need and what is reasonably related to a legitimate business or management objective
- Secure the files (lock them up, encrypt data and restrict access to those with business-related need to know)
- Separate medical, workers' comp, FMLA, OSHA, employee drug test records + I-9 forms from other files
- Abide HIPAA obligations, whether as plan administrator or plan sponsor
- Approach requests for access by third parties and under subpoenas with caution

Social Security Numbers

Take special care with Social Security Numbers

- Watch out for state laws (e.g., CA, IL, NJ, PA)
- Assign random numbers rather than social security numbers to identify employees
- Communicate to employees the company policy/practice not to use social security numbers as identifiers

Employee Monitoring and Surveillance

- Develop Information Systems/Usage Policies
 - Assure legal compliance
 - Electronic Communications Privacy Act
 - Stored Communications Act
 - State Wiretapping Laws
 - Clearly communicate systems owned by company
 - Discourage use/storage of private information
 - Advise deleting does not always erase files
 - Prohibit secret passwords, or at a minimum communicate that passwords are intended to prevent outside intrusion and are not an indication that an employee has any privacy rights in the content on the computer

Employee Monitoring and Surveillance

- Communicate notice of intent to monitor and the frequency and purpose of monitoring
- Express notice and consent – obtain employee acknowledgment
 - Communicate that monitoring extends to employee access to yahoo, msn and other email accounts
 - Monitor only what there is a business-related need to know
 - Stengart v. Loving Care Agency, Inc.
 - Global Privacy Partner v. Yessin

Employee Monitoring and Surveillance

- Beware your duty to monitor certain activities
 - *Doe v. XYZ Corp.*
 - *Maypark v. Securitas*
 - *Sigler v. Kobinsky*
 - *United States v. Ziegler*
 - *Delfino v. Agilent Technologies, Inc.*
- Various state statutes imposing affirmative obligation on computer technicians or internet service providers to report child pornography if then encounter it in the scope of their work (e.g., AR, IL, MI, NC, OK, SC)
- Inform employees in policies that company will cooperate with criminal investigations
- Train employees responsible for monitoring to promptly investigate allegations of unlawful conduct

Employee Monitoring and Surveillance

- Don't undermine your own policies!
 - *City of Ontario v. Quon*
 - *Pure Power Boot Camp v. Warrior Fitness Boot Camp*
 - *Watkins v. L.M. Berry & Co.*

Employee Monitoring and Surveillance

- Carefully implement any physical surveillance
 - Beware federal laws – NLRA
 - Some states require posting of notice (e.g., CT)
 - Others limit types and location of permissible surveillance (e.g., CA, DE, CT, NY)
 - Think twice about vehicle tracking and eavesdropping devices, as they are illegal in some states (e.g., CA, NY)

Employee Monitoring and Surveillance

- Be cautious in approach to workplace searches, including drug tests
 - Weigh negative employee relations with need for searches, i.e., to prevent illegal activity, theft or to provide greater safety
 - Provide notice, through policies and postings
 - Provide guidelines and training for employees performing searches – will help limit liability for invasion of privacy and other claims

Claims Against Employers by Employees Include:

- General Negligence
- Breach of federal and state statutes and regulations imposing affirmative duties to protect personal information
- Privacy/Intrusion Claims
- False Imprisonment/Battery
- Defamation Claims
- Emotional Distress Claims
- Violations of Employment Agreements or Union Collective Bargaining Agreements
- Wrongful termination and Whistleblower Claims

Questions?

Robert M. Jaworski, Esq.
rjaworski@reedsmith.com
609-520-6003