By Jeff Ubois

Trade secrets have been around since the first shaman held onto the recipe for a psychoactive brew much as Coca-Cola does with its famous secret formula. But today, they are more relevant than ever. The most valuable corporate assets now are created and stored in the minds of employees. Knowledge, rather than capital or labor, has become the dominant factor in commercial and production success. Often that knowledge includes trade secrets.

So earlier this year when high level executives moved from GM to Volkswagen, Proctor & Gamble to Clorox, and Borland to Symantec, lawsuits and even criminal indictments for theft of trade secrets followed. "These days, the competitive edge often is information, not megabucks of invested capital," says Stuart Kaufman, a San Francisco-based attorney specializing in trade secret law. "It used to be if you wanted to take market share from Ford, you had to build an auto plant. You just couldn't hire away a few managers."

The basic definition of trade secrets is straightforward. Nearly any type of information that gives an economic advantage because it is not known to the public and is safeguarded by reasonable efforts to keep it confidential qualifies as a trade secret. Computer programs, customer lists, manufacturing devices or formulas, and other marketing information all constitute potential trade secrets.

Like virginity, once trade secrets are gone, they're lost forever. If they are disclosed publicly, not safeguarded, or discovered through reverse engineering, they no longer are protected by law. That makes effective protection vital for companies that depend on trade secrets. A comprehensive trade secret management program will not only safeguard sensitive information, it will prevent future legal conflicts and expenses, and maybe even generate new revenue through licensing arrangements.

Experts warn, however, that blanket protection of all corporate data almost is as bad as none at all. "You need to know what is important to protect, otherwise you will be spread so thin you'll provide little protection to anything," explains Carey Heckman, co-director of the Stanford University Law and Technology Policy Center in Palo Alto, Calif. "It's like fighting a war. You can't use every conceivable weapon, so you have to pick and choose to fit the circumstances."

Selectivity is crucial. "Lawyers stress you should protect more than you thought, but there is as much danger in people being overprotective as being underprotected," Heckman says. "It's obvious when you look at it from a marketing perspective. If everything is held too close, you may have all the trade secrets in the world but no revenues."

Naomi Fine, president of Pro-Tec Data, an Oakland, Calif.-based consulting firm specializing in designing trade secret protection and management programs, cautions that a purely legalistic approach is insufficient to deal with the problem. "Just making rules won't work," Fine says. Instead, management needs to create a participatory program in trade secret protection, one that not only provides guidelines and policies but improves people's judgement.

"There is a misconception that protecting trade secrets is just common sense, but it is not," Fine says. "Intuitively, people have the inclination to share information. It's primary to getting jobs done and helping others. The subtleties of what should be guarded and under which circumstances require strategic thinking. You need to define what is confidential and understand how that information will be handled, shared, stored, and used. It's a matter of understanding what is more valuable to you if broadcast and what will be more valuable if kept confidential."

What needs to be protected varies from company to company. "There are companies proud of their customer list. They will tell anybody, 'We service Chase Manhattan Bank, IBM, Xerox,' because it gives them prestige," Fine says. "But there also are companies for whom a detailed customer list would expose their market to the company's disadvantage."

Fine stresses the importance of involving all relevant departments in trade secret management. Engineering, finance, legal, marketing and security need to be aware and involved in the program. "There is no outside person and no one inside person or department that can identify all information considered confidential or all the risk scenarios. Only an interdisciplinary, cross function team drawn from each strategic business unit can map a plan that will be out of business," says Fine.

Kaufman offers a number of steps to improve information handling and protection. These measures not only will safeguard corporate secrets, they can help prove theft of trade secrets in future litigation. First, Kaufman says, it's important to get good Nondisclosure Agreements (NDAs) with employees, contractors and customers privy to corporate secrets. Though NDAs oblige their signers to protect confidential and proprietary information, rarely do companies spell out exactly what the information is. "NDAs are more effective when they are coupled with a clear identification of the information to be protected," Kaufman says. "Most people will play straight if they understand what you require to be kept secret."

REASONABLE EFFORTS

Employee confidentiality agreements need special care. They clearly must set out the differences between the company's property, which is protectable, and the employee's knowledge, which is not. In addition, overly restrictive agreements may be useless because they can be interpreted as noncompetition agreements, which are not enforceable in some states, including California.

Protection efforts also should include confidential stamps on documents describing trade secrets, locked files for these documents, and careful, regular destruction of sensitive materials. Computerized information should be protected in analogous ways. Employees should be trained to handle phone calls and visitors. Outlining practices in the company's policy manual, periodic memos, and high visibility items like wall posters are good ways to prove the company is making reasonable efforts to safeway to protect intellectual property. "Copyrights, patents, trademarks and trade secrets have different strategic characteristics, and you want them to blend intelligently and reinforce one another," Heckman says. "You can't say that because you have a navy, you don't need an air force." For example, Intel copyrights mask drawings and microcode, patents new inventions, and protects other key aspects of its business with trade secrets. "Intel looks at its business from all these angles and recognizes it has part creative