Protecting Your Secrets & Yourself

By Alan Farnham, Fortune Magazine

Companies wanting to design effective programs for trade secret protection, for EEA compliance, or both, can get help from law firms specializing in intellectual property from Big Six accounting firms, and from such private consultants as Naomi Fine. Her company, Pro-Tec Data, located in San Leandro, California, has assisted some 200 corporations including Johnson & Johnson, McDonald's, Levi Strauss, Kodak, Mobil, Proctor & Gamble, 3Com, Sun, Synopsys, Seagate, and Apple.

Companies suffering maximum exposure, says Fine, include those: (1) growing rapidly through hiring; (2) using consultants or temporary workers, whose loyalties may be in question; (3) operating overseas; and (4) engaged in collaborations, such as outsourcing, that require heavy information-sharing.

Pro-Tec Data begins by performing an audit: What are a client's most valuable secrets? Then procedures are designed to make sure these get protection commensurate to their worth. The exercise, says client Ron Beaty, security director at Rockwell International, can be "pretty basic." Pretty cheap, too. 3Com's director of intellectual property, William Becker, says his company's program cost for working with Fine was "in the low to mid five-figures." Becker wanted it to address two different problems. One was "losing information." The other was the danger that 3Com might inadvertently ingest someone else's secrets.

"When you strengthen internal security, " he says, "part of your goal should be to make sure you're not letting anybody else's secrets in." New hires at 3Com are asked to sign a statement affirming they aren't bringing with them anything that could be construed as the trade secret of a past employer. They're also told that 3Com takes the handling of secrets—both 3Com's and other companies'—very, very seriously, and that mishandling can result in dismissal.

What other steps can you take?

- Periodically remind employees what you do (and don't) consider secret. An internal memorandum at Berkley, Inc., makers of fishing bait and tackle, clarifies that while "leader sink and flyline dressing products" are no longer considered secret, "we are now declaring the formulations and production processes used to make our poured baits to be trade secrets, and therefore, off-limits to outside personnel." Result: no wasted effort on dressings; greater vigilance on bait.
- Review speeches and public pronouncements, especially ones made by scientists or others aglow with the pride of discovery. Press releases

should be screened by product managers. (By one estimate, some 80-90% of information loss arises, not through theft, but through employee inadvertence.)

- Don't overcomply. Competitive intelligence expert Leonard Fuld, president of Fuld & Co., in Cambridge, Massachusetts, says companies frequently disclose far more information than they have to when submitting government forms. "Ask manufacturing personnel, or whoever is involved in submitting the report, to list data they'd prefer withheld," says Fuld. "Have counsel then determine how much of this can legitimately be eliminated."
- Customize information, raising it above the level of 'generic' and making it unmistakably yours. An ordinary client list, for example, can be made more clearly a trade secret if it includes details known only to you—a customer's taste in cigars, Scotch, or French underwear, for example. Software company, Cadence Design, first suspected its source code had been snitched when a Cadence engineer recognized in a rival's product quirks he had deliberately inserted into Cadence's original.
- Know whom you're hiring. Background checks, says Mike Slattery, executive managing director of Kroll Associates, corporate investigators, should be "step one" in any sound protection program. And don't limit them to senior personnel. "Even the janitor can do harm."
- Insist all employees, vendors, contractors, joint-venturers and anybody else privy to your trade secrets sign a nondisclosure agreement.
- Reconsider plant tours. Kellogg's, with reluctance, axed theirs after a foreign competitor, having taken the tour some 20 times, then set up a rival factory.

If you don't remember anything else from this story, remember this: The EEA is a bear-trap you don't want clamped around your leg. How might it get there? More easily than you suppose.

For the present, the law's safety-catch is on: Torren of the Justice Department notes Janet Reno herself has promised Congress she will exercise unusual restraint invoking it. (And much depends, of course, on how courts interpreted it.)

Nevertheless, the EEA, in the words of James Pooley, partner at Fish & Richardson in Menlo Park, California, "has the potential to change business behaviors in fundamental ways". He might well have added 'and in rinky-dink ways, too'—which, if anything, is scarier.

Consider these situations:

- You're on airplane. At takeoff, a report belonging to somebody a few rows up slides along the inclined floor, coming to rest against the toes of your well-waxed wingtips (or pumps, as the case may be). You pick it up noting it's stamped "CONFIDENTIAL". Hot diggidy! It's a marketing report

belonging to your arch-rivals at Nemesis Co. You gleefully digest its contents.
- Same airplane, different situation: Two guys seated next to you are blathering out loud about the sales presentation they'll be making when they land. Ignorant of the fact that you're the enemy, and that you'll be presenting against them, you soak up every detail.
- You're the head of Staples. (This example isn't hypothetical. It's taken from page 72 of Thomas G. Stember's 1996 exercise in braggadocio, "Staples for Success"). You want to get the drop on Office Depot. So you have your wife, Dola, apply for a job at Office Depot's delivery center in Atlanta. "Dola," Stember writes, "had experience in telemarketing and, in a soft, Southern accent, explained that she was anxious to move back 'home'. Staples did not offer delivery service at the time, so I wanted to investigate how Office Depot's delivery system worked, how may people were in the operation, and how it trained employees." Thanks to Dola's dodge, Stember got his info.

Such shenanigans are now illegal. Or *probably* illegal, since the EEA defines theft as the knowing misappropriation of a secret, without its owner's consent. No consent was given here. Where big fines and jail-time beckon, "probably" introduces an element of risk you'd be a chump not to eliminate, if you could. How can you? By returning the report (in situation one) unread. By telling your garrulous seatmates (in two), "Boys, I'd shut up if I were you. I work for the competition." And by not using your wife as a shill.

Are we saying you're obligated, now, to protect competitors from their own stupidity? Yes. That's assuming you want to adopt a belt-and-suspenders approach to self-protection, and that you wish to pass through life without ever having had proffered to you these words of consolation: "No, really, it's not so bad. San Quentin's nice this time of year.

Before the EEA, ethical lapses of the kind just described troubled one's conscience or exposed one to, at worst, civil penalties. Now? Jail. Says Pooley, "Good citizen companies are going to find themselves unexpectedly exposed to criminal prosecution,"

Was this what business had in mind when it schmoozed-up congress? Hardly.
