



Protecting Information from the “Insider Threat:”

When Good Employees Go Bad

By Joshua Mates

SF Bay InfraGard Quarterly Meeting

November 17, 2011

Overview

- ▶ Why Is This Important?
 - ▶ Information Protection in the Employment Context
 - ▶ Employer Limitations--Focus on the California Right to Privacy
 - ▶ Practical Pointers
- **Objective:** *Raise issues/awareness (not rid companies of all insider threats)*



Why Is This Important?

- ▶ Confidential information is critical to the success of business
- ▶ Protection of valuable intellectual property is essential
- ▶ To further business, employees must have access to confidential information and must create IP
- ▶ Employers have legal obligations to keep certain information confidential



Why Is This Important?

- ▶ What can happen if confidential information is improperly disclosed? Obvious examples:
 - ▶ Lose trade secret protection
 - ▶ Lose ability to obtain a viable patent
 - ▶ Lose race to the market
 - ▶ Lose value of the business
 - ▶ Violate legal obligations



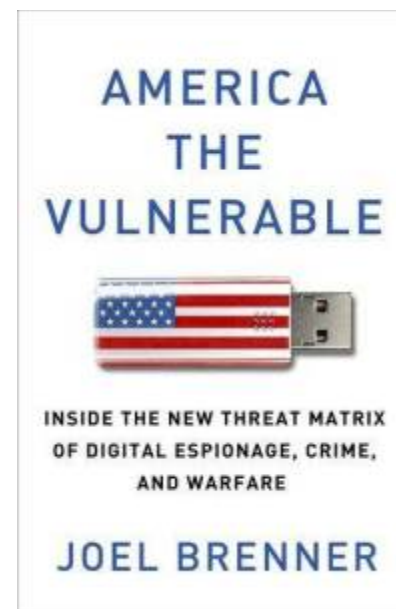
→ *Important to think about whether, when and how employees can access company confidential information*

Why Is This Important?

- ▶ **Many companies don't focus on these issues, especially with electronic information**
- ▶ 2011 Report: *"73 percent of companies surveyed had been hacked, but 88 percent of them spent more money on coffee than on securing their Web applications."*
 - ▶ Cited in Joel Brenner's AMERICA THE VULNERABLE (2011)



Joel Brenner, former Senior Counsel
at the National Security Agency



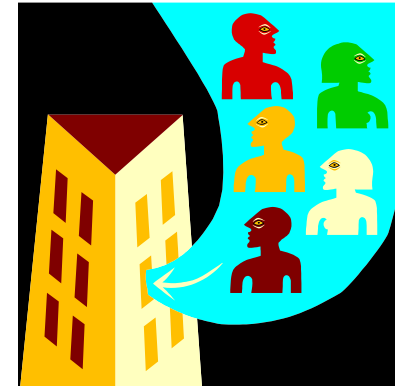
- ▶ Employer goal:

Protect company information, including from applicants, employees and former employees.



Information Protection in the Employment Context

- ▶ Employment situations:
 - ▶ Hiring
 - ▶ Managing Existing Employees
 - ▶ Separation
- ▶ At all times, employers should consider:
 - ▶ Access
 - ▶ Use
 - ▶ Monitoring
- ▶ **Note:** There are limitations to what employers can do.



Employer Limitations

- ▶ Statutes and court holdings limit employers' abilities.
- ▶ Hiring – Discovering information about job applicants
 - ▶ Fair Credit Reporting Act (California corollary)
 - ▶ Discrimination statutes
 - ▶ Right to association
- ▶ Monitoring Employee Conduct – Confronting employees suspected of wrongdoing
 - ▶ Tort law – false imprisonment; emotional distress
 - ▶ Cal. Labor Code §432.2 – no employee polygraph tests
 - ▶ Laws regarding wiretapping
 - ▶ Laws regarding personal lives of employees
 - ▶ Constitutional right to privacy



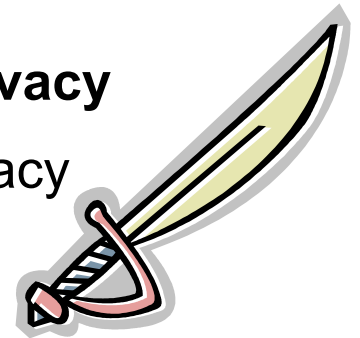
Employer Limitations – Focus on Cal. Right to Privacy

- ▶ “All people are by nature free and independent and have inalienable rights. Among these are ... pursuing and obtaining safety, happiness, and privacy.” (Cal. Const., Art. I, Sec. 1)
 - ▶ Balancing Act:
 - ▶ Employer’s need to ensure confidential information does not fall into the wrong hands
- vs.**
- ▶ Employee’s right to privacy






Employer Limitations – Focus on Cal. Right to Privacy

- ▶ Claim for Breach of the Right to Privacy:
 - 1) There is a **legally-protected privacy interest**
 - 2) The employee has a **reasonable expectation of privacy**
 - 3) There is a **serious intrusion** on the employee's privacy




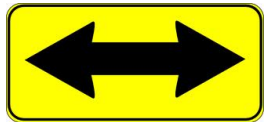

- ▶ **Defense:** Breach can sometimes be justified by a competing employer interest
 - ▶ **Most cases:** balance employee and employer interests
 - ▶ Factors to be considered include business customs, practices, and employee notice and consent



- ▶ Can an employer ...
 - ▶ Film restrooms or changing-rooms? 
 - ▶ Set up a hidden camera, operating only after-hours, to catch an employee viewing inappropriate websites? 
 - ▶ Secretly record or eavesdrop on private employee conversations, made on work phones during business hours? 

Employer Limitations – Focus on Cal. Right to Privacy

▶ Can an employer...

- ▶ Inspect an employee's web browsing history on a work computer, where the employee consented to company policy that computers could only be used for business purposes? 
- ▶ Read privileged attorney-employee communications on a work e-mail, where the employee consented to company policy of monitoring e-mails? 
- ▶ Read employee communications on a private e-mail account accessed by web browser from a business computer? 

Practical Pointers - Contracts

- ▶ Require all employees to sign ***proprietary information agreements***
 - ▶ Define “confidential information”
 - ▶ Explain do’s and don’t’s
- ▶ Require job applicants to sign ***non-disclosure agreements***



Practical Pointers – Handbook Policies

▶ Adopt **electronic data and computer use policies**

- ▶ Employer-allowed use of email and computers
- ▶ Employer ownership of all data on work computers
- ▶ Limit personal use
- ▶ Employee consent to monitoring and inspection
- ▶ Could include restrictions on social media use

▶ ***Remember:***

Expectation of privacy (or lack thereof)
could be key



Practical Pointers – Training

- ▶ ***Train employees*** about confidential information
 - ▶ Definitions
 - ▶ Use
 - ▶ Need-to-know basis (even within company)
- ▶ Hold **company-wide trainings** on computer use policies and electronic data confidentiality
 - ▶ (America the Vulnerable)



Practical Pointers – Monitor Use

- ▶ **Monitor** computer systems for suspicious activity
- ▶ Check **employee email** for warning signs (e.g., large attachments sent to personal email address)
- ▶ **Investigate** suspicious behavior



Practical Pointers – Eliminate the Opportunities for Data Theft

- ▶ **Adopt different data access filters** based on employee position
- ▶ **Encrypt** data on all mobile devices that are removed from the office (e.g. laptops, flash drives)
- ▶ Where possible, **automate security software updates**
 - ▶ (America the Vulnerable)



Practical Pointers – Exiting Employees

- ▶ Conduct detailed exit interviews
- ▶ Remind employees of continuing obligations
- ▶ Ensure immediate access cutoff and return of property
- ▶ Remain on the lookout for suspicious behavior



QUESTIONS?

