Employee Data Theft: Guarding the Gates in a Virtual Age

Presented by:

Margaret Santen Hanrahan, Esq.
Gary Berger – Director of Technology, Chief Security Officer
Ogletree, Deakins, Nash, Smoak & Stewart, P.C.
“They have computers. . .

. . . and they may have other weapons of mass destruction.”

-- Janet Reno
Feb. 27, 1998
Why Employees Steal

“I need this stuff for my new job”

“It’s a fringe benefit”

“I deserve it”

“Everybody does it; it isn’t really stealing”

“It’s so easy”

“Nobody cares; they expect it”

Greed

“The organization can afford it”
What is Employee Data Theft?

- Everyday employees have access to a wide variety of electronic information ranging from:
  - **important** (email lists and non-financial business information)
  - **confidential** (customer information)
  - **private** (employee records)
  - **business records**
Why Is This So Concerning Now?

• Current technology affords many methods for an employee to take large amounts of data from the Company.

• USB ports, smart phones, I phones, i pads and the like are easily concealed, ready to use, can hold vast amounts of data, and allow easy upload to the internet and other public forums.
What Employees Steal
Most Frequently Stolen Data

- Non-financial business information (45%)
- Customer contact lists (39%)
- Employee records (35%)
- Financial information (16%)
Some High Profile Examples: No Industry is immune

• **Bank of America (2011)**
  – Former Bank of America employee admits to stealing sensitive customer data and giving the data to scammers who then used the information to commit fraud against the customers. Theft left the bank with an estimated $10 million loss.

• **Disney (2011)**
  – Former Disney Secretary admits to stealing corporate secrets and then provide them to her boyfriend who tried to sell the data to investment firms.

• **Health Net (2010)**
  – Employee “lost” computer disk drive containing protected health information and other private information on more than 500,000 CT residents.
  – CT attorney-general negotiated settlement to include 2 years of credit monitoring, $1 million of identify theft insurance and reimbursement for costs of security freezes.

• **Microsoft (2011)**
  – Former Microsoft employee who left the Company to go to rival Salesforce.com accused of lying about retaining over 600MB of proprietary information after he left the company.
In March 2011, hackers stole millions of names and e-mail addresses from the Dallas-based marketing firm. Epsilon handles e-mail lists for major retailers and banks like Best Buy, JPMorgan, TiVo, Walgreen, and Kroger.

A study by CyberFactors, a cyber risk analytics company, estimates that the breach could cost between $225 million and $4 billion, depending on what happens with the stolen data, Business Wire reports.
Data theft: Top 2 most expensive data breaches

Sony

Hackers obtained personal information, including credit, debit, and bank account numbers in some instances, of PlayStation Network users and Sony Online Entertainment users. After discovering there had been a breach, Sony shut down both networks temporarily.

Ponemon estimates that the breach could cost Sony and credit card issuers up to a total of $2 billion.
Employee Data Theft

*My employees would never do that . . .*
The Present Threat to Employers

- 88% of IT workers surveyed would take sensitive data or passwords if fired
- 50-75% of all e-sabotage events are “inside jobs” by disgruntled workers
  - Yahoo, eBay, Amazon – All Hacked
  - Pentagon infiltration rate = 250,000/year!
The Present Cost of Cyber Crime

- Median cost is $3.8M / year
- 90% of cyber attacks are:
  - Malicious Web attacks
  - Malicious Code
  - Malicious Insiders
- Average number of days to address a cyber attack:
  - From the outside – 14 days
  - From the inside – 30+ days
Forms of Cyber Sabotage

- Theft of Trade Secrets
- Intellectual Property Infringement
- Data Mining
- Disclosure of Confidential Information
- Harm to Reputation
- Trade Defamation
- Identify Theft (of company or person)
Cyber Sabotage–Modern Thieves

• The 10-10-80 rule . . .
  – 10% will never steal from you
  – 10% will steal at any opportunity
  – 80% may steal/destroy if:
    • Personal financial woes
    • Opportunity with low risk
    • Payback
ER’s Anti Cyber Sabotage Plan must be two-fold:

• To minimize risk of occurrence
• To recover as quickly and inexpensively as possible
What Can Employers Do?

The Three “Ps”

• Prepare
• Prevent
• Protect
Prepare: Get Your Documentation in Order

- Confidentiality/Non-Disclosure Agreements
- Work for Hire Agreements
- Receipt for Company Mobile Devices
  - Inventory of Access/Authorization Codes
  - Procedure for assigning access rights for ALL data
Protect: Create, Update, Enforce Policies

- Social Media Policy
- E-mail Policy
- Internet Policy
- Password Policy
- Return of Property
- Comprehensive Set of IT Policies
- Acknowledgement of Receipt
  - Eliminate EE expectation of privacy!
Protect: Encourage IT Best Practices

- “Must Have” Encryption and Passwords
- Flag efforts to bypass normal security parameters
- Create logs that aggregate and analyze suspicious patterns
- Disable access when not necessary
Protect: Encourage IT Best Practices

- Map queries to identify and trace inappropriate activities
- Monitor activity between EE and competitors
- Constantly vet access of high level executives
- Give Network Admins authority to browse web and read email to limit virus spread
Protect: Mandatory Termination Process

- When any EE leaves, for any reason:
  - Manual override and reboot to prevent remote hijacking
  - Retrieve all mobile devices ON THE SPOT
  - Establish IT procedures to shut EE out of the system completely and permanently
Prevent: Be Vigilant

- Keep open communication between HR, IT, operations, executives
- Never give someone all the cards
- Nip defiant or suspicious behavior in the bud
- Investigate thoroughly/promptly
- Vet third parties before granting even limited access
- Monitor your brand and reputation online
  - Google alerts
  - TweetBeeps
Prevent: Audit Cyber Policies and Procedures

• Conduct full, regular audits
  – Look at Internet/e-mail use and systems
  – Assess effectiveness of current policies
  – Identify all practices that regulate email/data access/web access
  – Determine if federal/state wiretap or privacy laws limit your options
Audit physical resources and security protocols
  - Card access
  - Video surveillance
  - Limited access to/locked personnel files and other confidential business records
  - Routine security audits
• Monitoring concerns: beware of pitfalls and potential liability
• Key = Employee’s “Reasonable Expectation of Privacy”

• Employer’s Policy Critical
  – All Systems and Data owned by Employer
  – No “Expectations of Privacy” regardless of when/from where system accessed
  – Right to Monitor and Search at any time
Fight Back

- Liaise with local police department
- Report crime to FBI, Secret Service or DOJ Internet Crime Division (most employers don’t!)
- Sue employees where possible
- Encourage criminal prosecution
Federal Statutes Specific to Cyberspace

- Electronic Communications Privacy Act (ECPA)
  - Unauthorized access
  - In transit (wiretapping)
  - Stored

- Computer Fraud and Abuse Act (CFAA)
  - Access to protected computer
  - Fraudulent purposes (to obtain value)
  - For destructive purposes (vandalism, virus)
Common Law Applicable to Cyberspace

- Conversion
- Intentional interference with business relationships
- Breach of contract
- Breach of fiduciary duty or duty of loyalty
- Equitable claims, when an employee unjustifiably benefits from misconduct
- Invasion of privacy
State Laws Applicable to Cyberspace

- MA: Theft of ESI via computer is larceny
- UT: Cyber-attacks are criminal
- GA: Lock-out, corruption, deletion illegal
- SC: Computer crime and hacking illegal
- MO: “Tampering” illegal
- PA: Computer offenses and hacking illegal
- NJ: Unauthorized password use illegal
- State Trade Secret Laws
Do’s and Don’ts When You Suspect Employee Data Theft

• Check for Signs of Misappropriation
  – Recent access
  – Evidence of downloads

• Mirror Image of Hard Drive and Server Sections

• Retain Forensic Expert?

• Severance Agreement - confidentiality provisions

• Take Action
Theft or Disclosure of Trade Secrets/Confidential Info

- ER (rehab facility) documents e-mailed to home PC
- ER documents used to set up competitive business
- EE did not violate CFAA
  - because he had “authorized access”
  - ER had no confidentiality agreement
Theft or Disclosure of Trade Secrets/Confidential Info

- 2 current fitness company EEs plan to compete
- EEs steal passwords, info, and trade secrets
- ER accesses e-mail for evidence
- ER sues for theft, copyright infringement, unfair competition
- EEs countersue for violations of Stored Communications Act (SCA) and ECPA
Result

- Settled . . . of course

- You can’t catch a criminal with a crime
- Make sure your investigation is lawful
- Employers violate Stored Communications Act
Questions?