The Present Value of Trade Secret Protection: Do the costs outweigh the benefits?

Donald A. Degnan
Joseph T. Jaros
HOLLAND & HART LLP
ddegnan@hollandhart.com
jjaros@hollandhart.com

I. Introduction.

The world's most sophisticated companies are struggling to keep their trade secrets a secret. And the struggle is becoming more difficult and more important. Technology has already made the act of stealing many types of trade secrets practically instantaneous. With the click of a mouse – or the transmission of a photograph by mobile telephone – a trade secret can be lost forever. The FBI recently estimated that, with current technology, "[t]heft of trade secrets and critical technologies is costing the U.S. economy upwards of $250 billion per year." As technology continues to advance, so will the ability of a thief to access and transmit trade secret information.

In addition, as employees become more mobile and companies become increasingly global, the opportunities for loss and difficulties with enforcement loom even larger. These issues, coupled with the expanding value of intellectual property to large and small companies, have made the protection of all types of trade secrets a challenging priority.

This paper describes the current challenge of trade secret protection, then focuses on the practical steps every company should consider to protect its trade secrets, including seeking relief under theories of inevitable disclosure and vicarious liability.

II. The challenge of trade secret protection continues to evolve.

A. Protection of trade secrets is a real problem, even for the most sophisticated companies.

Complacency can be the greatest threat to a trade secret. Although most companies have written policies concerning the protection of trade secret information, the implementation, enforcement and reassessment of these policies may not be viewed as a top priority until a trade secret has been lost. *See, e.g.*, *Trends in Proprietary Information Loss*, ASIS and PricewaterhouseCoopers (September 2002) ("proper labeling and handling of classified information is not the norm among companies" (emphasis added)). As the following recent examples suggest, even the most valuable, best-protected trade secrets are continually at risk:

- *Microsoft*: Source code for Windows 2000 and NT has appeared on the Internet;
- *Lockheed Martin*: Boeing manager conspired with a Lockheed manager to steal documents relating to an Air Force rocket program;

- *Cisco*: Unidentified person provided a Chinese company with Cisco's router source code;

- *BellSouth*: Number two executive in charge of domestic operations hired by Sprint;

- *Sun Microsystems and Transmeta*: Two men, "funded" by the Chinese city of Hangzhou, stole microchip blueprints and other technology; and

- *InstallShield*: Competitor obtained access to servers and downloaded almost 1,000 highly confidential records, including trade secrets.

The challenge of trade secret protection is even greater for companies with a global presence. The United States government recently found that "[f]oreign businessmen, scientists, academics, and government officials from more than 90 countries continued targeting sensitive U.S. technologies and corporate trade secrets in both 2002 and 2003," concluding that "U.S. openness to foreign trade and investment and the country's commitment to global information sharing through academic and scientific exchange – tools that have served as engines for economic growth – unfortunately leave U.S. technologies highly exposed to foreign exploitation." *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage (2003)* at v.

B. For many types of trade secrets, technology has decreased the cost of theft, increased the cost of protection, and made loss detection more difficult.

On February 20, 2004, Microsoft issued a press release stating that portions of its source code were "illegally made available on the Internet." The release went on to state that:

> Subsequent investigation has shown this was not the result of any breach of Microsoft's corporate network or internal security, nor is it related to Microsoft's Shared Source Initiative or its Government Security Program, which enable our customers and partners, as well as governments, to legally access Microsoft source code.

Statement from Microsoft Regarding Illegal Posting of Windows Source Code. So, how did the source code make it to the Internet? It remains unclear.

Similarly, in the most recent decision in the widely-publicized DVD decryption technology cases, the court emphasized that there was "only very thin circumstantial evidence of when, where and how" the trade secret misappropriation occurred. *DVD Copy Control Association Inc. v. Bunner*, No. H021153, 2004 WL 362414, at *7 (Cal. Ct. App. Feb. 27, 2004). In making the obvious point that information "which is in the public domain cannot be removed by action of the states under the guise of trade secret protection," the *Bunner* court affirmed a recent observation by another court:

> The court is troubled by the notion that <u>any Internet user . . . can destroy valuable intellectual property rights by posting them over the Internet</u>, especially given the fact that there is little opportunity

> to screen postings before they are made. Nonetheless, one of the Internet's virtues, that it gives even the poorest individuals the power to publish to millions of readers . . . can also be a detriment to the value of intellectual property rights. The anonymous (or judgment proof) defendant can permanently destroy valuable trade secrets, leaving no one to hold liable for the misappropriation.

Id. at *8-9 (emphasis added).

As these cases demonstrate, once a thief gains access to a trade secret, global dissemination can be practically free and instantaneous. Perhaps more importantly, even the most advanced (and costly) protection technology may not secure the most valuable trade secret, especially against a highly motivated competitor or an anonymous computer hacker. *See, e.g.*, *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage* at v (describing a wide range of techniques used to steal trade secrets, including "cyber tools" and "unnecessary airport checks to . . . download proprietary information from laptops").

C. Increasing employee mobility and globalization compound the problem.

Former employees continue to represent the highest risk factor in the loss of trade secrets. *Trends in Proprietary Information Loss* at Table 3.1. And employee mobility continues to increase. *Number of Jobs Held, Labor Market Activity, and Earnings Growth Among Younger Baby Boomers*, Bureau of Labor Statistics (August 2002). At the same time, the trend toward a global workforce continues:

> U.S. corporations are picking up the pace in shifting well-paid technology jobs to India, China and other low-cost centers . . . . Morgan Stanley estimates the number of U.S. jobs outsourced to India will double to about 150,000 in the next three years. Analysts predict as many as two million U.S. white-collar jobs such as programmers, software engineers and applications designers will shift to low cost centers by 2014.

U.S. Companies Moving More Jobs Overseas, David Zielenziger (December 23, 2003) (emphasis added); *see also America's Job Machine is Showing Signs of Life*, U.S. News & World Report (March 8, 2004); *Is the Job Market Broken?*, CNN/Money (February 9, 2004).

These trends, along with the fact that foreign competitors and on-site contractors represent the other high risk factors in the loss of trade secrets (*Trends in Proprietary Information Loss* at Table 3.1), suggest that the opportunities for loss will continue to increase as the ability to detect and prevent loss becomes a truly global challenge. *See, e.g., Annual Report to Congress on Foreign Economic Collection and Industrial Espionage* at v (describing foreign joint ventures and the use of foreign services and products as a "means of gaining access to sensitive facilities and . . . information technology networks"); *The Seven Routes for Trade Secrets to Leak Out*, Financial Times (February 9, 2004) (identifying foreign joint ventures, foreign interns and foreign suppliers as sources of loss).

D. Enforcement of trade secret rights is becoming more difficult.

The world of trade secret protection is changing in at least three significant ways. *First*, there is no longer a "typical" defendant. In the past, misappropriation occurred most often through a former employee or a competitor. Today, a thief can be an anonymous hacker, a terrorist, a disgruntled current employee, or an "innocent" Internet user in any one of dozens of countries across the world. As the *Bunner* court explained in its recent decision involving DVD decryption technology:

> The typical defendant in a trade secret case is a competitor who has misappropriated the plaintiff's business secret for profit in a business venture. In that scenario, the defendant has as much interest as the plaintiff in keeping the secret away from good faith competitors and out of the public domain. . . . [Here] the alleged misappropriators not only wanted the information for themselves, they also wanted the whole world to have it.

Bunner, 2004 WL 362414, at *8 (emphasis added); *see also Trade Secrets in the Age of the Internet*, The Tennessean (February 2, 2004) (company believed that current employee posted sales estimates and trends on the Internet); *Speech*, Bruce Gebhardt, Deputy Director of the FBI (January 12, 2004) (two computer hackers in Bucharest, Romania corrupted data on a system in a United States research station in Antarctica); *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage* at 1 ("Strong global demand for U.S. technology also creates a retail market into which middlemen – in search of profits – acquire U.S. trade secrets for sale to the highest bidder. Global trading centers are frequently only stopover points for U.S. technology illegally acquired for sale in other markets.").

Second, theft is becoming harder to detect and prove. There may be nothing more than "thin" circumstantial evidence of theft by an anonymous source. And even where the evidence of theft is stronger, the person who stole the trade secret may be judgment-proof. Both of these emerging problems can prevent the trade secret owner from proving misappropriation against subsequent users because the owner must show that the information was still a "secret" at the time the "innocent" user received it. Unfortunately, as the *Bunner* court noted, a trade secret like the DVD decryption technology can lose its "secrecy" – and therefore its entire value – almost instantaneously. Thus, for many types of information, enforcement of trade secret rights against subsequent users may be impractical or impossible. *See, e.g., Cisco Systems, Inc. v. Huawei Technologies, Co.*, 266 F. Supp. 2d 551, 555-58 (E.D. Tex. 2003).

Third, international trade secret law is far from uniform. *Balancing Private Rights and Public Policies: Reconceptualizing Property in Databases*, 18 Berkeley Tech. L.J. 773, 820 (2003). Recent examples show that attempting to enforce trade secret rights abroad may be difficult for a variety of reasons:

- Under local law, the use of certain trade secret information may not be illegal. *See, e.g.*, *The Seven Routes for Trade Secrets to Leak Out*, Financial Times (February 9, 2004) (local licensing law may authorize the use of some trade secret information); *Cisco*, 266 F. Supp. 2d at 555 (defendant argued that "the trade

secrets law of China applies to Cisco's claim, and Cisco has done nothing to show that it can satisfy the requirements of that law");

- The foreign parent of a United States subsidiary may claim that an injunction entered by a United States court is inapplicable to activities abroad. *See, e.g.*, *Davis Issues an Order to End Improper Use of Trade Secrets*, The Legal Intelligencer (December 4, 2003); and

- There may be no practical enforcement mechanism in the country where the trade secret is being used. *See, e.g.*, *Dallas Software Pioneer Accuses Former Employee of Posting Source Code on Web*, The Dallas Morning News (October 22, 2003) (trade secret owner "unable to get Russian web site removed").

In addition, for countries where a civil remedy is unavailable or impractical, criminal prosecution may be difficult or impossible: "No other country in the world has laws specifically designed to punish the theft of commercial trade secrets." *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage* at 1. Although a trade secret owner may be able to pursue relief under the Economic Espionage Act of 1996, the number of prosecutions under this Act have been relatively limited: "The Act was passed in 1996 in response to a perceived need to close a gap in federal criminal law to protect intellectual and intangible property. Prosecutions under the Act started slowly, but the number of charged crimes has increased in recent years. As of July 15, [2003,] the U.S. Department of Justice reported 24 prosecutions since 2000." *Criminal Behavior: The Government Gets Tough on IP Theft*, IP Law & Business (October 2003); *see also Economic-Spying Case May Signal a Crackdown*, Chicago Tribune (November 28, 2003) ("When Congress passed the Economic Espionage Act of 1996, corporate security watchers hoped for a crackdown on foreign intelligence agents conspiring to steal corporate America's crown jewels. Seven years later, they're still waiting. To date, U.S. prosecutors have only twice in more that 40 alleged trade secret cases gone after foreign government involvement.").

E. Trade secrets are more valuable than ever.

Recent estimates show that, on average, intellectual property assets account for approximately 70 percent of the market value of a company. *See, e.g.*, *Trends in Proprietary Information Loss* at 3 ("70 percent or more of the market value of a typical U.S. company may derive from its intellectual property (IP) assets"); *Patent Office at Center Stage*, The National Law Journal (January 15, 2001) (value of intellectual property accounts for two-thirds of market valuation of U.S. companies); *Patents are a Virtue*, Sunday Telegraph (London) (April 14, 2002) ("Intangible assets now represent three quarters of the book value of the S&P 500.").

While patent assets may represent the bulk of this value for many types of companies, the trend toward the increasing value of intellectual property assets – including trade secrets – is expected to continue. *See id.*; *Trade Secrets – The New Risks to Trade Secrets Posed by Computerization*, 28 Rutgers Computer & Tech. L.J. 227, 228 (2002).

III. A practical guide to preventing the loss of a trade secret.

Because the enforcement of trade secret rights can be practically impossible for some types of trade secret information, the implementation, enforcement and reassessment of trade secret security measures is critically important for a broad range of clients. In addition, where a trade secret has been stolen but not yet disseminated, and your client wants to pursue a civil or criminal remedy, the most important objective evidence of the existence of a trade secret is almost always the extent of the measures that the trade secret owner used to protect the information:

> [Trade secret protection] measures constitute evidence probative of the existence of secrets. One's subjective belief of a secret's existence suggests that the secret exists. Security measures, after all, cost money; a [client] therefore presumably would not incur these costs if it believed its competitors already knew about the information involved.

Metallurgical Indus. Inc. v. Fourtek, Inc., 790 F.2d 1195, 1199 (5th Cir. 1986) (emphasis added); *see also Telex Corp. v. IBM Corp.*, 510 F.2d 894, 932-33 (10th Cir. 1975) (noting that IBM spent $3,000,000 on "additional guards, television cameras, sensors, locks, safes, computer-controlled access systems, and the like" in response to attempted trade secret misappropriation).

In fact, although courts require only "reasonable efforts" to maintain the secrecy of the information, most cases involving a failure to prove that information was a "trade secret" turn on the lack or inadequacy of security measures. *See*, *e.g.*, *Overview of Intellectual Property*, 762 PLI/Pat 11, 133-34 (January 2004); *Implement an Effective Trade Secret Protection Plan – Before It's Too Late*, Intellectual Property Today (July 2003) (court's decision that trade secret owner failed to make reasonable efforts to maintain secrecy "provides a poignant and all too familiar illustration of the fact that trade secrets . . . are valueless if not properly protected" (emphasis added)).

So, how can your client minimize the risk of trade secret loss? And, at the same time, be able to provide persuasive, objective evidence of the value of a trade secret to a court or prosecutor? The answers depend on the individual client and the type of trade secret. The specific measures necessary to protect experimental modifications to a manufacturing line may differ significantly from the measures necessary to protect data transmitted across a wireless computer network. Nevertheless, for every type of trade secret, consider asking your client about its security measures at the following potential loss points:

A. Conception.

- **Do you have a procedure concerning the discovery of new trade secret information?** Many clients have procedures to document and protect potentially patentable ideas. For example, a client may require its engineers to document their work in laboratory notebooks and submit novel discoveries to an "invention committee" that determines whether the idea has commercial value and may be patentable. Your client should consider implementing a similar procedure for trade secret information. Note, however,

that your client should seek to protect the information generated as part of such a procedure from subsequent discovery in litigation (through, *e.g.*, the attorney-client communication privilege) because the initial assessment of the value of the information by an employee or the "committee" may prove to be incorrect.

- **How do you enforce this procedure?** A procedure may have no value if it is not consistently enforced. Many clients have annual, mandatory programs to reinforce certain important company policies (concerning, *e.g.*, sexual harassment). Your client should consider implementing an annual program concerning the protection of trade secret information. In addition, your client should consider creating specific incentives (positive and negative) to motivate employees to follow the policies and procedure outlined in the program.

- **Who is responsible for reassessing this procedure?** Recent examples of trade secret theft, from the Microsoft source code to the Air Force rocket information to the DVD decryption technology, have made it clear that every client needs to periodically reassess its trade secret protection measures as new technology emerges. For example, has your manufacturing client updated its security measures to prevent an employee from using a mobile telephone to transmit pictures of an experimental production line? Does your information technology client restrict the types of information that can be transmitted on its wireless networks? Can your client's employees work on sensitive company documents in an Internet café or on an airplane? More generally, where is new trade secret information generated? And how could new technology affect these areas of exposure? If your client does not evaluate these types of questions periodically, its security measures may be outdated.

B. Identification of trade secret information.

- **How do you mark your trade secrets?** Almost every trade secret case involves the issue of inconsistent designation of trade secrets. In larger organizations, there will always be some variation in the manner that employees designate information. Some employees mark everything, others almost nothing. Nevertheless, your client should consider implementing a specific policy concerning the marking of trade secret information.

- **Is your marking policy practical and effective?** Ideally, a trade secret marking policy would advise employees to consider the confidentiality of every piece of information within their responsibility and mark it accordingly. This policy would include three levels of marking: (1) trade secret; (2) confidential; and (3) no marking. This "tiered" system of marking information can provide strong evidence that a client recognizes and protects its information. On the other hand, because employees in large organizations may designate the same information at different levels, a "tiered" marking system can weaken a trade secret claim. One alternative is to instruct employees to use a mark such as "This Document Contains Confidential, Proprietary or Trade Secret Information – No Reproduction or Use Without Express Authorization" unless the employee is confident that the information is (a) known to the industry or public or (b) not protectable (*e.g.*, an internal email setting a lunch date with a friend). Most importantly, almost every

marking policy should instruct employees to use reasonable efforts to (1) evaluate the nature of information within their area of responsibility whenever practicable; (2) mark information whenever practicable (*e.g.*, using a legend for documents, emails, diskettes, compact discs, *etc*.; a sign for physical assets, such as a proprietary assembly line; a pop-up notice as part of a password window for electronic information); and (3) mark only truly protectable information (*i.e.*, do not label every document or physical asset with a legend unless it really may include confidential, proprietary or trade secret information).

- **How is the marking policy enforced?** Even sophisticated clients with well-written marking policies may find that their information is not properly marked because of lax enforcement. Here again, your client should consider implementing an annual program in which the marking of trade secret information is discussed. In addition, your client should consider periodic "audits" to ensure that the policy works and is being followed with reasonable consistency. Finally, a periodic email to all employees emphasizing the importance of the marking policy may be appropriate for some clients.

C. Use – Generally.

- **How do you limit access to your trade secrets?** Often, the best objective evidence of secrecy is the measures taken to limit access. Consider asking your client how difficult it would be for a third party to gain access to a particular trade secret. Would it require a letter password? The agreement of a single disgruntled employee? A personal connection to the head of the IT department? In addition, as the Fifth Circuit pointed out in *Fourtek* (above), security measures cost money. The more money a client spends on measures to limit access to a trade secret, the greater the likelihood that a court or prosecutor will act quickly to protect it. Consider advising your client to document the costs of its security measures.

- **Do you have a record of all persons who have had access to your trade secret?** Access records serve at least two important purposes. *First*, they can be powerful objective evidence of a trade secret where the number of persons with access is relatively small. Information that is accessed strictly on a "need to know" basis is often held to be trade secret. *Second*, access records can provide a starting point to investigate the potential loss of a trade secret. Consider asking your client to evaluate how they record access to their trade secrets. For many secrets, a court may find common measures, such as a single entry point, a visitor log, temporary visitor badges, an employee escort and security cameras, to be "reasonable." *See, e.g., Wyeth v. Natural Biologics, Inc.*, No. Civ. 98-2469 (NJE/JGL), 2003 WL 22282371, at *3-5 (D. Minn. 2003).

- **How do you dispose of material that may contain trade secret information?** "Garbage picking" remains a source of corporate espionage. Plus, simply discarding documents or other materials reflecting trade secret information can be viewed as a failure to take reasonable steps to maintain secrecy. Make sure your client enforces its policies and procedures concerning the shredding or destruction of any material (documents, computer media, old machinery, *etc*.) that may include a trade secret.

- **How often do you reassess these security measures?** Many clients evaluate and update their security measures only after a trade secret has been lost. *See, e.g.*, *Telex*, 510 F.2d at 932-33 (IBM spent $3,000,000 to improve security after a threat of misappropriation). Depending on the type of trade secret, your client should consider periodic reassessment of the technology it uses to limit and record access to its trade secrets, including measures to detect unauthorized access (such as "decoy" information). *See, e.g.*, *InstallShield files lawsuit against Wise Solutions*, M2 Presswire (July 1, 2003) ("InstallShield discovered Wise's electronic espionage after Wise sent suspicious marketing materials to several unique 'decoy' contacts that were included on InstallShield's proprietary customer lists."). Although many trade secrets will not require "state of the art" security measures,[1] a client's periodic evaluation of its measures "constitutes evidence that a secret exists."

D. Use – Employees.

1. New employees.

- **Will your potential employee sell your trade secrets?** If a potential employee indicates a willingness to use confidential information from a previous employer, your client should consider whether this employee is just as likely to "sell" your client's trade secrets to the next employer. In addition, depending on the type of employee and their area of expertise, your client should evaluate whether it may liable for this new employee's wrongdoing. *See* discussion of the theories of inevitable disclosure and vicarious liability beginning at page 15 below.

- **What agreements must an employee sign before work begins?** At a minimum, every new employee should be required to sign (1) a confidentiality and non-disclosure agreement and (2) a certification of your client's policies and procedures (in the form of a code of conduct, employee handbook or policy manual). In addition, for some types of employees, a non-competition agreement, including non-solicitation and non-recruitment clauses, may be an effective means to protect against trade secret loss. For example, a well-written, narrowly tailored non-competition agreement is an effective way to prevent the disclosure and use of "short-term" trade secrets like new product information, financial projections and acquisition strategy. However, because several states will not enforce a non-compete provision, a client should not rely on this type of provision alone to protect its trade secrets.

- **What training does an employee receive before work begins?** Employees who will have access to trade secret information should receive training on your client's trade secret policies and procedures (including the new trade secret information procedure and trade secret marking policy). In addition, your client should consider whether employees should be informed that, as part of its trade secret protection measures, the employee's computer and email use may be monitored. *See, e.g.*, *Protecting Your Trade Secrets –*

[1] For example, many clients already have the most common security measures in place (such as key cards, passwords, limitations on the transmission of confidential files, a "clean desk" policy and locked file cabinets). But even where these typical measures are sufficient, consider advising your client to reassess and update them regularly.

Does your company have an effective computer use and email monitoring policy?, The Metropolitan Corporate Counsel (September 2003).

- **Is the confidentiality and non-disclosure agreement adequate?** Although the specific terms of the agreement may vary depending on your client's needs and state employment law, your client should consider including provisions on the following key issues:

  - Comprehensive yet clear definition of "confidential information" (including a description of the types of trade secret information that the particular employee is likely to receive[2]);
  - Cross-reference to, or incorporation of, relevant policies and procedures (including the marking policy and the new trade secret procedure);
  - Use of confidential information only for the benefit of your client and only during the term of employment;
  - Disclosure of confidential information must be authorized and made only on a "need to know" basis;
  - Duration and survival of the confidentiality and non-disclosure obligations; and
  - Return of confidential information when employment ends.

2. Current employees.

- **What steps do you take to reinforce your trade secret security measures with current employees?** Current employees should be trained on all of your client's trade secret security measures periodically. These measures include:

  - Procedures for new trade secret information;
  - Policies for marking information; and
  - Policies and procedures to limit and record access to trade secret information; *see*, *e.g.*, *Wyeth*, 2003 WL 22282371, at *3-5 (listing a number of common measures, including locked and user-protected copiers, locked storage for documents, closed circuit television cameras, signed confidentiality agreements with all third parties, a "check out" procedure for sensitive documents, a marking policy specific to each company location, and periodic affirmation of employee confidentiality agreements).

[2] Some clients resist the suggestion to "list" trade secrets because of the risk that failing to include information will suggest that the information is not a trade secret. For most types of agreements with employees, a client should consider listing only the types of trade secrets that likely will be received. In other contexts, such as a listing of assets in a purchase agreement, it will be necessary to specifically identify at least some trade secrets. Of course, any "list" of specific trade secrets should be scrutinized to ensure that the failure to include an item cannot be construed as evidence that the item has little or no value, or is simply not a trade secret.

- **How do you enforce your trade secret policies and procedures?** Again, enforcement – whether by reprimand, periodic reassessment, spot checks, or annual training – can be the most important objective evidence of the value of a trade secret to a court or prosecutor. Conversely, a failure to enforce can suggest that no trade secret exists. *See, e.g.*, *People v. Laiwala*, 9 Cal. Rptr. 3d 466, 467-70 (Cal. Ct. App. 2004) (court held that alleged trade secret apparently had no economic value where trade secret owner "took no action" as a result of misappropriation).

- **Do you ask employees to sign an acknowledgement that they have received trade secret information in the course of their employment?** For some types of employees, your client should consider asking for this acknowledgement as part of an annual training program (or a periodic update of policies and procedures). Your client should consider listing the types of trade secret information that the employee has received in the acknowledgement. For some clients, a general acknowledgement signed by all employees who receive confidential information may be sufficient to deter a later claim that no trade secrets were received.

3. Departing employees.

- **Do you monitor the activities of disgruntled current employees or departing employees?** Because former employees represent the greatest threat to trade secret information, your client should consider monitoring employees who may be on their way out, even where the employee is expected to depart amicably. *See, e.g.*, *Wyeth*, 2003 WL 22282371, at *6 (long-time employee and consultant sought out competitor, then disclosed trade secret information); *PRG-Schultz Int'l, Inc. v. Kirix Corp.*, No. 03 C 1867, 2003 WL 22232771, at *2-6 (N.D. Ill. Sep. 22, 2003) (four former employees marketed a directly competitive product, then argued that the trade secret owner's product was not a trade secret); *Dallas Software Pioneer Accuses Former Employee of Posting Source Code on Web*, The Dallas Morning News (October 22, 2003) (former employee who returned to Russia posted a slightly altered version of a trade secret on the Internet).

- **Do you conduct an exit interview for every departing employee?** Many clients conduct routine exit interviews whenever practicable. However, where a departing employee has received trade secret information, a comprehensive exit interview can be critically important. Consider these steps:

  - Ask the employee to sign a certification stating that all confidential information and client property received in the course of her employment has been returned;

  - If the employee is allowed to retain any confidential information or client property, ask the employee to sign a certification identifying these materials;

  - Attempt to gather as much information as possible about the employee's career plan (to determine whether an injunction is appropriate, and whether there is a risk of inevitable disclosure (discussed below));

- Keep a detailed record of the interview, including a list of information and property returned;

- Have two client representatives participate in the interview to provide a "witness" to the statements of the departing employee and the interviewer;

- Ask the employee to sign a certification listing the types of trade secret information they received and acknowledging their ongoing confidentiality and non-disclosure obligations;

- Consider providing the employee with an "exit letter" stating that they received trade secret information, reinforcing the confidentiality and non-disclosure obligations, and outlining the risks of working for a competitor in a similar position (including inevitable disclosure and vicarious liability); and

- Consider providing a copy of the "exit letter" to the new employer.

E. Use – third parties.

1. Joint venture partners.

o **Do you expect to lose some trade secret information?** Joint ventures present a tremendous challenge to the protection of trade secrets. In many cases, parties enter a joint venture because they have complementary technologies and operate in different segments of the market. Therefore, the parties presume, the technology disclosed within the joint venture will not be used in direct competition. In practice, unfortunately, joint venture partners (and, more broadly, all types of "strategic" partners) represent a high risk factor to the loss of trade secret information. *See, e.g.*, *VLIW Technology, LLC v. Hewlett-Packard Co.*, 840 A.2d 606, 608-10 (Del. 2003) (technology provided to strategic partner under license allegedly used in a subsequent research and development partnership with a third party); *Telecom America, Inc. v. Oncor Communications, Inc.*, 31 Fed. Appx. 809, 814-15 (4th Cir. 2002) (customer database provided to strategic partner not a trade secret where provider failed to use reasonable efforts to maintain secrecy).

o **What steps have you taken to ensure that your strategic partner uses reasonable efforts to maintain the secrecy of your trade secret information?** Almost every joint venture relationship will be governed by one or more agreements. These agreements should provide the same type of practical, effective trade secret security measures as your client's internal policies and procedures. Most importantly, your client must implement, enforce and <u>reassess</u> these policies and procedures throughout the course of the relationship. In addition, consider the following common joint venture issues:

- <u>Identifying trade secret information</u> – your joint venture partner may claim that they discovered your trade secret independently, that they contributed to the conception of your trade secret, or even that your trade secret is not valuable or secret. Consider advising your client to implement an effective system to identify

and document the source of trade secret information that is disclosed or discovered within the scope of the strategic partnership.

- Marking trade secret information – many strategic partner agreements require marking of all confidential information. While both parties may follow this marking policy in the beginning of the relationship, in some cases one or both parties veer away from the specific requirements of the agreement in the later years of the venture. Your client should insist on a marking policy that is practical and effective, including a provision protecting trade secret information even if it is not always properly marked.

- Trade secret security measures – assume that your joint venture partner eventually will discover the weaknesses and gaps in your security measures. Consider advising your client that, no matter how long the relationship continues, they should treat the strategic partner like any other third party who may be seeking to discover trade secret information (*e.g.*, limiting and recording access, providing information only on a "need to know" basis, *etc*.).

- Term of the confidentiality and non-disclosure provisions – do not assume that the technology disclosed or discovered within the scope of the strategic relationship will be obsolete in three, five or seven years. Where state law permits, your client should consider whether an indefinite confidentiality term best serves its long-term interests. *See, e.g.*, *VLIW*, 840 A.2d at 613-15 (licensee argued that a five-year confidentiality provision had expired; court held that the provision was ambiguous and denied the licensee's motion to dismiss). If a fixed-term is in your client's best interest, consider including a provision making it clear that the confidentiality obligation begins to run on the date the trade secret information is disclosed or discovered.

o **Are you prepared to treat your joint venture partner like a departing employee?** Many joint ventures involve complex, entrenched business relationships over the course of several years. Nevertheless, to the extent practicable, your client should consider taking the same measures with a former joint venture partner as they have with a departing employee. *See* discussion of departing employees at page 11 above.

2. On-site contractors, vendors, customers, consultants, *etc.*

o **How do you protect trade secret information that you must disclose to third parties?** In a recent ranking of trade secret loss risk factors, on-site contractors rank third and vendors/suppliers rank sixth. *Trends in Proprietary Information Loss* at Table 3.1. Recent cases support this risk assessment. *See, e.g.*, *Thermech Engineering Corp. v. Abbott Laboratories*, No. G030381, 2003 WL 23018553, *1-3 (Cal. Ct. App. Dec. 22, 2003) (supplier worked with customer to develop a proprietary process; customer then developed a process internally based on supplier's trade secret information). Like joint venture partners, third parties who must receive your client's trade secret information should be subject to the same practical, effective trade secret security measures provided by your client's internal policies and procedures.

- **Have you evaluated your confidentiality agreement based on the specific relationship with the third party?** Many clients have a "form" confidentiality and non-disclosure agreement that almost every type of third party signs. Consider advising your client to evaluate whether the relationship with the third party requires additional security measures. For example, if your client allows its customer to view the proprietary process it uses to manufacture a good for the customer, your client may want to consider adding a provision to its standard agreement that protects against a claim by the customer that (1) the customer developed a similar manufacturing process independently; (2) the process is not a trade secret; or (3) the process was not subject to reasonable efforts to maintain its secrecy. *See*, *e.g.*, *Thermech*, 2003 WL 23018553, at *6-8.

3. Potential buyer of your trade secret.

- **Take extraordinary security measures.** A potential buyer can present an even greater risk to your trade secret information than a former employee. In fact, a "buyer" may just be attempting to gather competitive intelligence. Either way, taking extraordinary security measures is in your client's best interest: the buyer will believe that the information is a trade secret, and your client will have a solid record as a basis to enforce its rights.[3] *See, e.g.*, *Knapp Schenk & Co. Insurance Agency v. Lancer Mgmt. Co.*, No. Civ. A. 02-12118-DPW, 2004 WL 57086, at *1-3 (D. Mass. Jan. 13, 2004) (seller of trade secret sued potential buyer for misappropriation; buyer disputed receiving certain information, then argued that information was not subject to reasonable efforts to maintain its secrecy).

F. Enforcement.

The enforcement of trade secret rights is just another aspect of the trade secret owner's duty to use reasonable efforts to maintain the secrecy of the information. Like other security measures, the extent of the measures the trade secret owner uses to enforce its rights can be the most important objective evidence of the existence of a trade secret. Moreover, as employees continue to become more mobile, a court or prosecutor may ask whether your client takes immediate and consistent action against the most common threat to trade secret information: former employees.

What action can your client take as soon as a trade secret is threatened? In addition to the most common security measure – the filing of a civil action once the secret has been used or disclosed – a trade secret owner may be able to seek an injunction before actual misappropriation has occurred (and before the confidentiality and non-disclosure agreement has been breached) under theories of inevitable disclosure and vicarious liability.

[3] Your client should consider, for example, (1) using a serial number to identify every piece of information provided to the buyer; (2) providing the buyer with a general description of trade security measures and the associated costs; and (3) providing the buyer with a redacted sample of comprehensive, tailored confidentiality and non-disclosure agreements.

1. Inevitable disclosure.

Although the doctrine of inevitable disclosure has existed for decades, it is neither generally accepted nor consistently defined. *See Inevitable Disclosure of Trade Secrets: Employee Mobility v. Employer's Rights*, 3 J. High. Tech. L. 161 (2004) (describing the history and status of the doctrine). Yet, in some jurisdictions – such as the Northern District of Illinois – it is fairly well-defined and can provide a viable remedy. *See, e.g., Lucini Italia Co. v. Grappolini*, No. 01 C 6405, 2003 WL 1989605, at *18 (N.D. Ill. Apr. 28, 2003).

In general, while some courts have used "modified" versions of the doctrine, many decisions discussing inevitable disclosure focus on evidence of direct competition, similarity of positions and necessary use of trade secret information. More specifically, once a trade secret owner proves that a secret exists, a court may enjoin an employee from working for a direct competitor where (1) the employee's duties and responsibilities for the competitor are substantially the same as those for the former employer; and (2) the employee cannot perform his job for the competitor without utilizing or disclosing his former employer's trade secret information (*i.e.*, it is inevitable that the employee will use or disclose a secret for a direct competitor). *Id.*

However, recent cases prove that, before seeking relief under this theory, you should check the current law of all potentially relevant states and choose the forum carefully:

- The Third Circuit upheld an injunction based on the doctrine, finding that "Pennsylvania courts have not explicitly adopted the inevitable disclosure doctrine . . . but we predict that, under the circumstances, the Pennsylvania Supreme Court would apply it or some variation thereof." *Doebler's Pennsylvania Hybrids, Inc. v. Doebler Seeds, LLC*, No. 03-4108, 2004 WL 260781, at *1 (3d Cir. Feb. 12, 2004).

- A Michigan federal court found that Michigan's Uniform Trade Secrets Act[4] "incorporated the doctrine of an inevitable disclosure of trade secrets," yet denied relief under the doctrine, apparently because of a lack of evidence concerning the former employee's "lack of candor" or "willingness to misuse trade secrets." *Leach v. Ford Motor Co.*, 299 F. Supp. 2d 763, 775-76 (E.D. Mich. 2004).

- An Illinois federal court denied a direct competitor's motion for summary judgment because an "employer may be held liable for misappropriation of a trade secret as a consequence of hiring a competitor's employee and placing the employee in a position resulting in the inevitable disclosure or use of the trade secret." *PRG*, 2003 WL 22232771, at *7.

- A New York federal court recognized that the inevitable disclosure doctrine is viable, but denied injunctive relief because the defendant employer was not a

[4] Pennsylvania recently became the 45th state to adopt the Uniform Trade Secrets Act. *Legislature Passes Uniform Trade Secrets Act – Pennsylvania is 45th State to Adopt Model Law*, The Legal Intelligencer (February 13, 2004).

direct competitor (and the information was not, after examination, a trade secret). *Legal Sea Foods, Inc. v. Calise*, No. 03 Civ. 4958 (DLC), 2003 WL 21991588, at *3 (S.D.N.Y. Aug. 20, 2003); *but see Marietta Corp. v. Fairhurst*, 301 A.D.2d 734, 736-37 (N.Y. Sup. Ct. 2003) (noting that the "doctrine of inevitable disclosure is disfavored" in New York).

- The Ninth Circuit found that "no California court has adopted the inevitable disclosure doctrine," yet upheld a jury's finding of misappropriation that was based, in part, on an instruction concerning inevitable disclosure because "even assuming that the complained-of instructions were erroneous, any error was harmless." *Bourns, Inc. v. Raychem, Corp.*, 331 F.3d 704, 707-08 (9th Cir. 2003).

- A North Carolina state court noted that, although the doctrine had not yet been adopted, "North Carolina case law does allow for an injunction preventing an employee from working for a former employer's competitor where there is a showing of bad faith, underhanded dealing, or inferred misappropriation (justified by circumstances tending to show the new employer plainly lacks comparable technology) . . . ." *Analog Devices, Inc. v. Michalski*, 579 S.E.2d 449, 454-55 (N.C. Ct. App. 2003).

- A Texas state court "found no Texas case expressly adopting the inevitable disclosure doctrine," noted that two Texas courts had adopted "similar" and "modified" versions of the doctrine, then held that it would not decide whether to adopt the doctrine because there was no evidence that the departing employee had trade secret information that might be used with his new employer. *Cardinal Health Staffing Network Inc. v. Bowen*, 106 S.W.3d 230, 241-43 (Tex. App. 2003).

- A Minnesota federal court noted that the doctrine has not yet been adopted in Minnesota. *Leucadia Inc. v. Intermas Nets USA, Inc.*, No. Civ. 02-4146 ADMAJB, 2003 WL 366590, at *3 (D. Minn. Feb. 18, 2003).

2. Vicarious liability.

The Uniform Trade Secrets Act prohibits disclosure or use by a person who, at the time of disclosure or use, knew or had reason to know that the trade secret information was acquired illegally. *See, e.g., Newport News Industrial v. Dynamic Testing, Inc.*, 130 F. Supp. 2d 745, 750-51 (E.D. Va. 2001). Although the plain language of the statute suggests that a new employer should not be held liable for trade secret misappropriation unless the employer had a "reason to know" that its new employee had misappropriated a trade secret, a Virginia federal court recently affirmed that, under Virginia state law, "[a]n employer can be held vicariously liable for trade secret misappropriation committed by an employee within the scope of his employment." *Tao of Systems Integration, Inc. v. Analytical Services & Materials, Inc.*, 299 F. Supp. 2d 565, 575 (E.D. Va. 2004); *see also Hagen v. Burmeister & Assoc.*, Inc., 633 N.W.2d 497, .503-04 (Minn. 2001) (because neither party disputed the principle that vicarious liability for trade secret misappropriation was available, the Minnesota Supreme Court assumed, "for this case only . . . that there is no legal prohibition to vicarious liability for UTSA violations" (emphasis added)).

Therefore, at least in the Eastern District of Virginia, a new employer may be held vicariously liable for trade secret misappropriation even if the new employer did not know – and had no reason to know – that its new employee had disclosed or used a trade secret within the scope of their new employment. The same might be true in Indiana state court. On May 30, 2003, the Indiana Supreme Court granted transfer and vacated an appellate decision holding a new employer vicariously liable. *Infinity Products, Inc. v. Quandt*, 792 N.E.2d 47 (Ind. 2003). Although the appellate court recognized that "neither this court nor our supreme court has had occasion to determine whether *respondeat superior* liability is available under the IUTSA," it agreed with the logic of the Virginia and Minnesota courts, then held that, because the employee was found liable for misappropriation that occurred within the scope of his new employment, the new employer was necessarily liable (without regard to whether the new employer knew or should have known of the misappropriation). *Infinity Products, Inc. v. Quandt*, 775 N.E.2d 1144, 1151-53 (Ind. Ct. App. 2002).

3. Practical implications of these theories.

At a minimum, your client should consider using an "exit letter" to advise its departing employees of the possibility of injunctive relief under theories of inevitable disclosure and vicarious liability. Depending on the specific employee, this letter may include a description of their duties and responsibilities and the types of trade secret information received. Your client may also want to consider providing a copy of the exit letter to the new employer.

Will these additional security measures have any effect? Recent cases suggest there is still no clear answer. While neither theory may ever provide a generally accepted, widely available remedy – and while neither theory can act as a substitute for a comprehensive trade secret security program – both theories, as they develop, may continue to motivate new employers to at least consider the risks associated with hiring your client's employees.

Conversely, when hiring an employee from a competitor, your client should consider the following precautionary steps to prevent a claim under either theory:

- Ask for copies of all agreements, certifications and acknowledgements signed by the potential new employee, as well as a copy of any exit information;
- Ask for a description of their duties and responsibilities;
- Provide a complete description of the requirements of the position to the potential employee;
- Carefully investigate the issue of whether the potential employee would necessarily disclose or utilize its former employer's confidential or trade secret information in the new position; and
- Where practicable, notify the employer of the possibility of hiring its employee (or former employee) and provide a detailed description of the duties and responsibilities involved in the new position. Alternatively, ask the potential employee to obtain a letter from the employer acknowledging that the employee

can perform the duties and responsibilities of the new position without revealing confidential or trade secret information.

G. Civil litigation and criminal prosecution.

Even the enforcement of trade secret rights presents a risk of loss. While every trade secret case involves a protective order, not every client assesses the risk of disclosure to every person involved on both sides of the case, including attorneys, consultants and expert witnesses. For example, most expert witnesses are hired because of their expertise in your client's industry or their experience with your client's area of technology. This type of third party would ordinarily represent a high risk factor in the loss of trade secret information. Even though the expert is "on your side," extraordinary security measures may be appropriate (*e.g.*, limited access, no use of mobile telephone on company property, no use of notes during tour of facility, *etc*.) Before retaining the expert, consider working with your client to assess the threat of trade secret loss (including, *e.g.*, the possibility of inevitable use or disclosure). In some cases, an expert without any former or potential ties to your client's global competitors may be necessary. Here again, the use of trade secret information – even within the confines of a law firm or with "friendly" third parties – requires the same security measures used internally.

IV. Conclusion.

For trade secrets like DVD decryption technology, the implementation, enforcement and reassessment of trade secret security measures has become critically important. If the secret is stolen, its value cannot be recovered. For other types of information, such as a supplier's manufacturing process, technology has made it easier to transmit the secret to a competitor quickly and without detection. While the cost of defending a trade secret against emerging technology may continue to increase, one point remains: <u>the value of a trade secret is measured by the extent of the efforts used to protect it</u>.

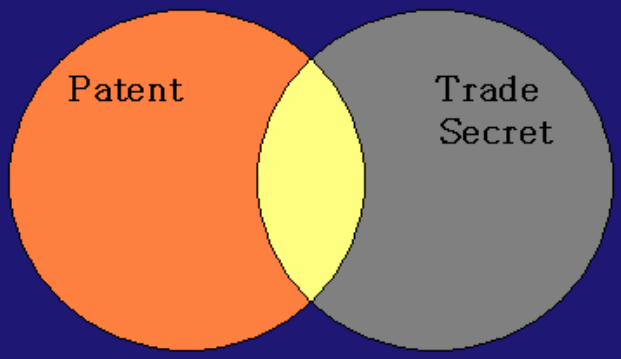
The Present Value of Trade Secret Protection:

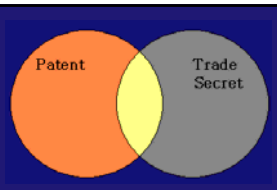
Do the Costs Outweigh The Benefit?

Donald A. Degnan
Holland & Hart, LLP

ddegnan@hollandhart.com
(303) 473-2724

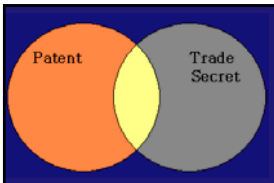
The Patent/Trade Secret Interface





Patent: Preferred Option

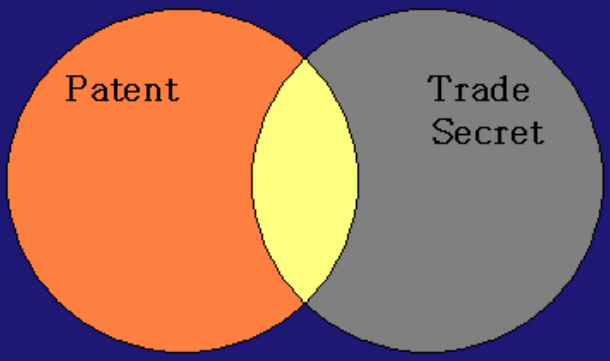
- Technology would likely be disclosed through sale of product or use of method/process
- High likelihood that technology would be reverse engineered/independently developed (*but not easily designed around*)
- It would be difficult or impractical (costly) to keep technology a secret
- No statutory bars to obtaining patent protection
- Have the funds to obtain a patent
- Need patents to attract investment capital (VC)

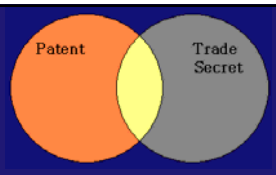


Trade Secret: Preferred Option

- Technology would *not* be disclosed through sale of product or use of method/process
- Difficult to reverse engineer/independently develop
- Steps could be taken to cost-effectively keep technology a secret
- Realistically able to take necessary steps to keep technology secret (*corporate/industry culture*)
- Not patentable subject matter

Preferred Option Uncertain





Preferred Option Uncertain

- Patentable subject matter and no statutory bar
- Difficult to reverse engineer/independently develop
- Technology would *not* be disclosed through sale of product or use of method/process
- Steps could be taken to effectively keep technology a secret (*and able to do so*)
- Additional secondary factors must be weighed

Can You Really Keep It Secret?

Statistics show misappropriation of trade secrets is on the rise

- FBI recently estimated that "theft of trade secrets and critical technologies is costing the U.S. economy upwards of $250 billion per year."
- 48% of high-tech companies have been victims of trade secret theft *(1998 National Institute of Justice Study)*
- Estimated that theft of trade secrets cost fortune 1000 companies between $53 and $59 billion in 2001 *(PriceWaterhouseCoopers study 2002)*
- Foreigners from almost 90 countries attempted to acquire sensitive information from the U.S. and U.S. companies in 2003 *(Annual Report to Congress on Foreign Economic Collection and Industrial Espionage—2003)*

Recent Headlines

FBI: Lucent Workers Stole Secrets

Associated Press

More U.S. trade secrets walk out door with foreign spies

Los Angeles Man Indicated For Theft of Trade Secrets For Stealing Information Pertaining to DirecTv's Most Advanced Conditional Access Card

c|net NEWS.COM TECH NEWS FIRST

Pair indicted in trade-secret theft

Can You Really Keep It Secret?

- **Technology** has decreased the cost of theft, increased the cost of protection, and made loss detection more difficult
- Increasing **Employee Mobility** compounds the problem
- Increased **Globalization and Global Competition** has also added to the risk of disclosure

Can You Really Keep it Secret?

New **Technology** Makes Theft Instantaneous and Tough to Detect

- **Internet**—allows quick (instantaneous) transmission of data out of company to anywhere in the world
- **CD/DVD Burners** —easy download of large quantities of data/documents
- **Flash Memory Cards** **(and other mobile data storage devices)** — miniaturization of memory makes theft harder to detect
- **Digital Cameras**—(still and video) extremely small, can transmit over internet
- **Camera Phones**—the latest problem; allow instantaneous transmission of photographs to anywhere in the world (difficult to trace)

Can You Really Keep it Secret?

Increased **Employee Mobility** presents the greatest risk of disclosure

- The workforce is increasingly mobile
  - Persons born from 1957 to 1964 held an average of 9.6 jobs from ages 18 to 36 (in 1978-2000) (*Bureau of Labor Statistics*)
  - Among jobs started by workers ages 33 to 36, 43% ended within 1 year and 76% ended in fewer than 5 years (*Bureau of Labor Statistics*)
- Senior employees pose the highest risk
  - It has been estimated that most trade secret theft (one expert estimates as high as 90%) involve senior employees
  - Senior people have access to the most sensitive information
  - A loss of a sense of loyalty to former employees is also a contributing factor (layoff rage)

Can You Really Keep it Secret?

Increased Globalization and Global Competition adds to the risk of disclosure

- U.S. corporations are shifting huge numbers of technology jobs (programmers, software engineers, application designers) to India, China and Pakistan
- Foreign joint-ventures with U.S. companies—and the increased use of outsourcing development and other functions to foreigners—is on the rise (and often a means to access computer networks and facilities to appropriate trade secret information)

Current Employees

Reinforce trade secret identity and security measures

- Implement procedures for identifying new trade secrets
- Implement and continually reinforce marking policies
- Implement and reinforce policies and procedures that limit and record access to trade secret information
- Update policies continually in light of new technologies
- Require signed nondisclosure agreements that identify the trade secrets to which that specific person will have access
- Periodically remind employees of obligations to keep secret

Newly Hired Employees

Educate regarding companies trade secret policies and procedures

- Describe policies and specific types of trade secrets to which employee will have access (training sessions)
- Execute nondisclosure agreement

Determine obligations to prior employer and assess risk

- Ask for (and review) agreements with prior employers
- Make sure new hires understand obligations not to disclose or use prior employer's trade secrets (get signed certification in writing if possible)
- Evaluate risk of exposure (inevitable disclosure, vicarious liability)

Vicarious Liability

Employer may be held vicariously liable for the use or disclosure of third-party trade secrets by its employees

- Even if the new employer *did not know* (*and had no reason to know*) that its new employee had used or disclosed a third-parties' trade secrets

Departing Employees

Conduct comprehensive exit interview

- Remind employee of obligation not to disclose trade secrets (identify)
- Obtain written acknowledgment of obligation
- Confirm that all documents (or other media) that contain confidential trade secret information has been returned (explore and interrogate)
- Gather evidence to determine whether new employment position possess a threat to the companies trade secrets (inevitable disclosure)
- Document (sign) and have at least two people conduct the interview

Search workspace and computer/interview co-workers

- Suspicious e-mails--recently deleted files--recent activities

Follow-up

- Send follow-up letter to employee
- Consider sending letter to new employer
- Determine whether policies/procedures should be updated

Inevitable Disclosure

Inevitable Disclosure may be available to prevent former employee from working for a competitor in a capacity where the employee would inevitably disclose those trade secrets

- Applied only in very limited situations
- **Focus** is on (1) evidence of direct competition; (2) similarity of positions; and (3) necessary use of trade secrets in position
- Seminal case is *PepsiCo, Inc. v. Redmond*, 54 F.3d 1262 (7th Cir. 1995)

Third Parties

Joint venture (strategic) partners

- Present high risk of disclosure
- Identify, mark and limit access
- Document who produced what and who owns what
- Get it in writing
- Take steps when the marriage ends

On site contractors, vendors, customers and consultants

- High risk of disclosure (adequate measures rarely taken)
- Don't use form nondisclosure or confidentiality agreements (one size does not fit all)
- Treat them as you would employees who have access (but with more caution)

Are You Prepared to Commit the Necessary Resources to Keep it Secret?

- Do you have a culture of maintaining secrets already in place?
- Ongoing costs (time and money) associated with the maintenance of trade secrets protection often outweigh the costs to obtain a patent
- Are you committed to quickly taking action to protect your rights?
  - Enforcement is risky, expensive, disruptive; discovery will be broad and confidential business information will be disclosed

What is the Economic Impact to Your Company if Your Trade Secret is Disclosed?

- Is it critical to your financial future?
- Once disclosed, likely your competitors will not be prohibited from using it?
- You may have no ability to be compensated for the harm caused by inappropriate disclosure
  - The rogue (judgment proof) discloser

Does Trade Secret Protection Ever Make Sense?

- In many situations, trade secret protection is the only option
- Faced with:
  - New technology that makes misappropriation easier and protection/detection harder
  - An increase in employee mobility and a decrease in loyalty
  - Increased globalization of companies' workers
  - Intense global competition for technology and innovation
  - And the inevitability that these factors will exacerbate over time,
- Trade secret protection is often not a desirable option
  - It is fraught with uncertainty and in the future may not be a viable form of long-term protection for many types of technology

Donald A. Degnan

Holland & Hart LLP

1050 Walnut Street
Boulder, CO 80302
Telephone 303.473.2724
ddegnan@iph2.com

Don specializes exclusively in the areas of trademark and patent litigation, Internet law, copyright, trade libel and trade secret law.

He was selected as a finalist in Denver's 2003 "Best of the Bar" Awards, sponsored by *The Denver Business Journal*, for the intellectual property category.

Don also co-chairs IPH^2 – the firm's Intellectual Property Group – and heads its Intellectual Property Litigation Practice.

Education and Professional Organizations

J.D. The University of Iowa College of Law, 1991
M.B.A. The University of Iowa Graduate School of Business, 1991
B.B.A. The University of Iowa, 1986

Committee Member, International Trademark Association (INTA), Meetings Planning Committee (1998 to 2003)

Committee Member, American Bar Association IPL Committee on Trade Secrets and Interference with Contracts (1997 to 2002)

Member, American Intellectual Property Law Association (AIPLA), Internet and Cyberspace Committee (1998 to present)

Member, American Intellectual Property Law Association (AIPLA), Trademark Practice Committee (1998 to present)

Member, American Intellectual Property Law Association (AIPLA), Patent Litigation Committee (1998 to present)

Member, American Bar Association, Patent, Trademark and Copyright Sections

Articles and Talks

Book - Montana and Wyoming Sections of multi-volume treatise entitled "State Trademark and Unfair Competition Law," *International Trademark Association* (2003)

Article - "What Is An E-Name: Domain Name Basics," Idaho State Bar CLE Materials from program entitled "An Introduction to E-Commerce", May 2000

Article - "When Can An Item Claim to Be 'MADE IN THE USA'," *H&H Intellectual Property Times*, May 1998

Speech - *Recent Case Law on Trade Dress Issues*, Moderator of Breakout Session, International Trademark Association's Annual Meeting, San Francisco, California, May 8, 2001

Speech - *Cyber Litigation Summit: Using Technology in Technology Litigation*, CLE sponsored by Glasser LegalWorks, December 4-5, 2000, San Francisco, California

Speech - *An Introduction to E-Commerce: Domain Name Basics*, CLE sponsored by the Idaho State Bar Association, May 2000, Boise, Idaho

Speech - *How to Register Domain Names*, Moderator of Breakout Session, International Trademark Association's Annual Meeting, Denver, Colorado, May 2000

Speech - *How to Conduct a Trademark Audit*, Moderator of Breakout Session, International Trademark Association's Annual Meeting, Denver, Colorado, May 2000

Speech - *Representing High-Tech Companies: "Defending IP Infringement Claims,"* CLE sponsored by CLE International, December 12-13, 1996, Denver, Colorado

Speeches - *Internet related IP seminars*, sponsored by H&H for its clients (1998 to present)

Speeches - *Trademark seminars*, sponsored by H&H for its clients (1995 to present)

Speeches - *Trade secret seminars (Audit)*, sponsored by H&H for its clients (1994 to present)