Tutorial Description

Title: The Computer Security Professional’s Role in Trade Secret Protection

Instructor: Christopher Marquart, J.D.
Associate Director
Proprietary Information Protection
Wyeth-Ayerst Global Pharmaceuticals

Summary of Tutorial Topics:

This tutorial will begin with a review the basics of domestic and international trade secret laws and subsequently reinforce these principles in a very practical way by applying them to real life scenarios. The intent is to teach computer security professionals the thought patterns which they need to adopt when establishing new security procedures or reviewing existing ones to ensure that they will meet the standards required to protect their legal interests in the intellectual property which they hold.

Speaker Bio

Mr. Marquart is an attorney currently serving as Associate Director of Proprietary Information Protection for Wyeth-Ayerst Global Pharmaceuticals, a major pharmaceutical company with operations in over 145 countries. In this capacity, Mr. Marquart is responsible for establishing information protection policy worldwide as well as ensuring compliance and investigating suspected compromises as a member of it’s corporate security division. Mr. Marquart has worked in the pharmaceutical industry for 15 years, beginning his career as a research scientist, with later assignments in manufacturing, quality assurance and regulatory. Mr. Marquart’s background affords him a unique view of how information flows through a high tech enterprise and the subsequent means needed to protect it.
NISSC 22nd

The Computer Security Professional’s

Christopher Marquart, J.D.

Proprietary Information Protection
Did you realize that you live in the “INFORMATION AGE”? 

- 1982 Brookings Inst. Study
  - 62 % Tangible Assets
  - 38 % Intangible Assets

- 1992 Brookings Inst. Study
  - 38 % Tangible Assets
  - 62 % Intangible Assets
“Indeed, the entire gamut of responses to our query on what actions were taken in the quake of intrusions seems to indicate a profound sea [of] change could be underway.”  Richard Power CSI/FBI 1999 Survey
How Long?
Proper Knowledge Management

PIP should not be viewed as a standalone security program but rather as an important part of a comprehensive Knowledge Management effort.
Chris’s 5 Minute College of Legal Analysis

Trade Secrets 101

- **Notice** - does something about the presentation of the information place the recipient on notice that it should be protected

- **Duty** - does the recipient have a legal duty to maintain confidentiality
Scenario #1: Company Proposal on Internet

- Normal practice
- Aggressive practice
- Unethical
- Illegal
Scenario #1: Company Proposal on Internet

- Normal practice
- Aggressive practice
- Unethical
- Illegal
Types of Intellectual Property

- Trademarks
- Copyrights
- Trade Secrets
- Patents
Characteristics of Trade Secrets

- No Federal Regulatory Scheme
- No Registration Required
- Very Broad Subject Matter
- Unlimited Life
- Reasonable Secrecy Must be Maintained
Current Trade Secret Legislation

**International**

- Country Specific Legislation
- General Agreement on Tariffs and Trade (GATT)

**Domestic**

- Restatement of Torts I, Section 757
- Uniform Trade Secrets Act (USTA)
- State Common Law
- The Economic Espionage Act of 1996
Definition of a Trade Secret
(Economic Espionage Act of 1996)

“Trade secret means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically or in writing if:

a.) the owner has taken reasonable measures to keep such information secret; and

b.) the information derives independent economic value, actual or potential, from not being generally known to … the public”
Review of EEA Cases

Recommended Website
Source: The Trade Secrets Home Page
by Mr. R. Mark Halligan, Esq.
http://www.execpc.com/~mhalligan
What would our burden be at trial as a Plaintiff?

- Does the information in question qualify as a “trade secret”?
- Prove that the measures taken to protect the information in question were “reasonable” under the “totality of the circumstances” (i.e., Value and importance of information, size of company etc.)

Failure to Meet Burden = NO Legal Protection
NO Chance for Rehabilitation !!!!
6 Factors Used by the Courts to Determine Trade Secret Status

- The extent to which information is known outside the applicant’s business.
- The extent to which it is known by employees and others involved in the business.
- The extent of measures taken by the applicant to guard the secrecy of the information.
6 Factors Used by the Courts to Determine Trade Secret Status

(Continued)

- The **value of the information** to the applicant and his or her competitors
- The **amount of effort or money expended** by him in developing the information.
- The **ease or difficulty** with which the information could be properly acquired or duplicated by others.
General Know How vs. Company Trade Secrets

- General GMP or GLP Compliance
- General Programming Principles
- General Accounting Practices
- General Manufacturing Procedures
- General Information

- Product Formulas
- Marketing Plans
- Specific Code
- Specific Manufacturing Procedures
- Customer Lists
- Specific Information
Scenario #2: Document on Airplane

- Normal practice
- Aggressive practice
- Unethical
- Illegal
Scenario #2: Document on Airplane

- Normal practice
- Aggressive practice
- Unethical
- Illegal
Review of Scenario

- Duty?
- Notice?
- Precautions Reasonable?
  - Value / Effort Expended
  - Known Inside / Outside the Business
  - Info Easy to Obtain / Produce
  - Current Protection Technology
Identifying Possible Threats

(ASIS Survey)

- Employees: current, former, retired, or part-time - 60%
- Vendors, Consultants, Joint Venture Partners or Subcontractors - 15%
- Outside Professionals (foreign and domestic, legal and illegal) - 25%
Competitive Intelligence Professionals

- Society of Competitive Intelligence Professionals (SCIP)
- Over 6,000 Member
- Librarian to ex-Intelligence Agency Employees
- Social Engineering (public and/or private)
- Continuum of Truth
Continuum of Truth

Total Truth

Innocuous Truth

Omissions

Half Truths

Misrepresentation

Duty ?

Notice ?

Reliance ?

Fraud
Current Threat Profile in Industry

#1 General Employee Naivete
#2 Employee Migration
#3 General Outsourcing
#4 Competitive Intelligence
#5 Globalization
Scenario #3: Int’l Phone Call

- Normal practice
- Aggressive practice
- Unethical
- Illegal
Scenario #3: Int’l Phone Call

- Normal practice ?
- Aggressive practice ?
- Unethical ?
- Illegal ?
Review of Scenario

- Duty?
- Notice?
- Precautions Reasonable?
  - Value / Effort Expended
  - Known Inside / Outside the Business
  - Info Easy to Obtain / Produce
  - Current Protection Technology
Scenario #4: Disposal of Data

- Normal practice
- Aggressive practice
- Unethical
- Illegal
Scenario #4: Disposal of Data

- Normal practice ??
- Aggressive practice ??
- unethical ??
- illegal ??
Review of Scenario

- Duty?
- Notice?
- Precautions Reasonable?
  - Value / Effort Expended
  - Known Inside / Outside the Business
  - Info Easy to Obtain / Produce
  - Current Protection Technology
Conclusion

- Apply Commonsense to Your Protection Strategy
- Don’t Try to Protect Everything
- Stay Current
- It is Better to Avoid Opportunities Which Would Lead to Litigation
- Find a Specialist if You Need to Litigate