Competitive Intelligence and Corporate Espionage – The Sword and the Shield:

A Primer on What is and is not Permissible Information Gathering and How To Protect Your Company’s Intellectual Property and Trade Secrets from Attack

December 13, 2007

Presented by the New Jersey Corporate Counsel Association through its Technology Industries Committee

Sponsored by Duane Morris

Sandra A. Jeskie
Partner, Duane Morris

Jon Olson
Division Counsel, Alcatel-Lucent

Eugene Weitz
Global Technology Lawyer, Alcatel-Lucent
WHAT WAS THE SUBJECT OF THAT BIG MEETING YOU WENT TO LAST WEEK?

ALL THEY TALKED ABOUT WAS TRADE SECRETS, TRADE SECRETS, TRADE SECRETS!

THEY MADE SUCH A BIG DEAL ABOUT IT THAT AS SOON AS I GOT BACK TO THE OFFICE I ACTED ON IT RIGHT AWAY --

I CALLED MY FRIEND BOBBY AND TRADED TWO BIG SECRETS WITH HIM.
Uniform Trade Secrets Acts ("UTSA")

"Trade Secret" defined as:

- information, including a formula, pattern, compilation, program device, method, technique, or process, that:

  (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and

  (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

UTSA §1.
Security Statistics

- Over 70 million security breaches
  - 4% - Lost backup tapes
  - 7% - Unauthorized access to documents
  - 19% - Human Error
  - 25% - Hacking
  - 45% - Stolen/lost computer or portable devices

Privacy Rights Clearinghouse
The Threat Within

- Inadvertent disclosures
- Use of unapproved devices
- Carelessness
- Lack of training
- Theft
Recent Thefts of Trade Secrets

● Coca-Cola
● Morgan Stanley
● Boeing
● Duracell
Disposal of Corporate Information
Dumpster Diving
Laptops
Flash/Thumb/USB Keychain Drives
iPhone/ iPod/ MP3
PDAs
Cameras

- PDAs
- Pen Cameras
- Wristwatch cameras
E-Mail and File Storage

- E-mail sent to personal accounts or put on personal lap tops
- Work files stored on personal devices or web backups
- Inadvertent disclosures by e-mail
  - the Eli Lilly example
Instant Messaging

IM with davisrefdesk from hmcpherson0893

hmcpherson0893 (11:48:52 AM): Hi, I am looking for an article by Bloss called "Cohabiting, Decohabiting, Recohabiting: The Routes Followed by Two Generations of Women." Could you help me?

davisrefdesk (11:49:20 AM): Sure, have you tried looking in any of the Library's databases?
P2P software

- P2P Software is installed at least once in 77% of companies
Managed Dedicated Server BLOG | FastServers.Net

March 6, 2007

The iceman cometh...with a hacker in tow.

Cedar Falls hit with an ice storm...our customers hit with a MokEnable exploit.

Continue reading "The iceman cometh...with a hacker in tow." »

March 5, 2007

Daylight Savings Time - Fix for Windows 2000 Servers

As my compadre TL mentioned last week on this blog, a change in DST ([Daylight Savings Time]) for the nation has resulted in the need for an update of timezone data for all servers within our network. While for most machines, this can be resolved with a simple vendor-supplied patch, users supporting their own OSes that are no longer covered by vendor support (IE, Windows 2000) appear to be left out in the cold regarding this change. Fortunately, by using commonly available tools, Windows 2000 users are able to modify the timezone data on their local machine to reflect this new change. Read on for more information!

Posted by Steven Anderson at 2:50 PM | Read the post
Delaware

Delaware (IPA: /dəˈlaʊrə/) is a state located on the Atlantic Coast in the Mid-Atlantic and Southern regions of the United States[3]. The state is named after Delaware Bay and River, which were named for Thomas West, 3rd Baron De La Warr (1577–1618).[4] Population estimates by the Census Bureau for 2005 place the population of Delaware at 843,524. Despite being the 49th most populous state, it is the seventh most densely populated state, with a population density of 320 more people per square mile than the national average, ranking ahead of states such as Florida, California, and Texas.[5]

Contents

1 State nickname
2 Geography
   2.1 Topography
   2.2 Climate
3 History
   3.1 Native Americans
   3.2 Colonial Delaware
   3.3 American Revolution
   3.4 Statehood and race
4 Demographics
   4.1 Languages
   4.2 Religion
5 Economy
6 Transportation
Wireless Security
Best Practices - The Use of Technology

- Identify trade secrets and proprietary information
- Conduct a risk assessment
- Develop a Technology Compliance Plan
- Train employees
- Audit regularly
Outsourcing and International Risks

- Proving ownership of intangible trade secrets is difficult
- Foreign countries do not always recognize or offer protection for trade secrets in a similar manner
- Foreign countries may not enforce laws
Outsourcing

“A company that is subject to U.S. laws is responsible for the use and maintenance of consumer information in accordance with those laws. . . . Simply because a company chooses to outsource some of its data processing to a domestic or off-shore provider does not allow that company to escape liability for any failure to safeguard information adequately.”

Timothy J. Muris, Chairman, FTC
Best Practices in Outsourcing

- Due diligence in outsourcing firms
  - Background checks
  - Review company’s history
- Monitor technologies used
- Train partners
- At termination, remove data
The Threat Outside - Competitive Intelligence and Business Espionage

- Business Espionage/
- Economic Espionage
- Industrial or Commercial Spying
Economic Espionage

- The U.S. Attorney General defined economic espionage as:

  “the unlawful or clandestine targeting or acquisition of sensitive financial, trade, or economic policy information, proprietary economic information, or critical technologies.”

  *Economic Espionage and Industrial Spying 2005*
Competitive Intelligence

- Competitive Intelligence is defined as:

  “a systematic and ethical program for gathering, analyzing and managing information that can affect a corporation’s plans, decisions and operations.”

  *Nasher, Economic Espionage and Industrial Spying*
Examples of Business Espionage

- Maytag “Front Loader”
- Ringling Brothers
- Oracle
- SAP
- HP
90% of large companies have CI staff and many large U.S. businesses spend more than a $1 million annually on CI.

*Economic Espionage and Industrial Spying 2005* (citing *Business Week 2002*)
Legal Collection of Competitive Intelligence

- Public records (on-line databases, industry periodicals, competitors’ promotional documents or a review of annual reports, patent filings)
- Trade shows
- Attendance at conferences and seminars
- Analysis of competitor’s products
- Customer surveys
- Visual observation of a competitor’s site
- Dumpster diving?
Restatement of Torts (1939)

- "The privilege to compete with others includes a privilege to adopt their business methods, ideas, or processes of manufacture. Were it otherwise, the first person in the field with a process or idea would have a monopoly which would tend to prevent competition."

- "It is the employment of improper means to procure the trade secret, rather than the mere copying or use, which is the basis of the liability. . . ." Section 757, cmt a.
Economic Espionage Act of 1996

Prohibits

- theft of trade secrets or
- knowing possession or use of a misappropriated trade secret

10 years and/or $500,000 maximum

18 U.S.C. 1832
Uniform Trade Secrets Act

Prohibits

- misappropriation of trade secrets through “theft, bribery, misrepresentation, breach or inducement of a breach of duty to maintain secrecy, or espionage”

- knowing acquisition, disclosure or use of a misappropriated trade secret

Prohibits unfair or deceptive trade practices

FTC actions concerning pretexting and other deceptive practices
Other Statutes

- Federal Wiretap
- Computer Fraud and Abuse Act
- Gramm Leach Bliley
- Telco Privacy Act
- State trade secret laws
- New FCC rules to protect privacy of consumers phone records
Legal Duty to Provide Information Security

- Sarbanes Oxley, Section 404
  - “internal controls”
- Gramm-Leach Bliley
  - “safeguards rules”
- HIPAA
  - “privacy rule”
- FTC Fair Practices Standards
Best Practices

- Identify sensitive business information and trade secrets
- Conduct a risk assessment
Best Practices - continued

- Develop a Trade Secret Compliance plan and Business Ethics guidelines
  - put employees/contractors on notice
  - include confidentiality provision in contracts and other documents
  - require non-disclosure agreements
  - protect trade secrets with passwords, encryption, visitation procedures, locks on file cabinets etc.
  - identify and protect trade secrets in *any form*
  - limit access on a need to know basis
Best Practices – continued

- Develop a Document Retention Policy
  - Good litigation preparedness tool – e-discovery!
  - Ensures that documents are properly destroyed when no longer needed
  - Addresses documents in all forms
Best Practices - continued

● Develop a Data Security Plan and Incident Response Plan
  ▪ comprehensive approach for your most valuable assets
  ▪ protects the company from significant financial loss and damage
  ▪ protects customers from loss of confidential information
  ▪ contain any intrusions, restore systems and provide assistance to customers (if necessary)

▪ approach the plan from “when”, not “if”
Best Practices - continued

Develop and Enforce CI Gathering policy prohibitions:

- Collecting or using the confidential information of another improperly (e.g. misappropriation, breach of NDA)
- Exploiting new employees for confidential information
- Asking/Receiving confidential information from a supplier or customer unless you know the supplier or customer is authorized to disclose
Best Practices - continued

Usually Acceptable Methods of Gathering CI

- Gathering information at trade shows (wearing badge)
- Public Domain
  - Internet (with caveats)
  - Newspapers, magazines, technical journals
  - Court and Governmental Records
  - Press releases
- Reverse Engineering (if no prohibitions)
- Consultants
Best Practices - continued

Tougher Calls:

- Customers/Suppliers passing on information about competitors
- Consultant’s material used for others
- Information found in a non-public place (e.g., customer’s office)
- Information found in a public place
- Conversations overheard in a public place
Best Practices - continued

- Apply all policies and procedures to outside consultants, as well as employees
- Train employees
- Conduct regular audits
Questions?
WHERE TO LEARN MORE

- Society for Competitive Intelligence Professionals
  http://www.scip.org/

- Department of Justice Website
  http://www.usdoj.gov/criminal/cybercrime
THANK YOU !!!

Sandra A. Jeskie
Partner
Duane Morris LLP
30 South 17th Street
Philadelphia, PA 19103-4196
215.979.1395
jeskie@duanemorris.com

Eugene Weitz
Global Technology Attorney
Room 3A-517
Murray Hill, N.J. 07974
908-582-4820
weitz@alcatel-lucent.com

Jon W. Olson
Division Counsel
Room 3A-515
Murray Hill, N.J. 07974
908-582-0420
jwolson@alcatel-lucent.com

[ www.duanemorris.com ]