Protecting Trade Secrets During Employee Migration: What You Don't Know Can Hurt You

By Kenneth A. Kovach,* Mark Pruett, Linda B. Samuels, and Christopher F. Duvall

Kenneth A. Kovach was a Professor of Human Resource Management and Industrial Relations School of Management, at George Mason University.

Mark Pruett (Ph.D., University of Illinois) is an Assistant Professor of Strategic Management at Appalachian State University.

Linda B. Samuels is Professor of Legal Studies in the School of Management at George Mason University in Fairfax, Virginia.

Christopher F. Duvall currently works for the global consulting firm Booz Allen Hamilton. During the research and writing of this article he worked for the U.S. Department of State.

On the night of Monday, January 24, 2000, Lt. Gen. Michael Hayden, director of the U.S. National Security Agency—the world's most technologically advanced spy agency, with 30,000 employees—learned that the entire computer network at his agency's headquarters had broken down. Data was still arriving in enormous quantities, but it could not be used or analyzed. The agency was, as the Washington Post later reported, "brain-dead". Hayden informed his superiors and, by Thursday, with the system still non-functional, delivered a presentation via closed-circuit television to his employees: "We are the keeper of the nation's secrets. If word of this gets out, we significantly increase the likelihood that Americans will get hurt. Those who would intend our nation and our citizens harm will be emboldened. So this is not the back half of a sentence tonight that begins, 'Honey, you won't believe what happened to me at work.' This is secret. It does not leave the building." By Saturday afternoon, however, a television network had learned about the disaster and was asking for the story

about the still only partially functional network. Hayden discovered that the leak had come from the Pentagon, not from the NSA. As he later told his employees, "You held the line. You kept it secret while it had to be secret."[1]

TRADE SECRECY—WHAT'S THE PROBLEM?

The problem is that employees move from firm to firm, carrying with them trade secrets and other intellectual property. Not all former employees can keep a secret. What can a firm do to avoid giving competitors its specialized knowledge? Recent studies indicate that roughly two-thirds of the more than thirty significant cases of trade secret violation brought to U.S. courts under the provisions of the 1996 Economic Espionage Act were due to wrongdoing by insiders, not direct theft by outsiders. We suggest that the useful course of action lies in Lord Acton's famous quote, "Everything secret degenerates...nothing is safe that does not show how it can bear discussion and publicity."

Firms participating in a knowledge-based economy are sensitive to the issue of trade secrecy. The issue is particularly prominent in the area of so-called "high" technology, which encompasses a range of knowledge-focused activities, including telecommunications and information technology hardware, software, and services; biotechnology; advanced manufacturing technology; and advanced product technologies. Knowing how to secure the economic benefits of those innovations is a central concern for commercialization.[2]

The NSA network failure, though governmental, suggests two issues central to corporate concerns about sensitive information. First, intellectual property is a crucial element of competitive success. Second, although there are important technological and organizational mechanisms to protect information, the foundation of protection for an organization's intellectual assets rests on the twin cornerstones of two organizational values—the vigilance and loyalty of employees. This article focuses on the impact of employee migration to new employers on the former employer's intellectual property and on ways firms can improve its protection. We argue that the more open a firm is about its trade secret policies and what is expected from employees regarding those trade secrets, the greater the chances are that both current and former employees will act in the firm's best interest.

We examine the trade secret violation problems associated with the desire of migrating employees to use their knowledge in their new position and suggest options available to firms to solve these conflicts. Taking the perspective of the general manager, we begin by discussing the importance of the secrecy issue and the competitive significance of knowledge, and provide brief examples of recent trade secret disputes in the high-technology arena. The second section provides a legal perspective on applicable law, definitions of trade secrets, and the typical types of violations found. The third section discusses the technological, contractual, and organizational protections available to a firm, and offers insights into how to manage the process of assessing and protecting trade secrets.

EXAMPLES OF TRADE SECRET DISPUTES

> "The future of the nation depends in no small part on the efficiency of industry, and the efficiency of industry depends in no small part on the protection of intellectual property."[3]

The loss or leakage of knowledge assets is not an isolated problem. As early as 1988, an unpublished study by the National Institute of Justice found that almost half (48%) of 150 large high technology firms surveyed believed they had been the victims of trade secret theft. Almost 80% of the cases involved participation by an insider. Estimates of the economic value of stolen secrets range in the tens of billions of dollars.[4]

The problem is relevant for many kinds of firms, but it appears particularly significant for firms that deal with research, development, and manufacturing, whether in information

and communications technology, advanced manufacturing technologies, software development, innovation in established industries, or in bio-science efforts in genetics, chemistry, and other fields.[5] For example, a firm may invest years and millions of dollars in research and development of a new medical device, computer program, or genetically-altered plant, developing a great deal of information which is known only to that firm. If a competitor accesses and uses this information to eliminate developmental dead-ends, and introduces a competitive end-product sooner and at lower cost, the first firm loses some or all of its advantage.

The threat exists in economic booms, as well as in slowdowns. As a case in point, consider information-technology service firms. During the Internet boom, the common perception that first-mover firms could gain advantages sometimes led new employers to troll for their competitors' personnel in order to gain crucial information and release a product first. Since the bursting of the Internet "bubble" and the consequent failure of many such firms, the survivors may not be doing as much hiring from competitors, but they are increasingly focused on protecting their trade secrets and other intellectual property.

Traditional "assets" like cash, inventory, facilities, and equipment are not necessarily easy to protect against loss, theft, or vandalism. The task, however, is relatively clear-cut: to design facilities and procedures to reduce such risks. In contrast, a company possesses a great variety of information and knowledge that can contribute to its competitive advantage, yet those assets are harder to protect, and retain, because of their intangibility and because of employee mobility. For example, Wal-Mart found it necessary to file suit against the online bookseller Amazon.com for hiring away its employees by "targeting a specific combination of individuals for their expertise and insider knowledge of Wal-Mart's distribution, data warehousing, and merchandise management systems."[6]

There are numerous other high-visibility disputes about the theft of trade secrets by employees who moved to new employers. It is important to note that companies have mixed success pursuing legal remedies to such situations.

- ***eBay hires an Amazon.com senior executive.*** In some instances, courts may refuse to hear disputes, leaving resolution to the parties. In 2001, Christopher Zyda, Amazon's treasurer and chief financial officer, announced he was leaving Amazon to work for its primary direct competitor, eBay, as vice-president of financial planning. Amazon sought an injunction because its "trade secrets will be misappropriated if Zyda is permitted to sign on to eBay." eBay countersued, contending that Zyda agreed not to disclose any of Amazon's trade secrets and stating that Amazon was trying to thwart Zyda's freedom of employment. Amazon's case was ultimately dismissed on jurisdictional grounds and eBay's countersuit dropped.[7]
- ***Intel hires numerous Motorola employees.*** In other instances, it may simply be easier, more practical, or faster to resolve trade secrets disputes out-of-court. In 1999, Motorola alleged that Intel's "concerted, predatory targeting of key designers" would provide valuable trade secret information on semiconductor design and business strategy if Mark McDermott, the former director of a Motorola design center, were allowed to join competitor Intel. Intel had already hired away more than a dozen Motorola employees. The two companies eventually reached a private settlement out of court.[8]
- ***Cadence employees leave and create competitor Avant!*** Sometimes, however, a company may be sufficiently damaged by the loss of trade secrets that persistent legal action appears the most viable course, even if it is time-consuming. In 2001, seven then-current and former executives of Cadence Design Systems agreed to plead no contest to misappropriating Cadence's computer code for use in the products of Avant!, the new firm they founded. The case, which began in 1994, took years and

numerous actions (including a Supreme Court appeal) to progress through the legal system due to the complexity and novelty of the allegations. A number of the defendants were given prison sentences and multimillion dollar fines arising from charges of trade secret theft, conspiracy to commit trade secret theft, concealing stolen property, and securities fraud. In addition, Cadence's civil suit against Avant! ended in 2002 when Avant! agreed to pay $265 million in damages.[9]

- ***Lucent employees indicted for theft of trade secrets from multiple companies.*** In 2001, three Chinese nationals, two of whom worked for Lucent Technologies, were indicted on charges of conspiracy to steal trade secrets from Lucent and transfer them to a Chinese state-owned company. The three men formed a company which then entered into a partnership financed by the Chinese company. The partnership was used to transfer technology and software stolen from Lucent. In 2002, the indictment was amended to include trade secrets stolen by the three from several of Lucent's suppliers. The indictment alleges, among other things, that the men used aliases to obtain cell phones, business cards, and email addresses that concealed their ties to Lucent. The case has not yet been resolved.[10]

KNOWLEDGE ASSETS AND EMPLOYEE MIGRATION

The past decade has seen a marked change in emphasis on the sources of competitive advantage from managers and scholars. Attention shifted away from tangible physical assets toward knowledge as the key to competitive success. One notable early piece on this topic was Hamel and Prahalad's 1990 article "The Core Competence of the Corporation," which posited that the basis of a firm's advantage was in a particular activity(ies) that the firm did remarkably well, and that the key to maintaining the advantage was to continue to build and exploit that singular competence.[11] An important part of this competence may be highly personal, undocumented, loosely-defined, hard to codify and quantify, and perhaps under-appreciated for its significance—what is referred to as tacit knowledge.[12] In addition, knowledge that provides a competitive advantage may also be more explicit. For example, Deming and others raised the concept of quality as a competitive focus for the entire firm, not just an issue for a group of specialized technicians. They emphasized that quality was achieved not through amorphous understanding, but through the development and application of specific knowledge.[13] Moreover, it is interesting to observe that many of the particular managerial practices, organizational practices, and analytical tools associated with quality are, at their core, ways to improve communication and increase the sharing of data and ideas. For instance, adapting a team-based organizational structure, using statistical process control and other data analysis techniques, and building tight operational links with suppliers and customers—all of these are about developing, transferring, and applying knowledge.[14]

More recently, we have seen a significant increase in corporate interest in gaining competitive advantage through information-centered concepts such as innovation and the use of information technology for competitive analysis, communication, data-mining, value-chain integration, and enterprise management. Skills, competence, patents, copyrights and trade secrets— all such forms of knowledge are now widely appreciated as a crucial ingredient in business success. How, then, can a manager build a firm that thrives on creating such crucial specialized knowledge and protects that knowledge from competitors at the same time?

Companies develop and use many different types of knowledge they do not wish to make available for use by their competitors or by the public. Sometimes this information is commonly known throughout the company and is protected by intellectual property (IP) laws that provide firms with property rights to inventions, written materials, and symbols. These three forms of legal protection—patents, copyrights and trademarks—usually require the

firm to register the IP with the government and to provide public disclosure.

A trade secret, the fourth type of intellectual property, has no requirement for public disclosure. In fact, to qualify for legal protection as a trade secret the information's distribution must be tightly controlled by the firm. However, because the knowledge is intangible, many companies do not implement the steps required to maintain secrecy. Even firms cognizant of these requirements that take steps to closely protect their information may face a problem when employees who have had access in the course of their work leave to work with a competitor or one which provides advice to competitors.

When employees leave, they "mentally" take all the knowledge they have developed or used during their time with the firm. That knowledge is both specific and general. Specific knowledge may include technical knowledge of the firm's production and service delivery processes, customer relationships, cost analyses, pricing plans, new product development plans, plans to raise or invest capital, and research and development activities, to name only a few. They may also have intimate knowledge of the firm's broader organizational strengths and weaknesses—such as its long-term strategy, financial situation, ties with other firms, and planning process.

Consider items even as broad as organizational culture. Although culture itself is not a secret, it may be a substantial contributor to competitive advantage as in, for instance, 3M's belief in innovation or the famous dedication of firms like Toyota and Motorola to improving quality. A departing employee may have substantial knowledge about closely-held specific methods and steps the firm took to develop and maintain its unique culture, which may qualify as a secret.

As we saw in some of the examples cited earlier, a departing candidate may even leave with knowledge about which remaining employees would be attractive candidates for the new firm to lure away.

While not all of these kinds of knowledge can be protected as trade secrets or even as other types of IP, steps can be taken to put the firm on stronger footing when employees leave. To be successful, managers need to know what is required for trade secret protection.

SO, WHAT CAN BE A TRADE SECRET UNDER U.S. LAW?

In the United States, trade secret law is now a combination of state and federal law. Many states have enacted statutes based on the Uniform Trade Secrets Act (UTSA) of 1979 (amended 1985). In those states, these statutes provide the legal basis for protecting business secrets and provide civil remedies for when there are violations. In addition, the Restatement (Third) of Unfair Competition (Restatement) (1995) gives advice regarding the application and interpretation of the UTSA and provides recommendations to be considered by the courts in those states that have not enacted it. On the criminal side, the federal Economic Espionage Act of 1996 provides penalties for knowing theft of private trade secrets by both foreign and domestic entities. This law was passed in recognition of the importance of trade secrets to business and the growing ease of technologically-aided theft. The Act criminalizes the knowing but unauthorized taking, alteration or destruction of a trade

• • • A COMPANY POSSESSES A GREAT VARIETY OF INFORMATION AND KNOWLEDGE THAT CAN CONTRIBUTE TO ITS COMPETITIVE ADVANTAGE, YET THOSE ASSETS ARE HARDER TO PROTECT, AND RETAIN, BECAUSE OF THEIR INTANGIBILITY AND BECAUSE OF EMPLOYEE MOBILITY.

secret by any means, as well as the knowing receipt of a trade secret taken without authorization. In addition, most states have computer crime and other criminal theft laws that may apply to some situations. The two central factors are that the material has been kept confidential and would be valuable to competitors.[15]

The UTSA, the Restatement, and the Economic Espionage Act of 1996 all provide similar definitions of what may be protected as a trade secret. Since there are no specific subject matter limits, many types of business information may qualify. Knowledge that may qualify includes scientific and technical information as well as business, financial, marketing and other information—potentially protectable knowledge is very broad.[16]

For some types of knowledge, trade secrecy can offer superior IP protection, better than patents or copyrights. For example, although patents for new technologies eventually expire, usually in twenty years, trade secrets may endure without a time limit. This can happen if the information is properly guarded and is not developed independently or reverse engineered by competitors:

> Virtually any information or expression, whether or not recorded, qualifies for trade secret protection if its limited availability gives it economic value and it is reasonably guarded. Trade secrets are not limited to scientific or technological information; they may include business and financial information such as costs, preferred suppliers, prices and customer lists. Such things as formulae for materials, recipes, production processes, and compilations of information, computer programs, and computer program algorithms may be trade secrets.[17]

The Uniform Trade Secrets Act defines a trade secret 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.

According to the Restatement (Third) of Unfair Competition, Section 39,

> A trade secret is any information that can be used in the operation of a business or other enterprise and that is sufficiently valuable and secret to afford an actual or potential economic advantage over others.

While reasonable efforts to maintain secrecy are explicitly part of the Uniform Act definition, they are but one factor to be considered under the Restatement definitions, so efforts to maintain secrecy could arguably be absent if other factors are present in those states which have not enacted the Uniform Act. However, under the Uniform Act, reasonable efforts to maintain secrecy are required. In addition, from the practical perspective, without reasonable efforts to protect, trade secrets may be easily lost to the competition.

Section 1839 of the Economic Espionage Act of 1996 tracks the definition found in the Uniform Trade Secrets Act, in a more explicit manner, as required by a criminal statute. It defines a trade secret as:

> (3) the term '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, methods, techniques, processes, procedures, 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 thereof 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, and not being readily ascertainable through proper means by, the public.

The statute covers both foreign and domestic trade secret theft. It was originally thought this statute would be applied primarily to espionage by foreign companies and governments. So far, however, prosecutions have been primarily against U.S. firms rather than foreign firms or governments.

WHAT CAN BE A TRADE SECRET IN OTHER COUNTRIES?

Faced with common interests in protecting knowledge, many countries have developed similar IP laws and entered into treaties and agreements, in connection with patents, copyrights and trademarks. Trade secret laws, however, vary greatly from country to country.

While the British Commonwealth countries including Britain, Canada and Australia have well-developed laws in this area, many countries do not. Some countries track the UTSA with deviations, while other countries have unique laws. For example, in some Asian countries, employees—not firms—have ownership to inventions and other new technology. Others, including Brazil and Mexico, focus on the benefits of technology transfer as a spin-off of foreign investment and therefore do not allow undue restrictions on the use of information. Some countries have no trade secret laws at all—Chile, Colombia, Costa Rica, Ecuador and Venezuela are examples of such countries. Countries that do have trade secret laws include Argentina, Australia, Austria, Brazil, Canada, Cyprus, Denmark, Egypt, Finland, Germany, Greece, Hong Kong, India, Ireland, Israel, Jamaica, Japan, Malaysia, Mexico, the Netherlands, New Zealand, Norway, Peru, Portugal, Singapore, South Africa, Spain, Switzerland, Taiwan, Thailand, Trinidad, the United Kingdom and Uruguay. However, the presence of a trade secrets law does not necessarily mean that a country provides for criminal penalties.

TYPES OF TRADE SECRET VIOLATIONS

With the above definitions in mind, several different types of trade secret violations are worrisome to a firm, including the malicious theft or release of information, and leakage from employee turnover. Threats to trade secrets can come from outsiders and insiders, including present and former employees and third parties with whom the company has contracts. While bribery, theft or industrial espionage can be involved, trade secret disputes often revolve around breach of confidence by insiders when they leave to work for a competitor or start their own firm.

One common problem is the general malicious release of private information to the public as occurs when a company's computer system is "hacked" by outside parties, whether for the thrill of being able to do it or out of anger. Sometimes, the hacker is a disgruntled former employee. Hacking a system to release a firm's secrets can mean jail time and stiff financial punishment under the Economic Espionage Act and other federal and state criminal laws. Though these laws are likely to have some value as deterrents, many hackers are never caught. One reason for this is that many firms never report security breaches, fearing that it will advertise their vulnerability to other criminals, their competitors and their clients.

Hackers aside, the more common scenario arises when an employee leaves a firm and either joins a competitor or starts a new company in competition with the original employer. The

originating firm must try to prevent the competitor from gaining a competitive advantage which would enable it to eliminate the time consuming and expensive middle steps in research and development, beat the original firm to the market and/or improve on the original idea. Here, the employee's former company can take preventive steps to restrict the release of its trade secret(s) which have both physical security and legal dimensions. In part, this can occur through the enforcement of the company's rights of confidentiality arising out of trade secret law. Companies can enforce their rights under the UTSA or state case law and state and federal criminal statutes. They can also supplement these with employment contracts containing special non-competition and non-disclosure clauses. The company can sue both the former employee, and the new employer to stop the release and use of the information. Additionally, the company can request criminal prosecution by the government.

However, from a practical viewpoint, a firm may have little recourse to protect trade secrets that already have been electronically accessed and released. A firm's possession or use of another company's trade secrets may not necessarily violate secrecy laws. For example, AT&T lost its secrecy lawsuit against Berkeley Software Design because AT&T's secret software code was stolen and then posted on a publicly-accessible website. Copyright protection may still have attached, but the trade secrecy protection was nullified by wide public access. On the other hand, information does not lose its trade secret status simply because it has been misappropriated, regardless of how it was misappropriated.[18]

As suggested by the earlier Amazon-Wal-Mart example, the practice of poaching groups of employees from the original firm is related to this problem. Poaching may be even more harmful than the theft of trade secrets by a single employee. This is because a larger migration of employees can increase the impact of the disclosure and can move the original company back to the very beginning of its research and development efforts. For example, if an entire research and development team is wooed away from a company, not only does the company potentially lose the trade secrets contained in the team's collective heads, but it also loses valuable, experienced research and development employees that it must then replace and train. The poaching of additional employees will be further discussed in the non-solicitation clauses section.[19]

A MANAGERIAL PERSPECTIVE ON PROTECTING SECRETS

In general, a firm needs to meet five points if it is to manage knowledge as trade secrets.

- Existence — a firm must prove that what it is referring to is actually a trade secret under the legally recognized definition.
- Access — a firm must control access to trade secrets. If it wishes to prosecute an employee for violating the company's trade secret(s), the firm must prove the employee had access to them.
- Notice — a firm must tell employees what their trade secrets are. There must be a record of this communication. Town hall meetings, company wide notices, or one-on-one documented discussions are important.
- Use — a firm must prove that an employee used or disclosed his/her knowledge of the trade secret improperly.
- Damages — a firm must indicate that harm will come to it if its trade secrets are improperly revealed or used by competitors.[20]

From the standpoint of the general manager, where should a firm begin to address these requirements? The following pragmatic approach can help a firm inform employees of, and then act on, the importance of information assets. It reflects the organizational values posed at the beginning of this article—openness, vigilance and loyalty.

WHAT DO WE KNOW THAT WE WANT TO KEEP PRIVATE?

A trade secret inventory or audit is the logical place to begin. Study and assess the significance of sensitive data to the firm. It makes little sense to introduce solutions without an

assessment of what intellectual assets the firm possesses. A trade secret inventory also offers the firm the chance to learn how to quantify the value of its intellectual assets.

Addressing the topic on a company-wide basis presents an excellent opportunity not only to gain the insights of employees but to sensitize them to the topic as well. It is important to make clear who is spearheading the effort, but the firm will be best served by involving many employees. Broad employee involvement changes employee expectations, and research has shown that changing employee expectations can significantly reduce employee theft.[21] Accordingly, we suggest it is a mistake to relegate the responsibility for trade secrecy analysis and protection to a small group or, for that matter, only to the corporate counsel. Firms often use outside consultants in the audit process to provide expertise and act as a catalyst. However, they should be used as a complement, not a substitute, for employee involvement.

WHAT INFORMATION COULD COMPETITORS REALLY USE, AND WILL THEY FIND HARD TO OBTAIN?

Assessing the competitive value of a firm's information requires an honest evaluation of whether competitors would desire and be able to make use of that information, and whether the information is already known or readily obtainable. Protecting genuinely useful information is worthwhile; protecting information that realistically provides little utility to competitors, or is already available through other sources, would not be. For example, consider the NSA example at the beginning of this article—it is interesting to observe that the U.S. government continued to officially deny the very existence of the agency for years after the fact of its existence was common knowledge to the domestic and international public and press. It would seem that the efforts to protect that information could have been put to use to protect other secrets.

One litmus test for whether information is worth protecting is for a firm to ask how, specifically, it would use similar information about or from its own competitors. If that question cannot be readily answered, it begs the question of whether such information deserves protection.

WHAT TECHNOLOGICAL AND PHYSICAL PROTECTIONS ARE APPROPRIATE FOR OUR COMPANY?

Firms can not retain employees against their will once they have decided to seek other employment. However, firms can employ methods to safeguard trade secrets and mitigate losses if and when employees go to work for competitors.

Examples of technological and physical protection of information include the use of roving guards, computer passwords, passkeys, identification badges, biological identification checkpoints, and even intra-facility positioning systems (similar to global positioning systems in that the location of employees is always known). These are examples of both simple and complex methods a company can utilize to control the access and distribution of sensitive information. While some barriers may be cumbersome and expensive to implement, the risks of the release of valuable corporate information may outweigh the short-term aggravation associated with these solutions. In addition, since reasonable efforts must be made to maintain a secret under both the UTSA and the Economic Espionage Act, the firm may be forfeiting its legal recourse if it does not make a serious effort at such technological and physical protection of its valuable secret information. However, what would be realistic to expect in terms of reasonable efforts may depend on the industry practices and other practicalities and is therefore difficult to definitively pin down. Moreover, technological and physical barriers cannot protect trade secrets that are in the employee's minds.[22]

WHAT CONTRACTUAL PROTECTIONS ARE APPROPRIATE FOR OUR COMPANY?

Employee reassignments and promotions are practical time points when firms can teach

about and reinforce trade secret obligations. In the United States and other countries with well-developed trade secret laws, it may not always be necessary to specify restrictions in employment contracts. Clearly, where trade secret protection exists, current employees may not use business confidences to compete with their employer. Further, when the employment relationship is severed, the employee has continuing duties of confidentiality for information that qualifies as trade secrets, where the circumstances of its disclosure to that employee created a duty of confidence. In countries with non-existent or weak trade secrets laws, contractual limitations can take on greater importance, if the law of that country would recognize the contractual restrictions as enforceable. In addition, even in locations with trade secret laws, as in the U.S., contractual restrictions may supplement that law and protect information that might not otherwise clearly qualify as trade secrets. This is because an important function of nondisclosure agreements is to clearly identify information considered secret by the employer and to warn employees to guard that information. This could apply even in situations where the employee being warned against disclosure developed the information. Non-disclosure agreements also can potentially help if the company was deficient in its efforts to take reasonable measures to maintain secrecy. Also, non-disclosure agreements may even provide avenues of relief that may not otherwise be available under existing statutes. Also, even where they cannot be enforced on their own, non-disclosure agreements can serve the important role of employee notification under trade secret statutes and case law and may warn against disclosure.

These contractual protections should be highlighted when hiring employees and periodically, with current employees, to reinforce their purpose and to impress on employees how seriously the company considers these obligations. These clauses can be customized to protect different types of information and activities and differing employment environments. Also, since litigation is usually very expensive and may take years to complete, a mandatory arbitration clause may be a better way to provide for resolution of disputes under the agreements. However, employers should retain the right to go to the court system for a preliminary injunction to guard against the release of the information.[23]

WHEN EMPLOYEES LEAVE, THEY "MENTALLY" TAKE ALL THE KNOWLEDGE THEY HAVE DEVELOPED OR USED DURING THEIR TIME WITH THE FIRM.

NON-COMPETE CLAUSES

The most widely known and frequently used contractual legal protection is the non-compete clause in an employment agreement or a stand-alone agreement that pertains to trade secrets and confidentiality (see Appendix A for an example of a typical non-compete clause). This clause is usually included in an employee's employment contract and specifies the duration and geographic boundaries of the non-competition. Typically, it also details what types of information are protected as confidential and with whom the employee can share their acquired skills and knowledge after departing.

Unfortunately, the non-compete clause can be difficult to enforce and may have limited value if employees are not periodically reminded of their responsibilities, such as during annual evaluations, company "town hall" or "all-hands" meetings, and/or firm-wide notices. The company should not make the non-compete clause overly broad. This is because to be enforceable, both the time and geographic location covered by the clause must be limited in scope and reasonable. Depending on the circumstances, the typical cause is not longer than two years, with three years being the maximum. Beyond this the employer can be found to infringe on the

employee's legal right to seek employment elsewhere. In addition, the geographic coverage cannot be too broad and must be reasonable in light of the type of business being protected. The clause may limit an employee not to compete in the area, for example, surrounding Austin, Texas, or in the state of Texas, or even the Southwest United States, but cannot usually include a whole country or a continent or be world-wide.[24]

As always however, there are exceptions. A Canadian ruling, for example, upheld a six-month non-compete clause covering North America and the United Kingdom in a software programmer's employment contract.[25]

One important point to note about non-compete clauses is that courts in California typically do not honor them; nor does that state allow clauses signed in other states to remain valid within its borders. As an illustration, if an employee signs a non-compete contract in New York with a two-year time period, and the employee is then transferred to California, quits, and enters employment with a competitor within the time frame, the non-compete clause will not be enforced by the California court system. The employee will be permitted to work for the competitor. This is so because the California Business & Professional Code provides that "every contract by which anyone is restrained from engaging in a lawful profession, trade, or business of any kind is to that extent void." Interestingly, California's legal approach may actually benefit firms on a general basis. In the past decade, the cluster of high-technology firms in California's Silicon Valley has thrived relative to the similar cluster of firms in Massachusetts on Route 128. Some research suggests that Silicon Valley thrived precisely because of its high employee mobility and attendant dissemination of intellectual property. Conversely, Route 128 may have suffered, not despite their legal protections, but because of them.[26]

From society's point of view, employee mobility may be useful and desirable:

> ... [The freedom to pursue any job desired is] important where the employee's training and skill are so specialized as to allow only a limited field of employment.... Many courts try to find the appropriate balance by drawing a line between an employee's general skill, knowledge, training and experience which no one else may own and specific information provided by the former employer with the understanding that it would be kept confidential.[27]

In fact, the enforceability of non-compete clauses is a frequent basis for disputes between companies and former employees and their new employers. The extent of their enforceability is a difficult public policy area for the court system in the U.S. and in other countries. Courts consider the adverse effect on the original company of the disclosure of its information and the resulting limits on encouragement of innovation. At the same time, courts scrutinize limits on employee mobility and their ability to earn a living. Courts consider whether the employee limitation is reasonable in light of the particular facts of the case. In rapidly changing fields, a reasonable time limitation may be very short, indeed, even less than one year. A reasonable geographic restriction is generally no greater than the actual area where the employee (not the employer) was active. When the scope of the restriction appears too general and overly inclusive, a court is likely to reject it. However, even if enforceable, it may be inadequate since it may be difficult to list all types of information.

Customer lists can qualify for protection in the U.S., but the results are far from uniform. It is more likely that protection will be afforded where the customer lists included information about the customer, beyond names and addresses, and where the departing employee did not contribute to the list. Moreover, it should be pointed out that information that is generally known would not qualify for protec-

tion. Sometimes, information can start out as protected, but would not retain that status for long in an innovative industry as other firms develop the same knowledge.[28]

NON-SOLICITATION CLAUSES

Another common legal restriction is the non-solicitation clause, which is an attempt to protect a company from "corporate raiding." A non-solicitation clause is included in an employment contract to protect the firm from an employee, who has left for a competitor or to start a business, and who is attempting to entice additional employees away from the parent firm. By soliciting these employees, the former employee drains information and secrets vital to the original business. This is a common problem for many firms, as competitors find it easier to hire away a whole research and development team rather than just individual scientists. In the biotechnology field, firms often have individual star scientists developing formulas, but even more importantly, have teams working on whole systems and developmental processes that can provide huge dividends, in the form of patents, industry-altering technology, or highly efficient processes, far into the future. Surprisingly, non-solicitation clauses are more easily enforced than non-compete clauses as they can be strictly defined and more easily proven in court.[29]

STRUCTURE AND PROCESSES—THE BALANCE BETWEEN OPENNESS AND CONTROL

Sensitive information should be an element in questions of organizational structure and decision-making processes. What information must employees have to perform successfully? What information do they generate, and who needs access to that information? To whom should the employees report?

Answers to such questions are already, implicitly, part of structural decisions about functional or other arrangements, hierarchy, centralization, autonomy, span of control, access to information systems and reports, and so on. Viewing information as a competitive asset should lead the firm to make it an explicit part of structural and procedural decisions.

For example, some research has shown that, if a company is operating in an environment with weak legal protection, it may indeed be better to restrict access to trade secrets even if it reduces productivity. For the firm eyeing foreign markets, exporting may protect trade secrets better than investing in subsidiaries or joint ventures. Strategic alliances with other firms also raise the risk of trade secrecy exposure and must be monitored.[30]

FACED WITH COMMON INTERESTS IN PROTECTING KNOWLEDGE, MANY COUNTRIES HAVE DEVELOPED SIMILAR IP LAWS AND ENTERED INTO TREATIES AND AGREEMENTS IN CONNECTION WITH PATENTS, COPYRIGHTS AND TRADEMARKS.

Certainly, firms need to evaluate the need for internal dissemination of, access to, and use of sensitive information. Underlying that evaluation, however, should be a prudent understanding of the risks of restricting the internal distribution of information. Consider the impact of compartmentalization—the practice of controlling sensitive information by limiting its access to those who are believed to need it. A sensible approach, to be sure—one that clearly arises from the sensitive nature of certain information, but that also stems from organizational forces. If knowledge is a competitive asset, then it can also become the basis of power within the organization. Over time, the compartmentalization approach to controlling information may tend to reinforce the rigidity of organizational structure, weaken the strength of collaboration between units, foster an inwardly-focused view of the world, and decrease the ability of much of the organization to think beyond the confines of units. Conversely, compartmentalization may not help stimulate organizational change, in-

teraction, responsiveness to the external environment, or strategic thinking throughout the organization. The question managers must ask of themselves then becomes—is the protection of the information worth the resultant organizational cost?

CORPORATE CULTURE—PROTECTING SECRETS WHILE FOSTERING INNOVATION

Culture plays a significant role in how employees view their firm and in the degree of their emotional commitment. It also has a significant impact on a firm's ability to innovate. One study of culture and innovation by Jassawalla and Sashittal finds that cultures supportive of product innovation have four critical tenets:

- Creativity and risk-taking are important and expected.
- Participants are trustworthy, equally important stakeholders.
- Important customers, suppliers, and other functional areas should be considered insiders early in the innovation process.
- Organizational change is seen as beneficial, not threatening.

Clearly, these characteristics center on the themes of openness and sharing of information. Those themes continue as Jassawalla and Sashittal note that participants in innovation-supportive cultures have distinct behaviors—the ability to control processes, collaborative work, and willingness to receive feedback.[31]

However, strong systems for the rapid internal diffusion of information and expertise come with a price. We should expect that internal diffusion of information is likely to foster external diffusion if for no other reason than that it creates more possibilities for leakage. Indeed, as Zander and Kogut showed, firms with such capabilities also are more susceptible to imitation by competing firms.[32]

EMPLOYEE DEPARTURES—UNDERSTANDING AND MANAGING THE REASONS

The various controls and solutions for loss of trade secrets through employee migration are responses to a problem. Arguably, job-hopping by employees is not the underlying problem but the symptom. The problem may rest in employee dissatisfaction with their present employer (job frustration), or with the perception of better opportunities elsewhere. The departure also may be due to non-work-related causes, some of which may be easily remedied by the firm, thereby avoiding the departure and its attendant problems. If valued employees leave, the wise firm is the one which seeks to understand why. This should be an integral part of the firm's IP protection efforts.

Ashkanasy and Daus provide an interesting overview of the role of emotion in the workplace by addressing the links between personality, work environment, events at work, and the impact on the emotions experienced by workers and on the formation of attitudes. As we might expect, their model suggests that job dissatisfaction and decreases in loyalty and commitment may lead to quitting or anti-social behavior.[33]

Although Ashkanasy and Daus do not address the issue of trade secrets explicitly, the implication is clear. Negative emotions sparked by the general work environment or by events at work, and the attendant decline in loyalty and commitment, may help sow the seeds of a willingness to violate trade secret confidences.

The firm that treats departures, whether voluntary or involuntary, in a cavalier manner, "burning its bridges" with former employees, does so at its own risk. Hand-in-hand with trade secret protection planning, the firm should try to understand why valued employees have left, or may be intending to leave, and how to remedy the situation. Although exit interviews are increasingly common, many remain essentially unlinked to a meaningful feedback system regarding organizational practices. Further, since the exit interview itself may be the departing employee's last significant face-to-face contact with the formal organization, it may reinforce positive or negative feelings toward the firm. A poor departure experience is likely to reinforce any propensity to misuse trade secrets.

Another approach to the same problem (turnover of key employees) is for the company to retain the knowledge of valuable employees by creating a spin-off company that can better leverage those employees' expertise.[34] While this may seem like an extreme step, retention of these employees, and their knowledge and expertise, may be worth the price in the long run.

ADDRESSING TRADE SECRECY OPENLY AND HEAD-ON

The protection of intellectual property is a balancing act. Trade secrets, like other intellectual property, are assets worthy of protection. However, the pursuit of trade secret protection through physical and technological barriers, detailed employment contracts, pursuit of former employees in the legal system, and the variety of organizational controls that can be placed on information may, if done in an ill-informed, indiscriminate, or aggressive manner, only exacerbate the problem by reducing employees' job autonomy and commitment.

A firm that does not understand and manage its trade secrets is a firm with substantial handicaps, one that ignores the trade-offs in protection at its own peril. Employees have the right to work in their field of expertise and experience, and in many countries this mobility right is largely supported by law. At the same time, firms have the right to protect the information and processes from which they derive revenue, even when they were developed by departing employees. Conflicts between these two rights are likely to increase in an increasingly dynamic and interlinked global business system.

A firm should make an organized effort to understand the nature and value of its trade secrets. Also, it should evaluate whether and how to manage employees' access to certain information. However, to bear the most fruit, in the short run as well as the long run, we believe that in general the best approach is to encourage discussion about the subject throughout the organization. A broad base of participation in the firm's analysis should lead to greater awareness and understanding of, and thus better solutions for, the firm's secrecy problems and opportunities. It also should lead to greater satisfaction with solutions, greater employee commitment to the firm, and— perhaps—a decrease in employee turnover. That is, the effective management of trade secrecy will rest on the twin cornerstones of broad organizational vigilance and loyalty.

Maintaining vigilance and fostering loyalty are inescapably the responsibility of managers. If managers are passive about trade secrets in a firm that depends on such secrets, then they may be able to say that the classic Pogo cartoon strip was correct —we have met the enemy and he is us! ▲

APPENDIX A

Sample Employee Non-Compete Agreement

(Reprinted with permission of Kinsey Law Offices (http://www.kinseylaw.com).

For good consideration and as an inducement for_____
(Company) to employ (Employee), the undersigned employee hereby agrees not to directly or indirectly compete with the business of the Company and its successors and assigns during the period of employment and for a period of _____ years following termination of employment and notwithstanding the cause or reason for termination.

The term "not compete" as used herein shall mean that the Employee shall not own, manage, operate, or consult in a business substantially similar to or competitive with the present business of the Company or such other business activity in which the Company may substantially engage during the term of employment.

The Employee acknowledges that the Company shall or may in reliance of this agreement provide the Employee access to trade secrets, customers, and other confidential data and good will. Employee agrees to retain said information as confidential and not to use said information on his or her own behalf or disclose same to any third party.

This agreement shall be binding upon and inure to the benefit of the parties, their successors, assigns, and personal representatives.

Signed this ____ day of _____ 20___

_____
Company

_____
Employee

ENDNOTES

* Ken Kovach died before the final publication of this paper–we value his insights and miss him.

1 Loeb, V. 2001. *Secret Weapon.* THE WASHINGTON POST, Sunday, July 29: Magazine, cover story.

2 Pruett, M., Lee, H., Lee, J., and O-Neal, D. 2003. *How high-technology start-up firms may overcome direct and indirect network externalities.* JOURNAL OF IT STANDARDS AND STANDARDIZATION RESEARCH, Jan-Mar: 33-45.

3 Rockwell Graphics Systems v. DEV Industries, 925 F.2d 174, 180 (7th Cir. 1991).

4 Mock, L. and Rosenblaum, D. 1988. *"A Study of Trade Secret Theft in High-Technology Industries,"* NATIONAL INSTITUTE OF JUSTICE; Carr, C. and Gorman, L. 2001. *The Revictimization of Companies by the Stock Market Who Report Trade Secret Theft Under the Economic Espionage Act,* BUSINESS LAWYER (51).

5 Computer Crime and Intellectual Property Section. 2001. Prosecuting Intellectual Property Crimes: Overview. (http://www.cybercrime.gov/ipmanual/01ipma.htm)

6 *Amazon, Wal-Mart Agreement Puts Net Firms On Notice About Hiring Away Blocks of Talent.* INTERNET WORLD, April 19, 1999.

7 Mellahi, K. and Johnson, M. 2000. *Does it pay to be a first mover in e-commerce? The case of Amazon.com.* MANAGEMENT DECISION, 38 (7): 445; Also *see* Sinrod, E.J. 2001. E-legal: Battle lines drawn between Amazon and e-Bay, Law.com (http://www.law.com) October 9. Judge dismisses Amazon employment suit. News.com, October 29, 2001.

8 Sykes, R & Haney, C. 1999. Motorola sues Intel. IDG News Service PCWorld.com, March 12. Motorola and Intel Settle Trade-Secrets Suit. cnn.com. May 3, 1999.

9 Armstrong, R. 2001. How to squelch innovation. BayArea.com. May 30; also see Santarini, M. 2001. Avant! pleads no contest, officials headed to jail. June www. (http://www.eetimes.com); also see Lafferty, S. 2001. A calculated risk. The Recorder December 11; see Cadence Design Sys. v. Avant! Corp., 125 F.3d 824, (9th Cir. 1997), cert. denied 523 U.S. 1118 (1998), appeal after remand (unpublished opinion) 189 F.3d 472 (9th Cir. 1999), 1999 U. S. App LEXIS 18302; certified question answered by 29 Cal. Rptr. 4th 215 (2002).

10 Reuters News Service 2001. Three indicted in Lucent trade secret case. June 1. Also see New indictment expands charges against former Lucent scientists accused of passing trade secrets to Chinese company, U.S. Department of Justice Press Release, April 11, 2002 (http://www.cybercrime.gov/lucentSupIndict.htm). Also see O'Hare, T. & Sozio, S. 2001. Industrial spy? Moi? The Fine Print. Legal Research Center. (www.cio.com/research/legal/edit/100401spy.html).

11 Prahalad, C.K. and Hamel, C. 1990. The core competence of the corporation. Harvard Business Review, 68 (May-June): 79-91.

12 Polyani, M. 1962. Personal Knowledge: Towards a Postcritical Philosophy. Chicago:University of Chicago Press.

13 Deming, W.E. 1986. Out of the Crisis. Cambridge: MIT Center for Advanced Engineering Study.

14 Pruett, M. and Thomas, H. 1996. Thinking about quality and its links with strategic management. European Management Journal, 14 (1): 37-46.

15 Dratler, J. 2001. Intellectual Property Law: Commercial, Creative, and Industrial Property, Law Journal Seminar Press. See also Economic Espionage Act of 1996 (http://loc.thomas.gov); Restatement of Torts (American Law Institute, 1934); Restatement of the Law of Unfair Competition (American Law Institute, 1995); Uniform Trade Secrets Act With 1985 Amendments (National Conference of Commissioners on Uniform State Laws, 1979, 1985); Samuels, L.B. and Johnson, B.K. 1990. The Uniform Trade Secrets Act: The States' Response, Creighton Law Review; Religious Technology Center v. Netcom On-Line Communication Services, Inc., 923 F. Supp 1231 (N.D. Cal. 1995).

16 Cohen, J. and Gutternam, A.S. 1998. Trade Secrets Protection and Exploitation, The Bureau of National Affairs, Inc.

17 Dratler, op. cit.; Goslar, M. 2000. Are your trade secrets protected? (http://www.zdnet.com/techupdate/stories/main/0,14179,2655461,00.htm).

18 UNIX Systems Laboratory v. Berkley Software Design, Inc., 27 U.S.P.Q. (BNA) 2d 1721 (D.N.J. 1993); IMED Corp. v. SEAC, 602 So.2d 344 (Ala. 1992); Rockwell Graphics Systems v. DEV Industries, 925 F.2d 174, 178 (7th Cir. 1991); U.S. v. Wang, 1995 WL 564447 (D. Colo. 9/15/95); U.S. v. Riggs, 743 F.Supp. 556 (N.D.Il. 1990); United States v. Seidlitz, 589 F.2d at 160 (4th Cir. 1978). Also see Arensman, R. 2000. Keeping Secrets. Electronic Business. May.

19 Flynn, G. 2000. Protect trade secrets from a corporate raid. Workforce. February.

20 Arensman, op. cit.

21 Latham, G. 2001. The importance of understanding and changing employee outcome expectancies for gaining commitment to an organizational goal. Personnel Psychology, 54 (3): 707-716.

22 Paetkau, T. 2000. Protect trade secrets with utmost diligence. Business Journal. July 7. Also see Harrold, T. and Michalyshyn, M. 1998. Confidential Information And Technical 'Know How": What Leaves With Your Employees? Intellectual Property Journal. November; also see Lazzara, S. 2001. Safeguarding the company's jewels. Machine Design. March; Also see Lytle, R.B. and Steinheider, M.F., 2000. What the Sensitive Security Device Cannot Protect: Trade Secrets in the Minds of Employees, Intellectual Property Today. October.

23 Dratler, op. cit.; Cohen and Gutterman, op. cit.; Lytle and Steinheider, op. cit.

24 Berger, C.J. 2000. How to protect trade secrets. Real Estate Weekly. March 1. Also see Jennero, K. and Schreiber, P. 1999. Labor and employee relations: Drafting enforceable non-competition agreements. Employee Relations Law Journal, 25 (3): 119-144. Also see Paetkau, op. cit.

25 Goldstein, S. 1998. Trade secrets need to stay secret. Computer Digest News. November 9. Also see Halligan, R.M. 1997. The Economic Espionage Act of 1996: The theft of trade secrets is now a federal crime, Trade Secrets Homepage, (http://my.execpc.com/~mhallign/iindex.html). Also see Computing Canada: Less is More in Restrictive Covenants: Non-compete clauses are a necessary evil when it comes to protecting intangible investments, (http://www.plesman.com/index.asp?theaction=61&sid=26559).

26 Gilson, R. 1999. The legal infrastructure of high technology industrial districts: Silicon Valley, Route 128, and covenants not to compete. New York University Law Review, 74 (3): 572-629. Flynn, op. cit.; Sinrod, op. cit.

27 Dratler, op. cit.

28 Berger, op. cit.; Cohen, op. cit.; Dratler, op. cit.; Harrold and Michalshyn, op. cit.; Lytle, op. cit.

29 Zelsman, M. 2001. Insider's knowledge – to protect businesses and employees, trade secrets must be specifically defined and spelled out in binding contracts. InfoWorld. July 9.

30 Fosfuri, A., M. Motta and T Ronde. 2001. Foreign direct investment and spillovers through workers' mobility. Journal of International Economics, 53 (1): 205-222; Also see Norman, P. 2001. Are your secrets safe? Knowledge protection in strategic alliances. Business Horizons, 44(6): 51-60; Also see Ronde, T. 2001. Trade secrets and information sharing. Journal of Economics and Management Strategy, 10 (3): 391-417.

31 Jassawalla, A. and Sashittal, H. 2002. Cultures that support product-innovation processes. Academy of Management Executive, 16 (3): 42-54.

32 Zander, U. and Kogut, B. 1995. Knowledge and the speed of the transfer and imitation of organizational capabilities–An empirical test. Organization Science, 6(1): 76-92.

33 Ashkanasy, N. and Daus, C. 2002. Emotion in the workplace: The new challenge for managers. Academy of Management Executive, 16: 76-86.

34 Anton, J. and D. Yao. 1995. Start-ups, spin-offs, and internal projects. Journal of Law Economics and Organization, 11(2): 362-378.