



Now that the cold war is history, intelligence pros are turning their black-bag wizardry toward corporate targets—maybe even the likes of you.

BY ALISON BASS

JOHN NOLAN, A FORMER U.S.

advertisers

intelligence officer, took the call on a hot sticky day in July. It was from the CEO of a major consumer electronics company in California. He told Nolan that his company was working on a mysterious new technology that once launched, would change the face of his industry and double the company's revenue base. The CEO said he had taken "extraordinary security measures" to make sure no competitors found out about the new product. But just to make sure, he wanted Nolan, who had founded his own intelligence agency after retiring from the Department of Defense, to penetrate his company's fortifications and find out what his R&D group was working on, how much money was being invested and when the new product would be rolled out—all in 30 days or less.

It took Nolan's crew about three hours of working the phones to find out that one of the company's senior managers had been out of the office for the past three months. So they staked out the executive's home and early one morning, tailed him as he drove to a nondescript building about 15 miles from the company's headquarters. An armed guard let the executive through. Nolan's people made no attempt to follow. Instead, they took down the license plate numbers of every car in the parking lot and ran those numbers against Web databases until they had the identities and after more digging, the work titles of every person who had driven to the facility that day.

Posing first as pollsters and later as headhunters, Nolan and his crew covertly interviewed almost all of the key engineers involved in the project. They not only discovered what the top secret technology was, how much it cost to develop and when it would be launched. They also—and well within the 30-day deadline—gave the shocked CEO the names and contributions of six strategic partners in the project.

Nolan, whose Huntsville, Ala.-based Phoenix Consulting Group is one of the best-known competitive intelligence (CI) firms in the business, says he only does the James Bond stuff to show companies their vulnerabilities. But according to Nolan and others in the field, a growing number of intelligence gatherers regularly transgress ethical

How Far is Too Far?

In this heated business environment, competitive intelligence is not optional. There are many ways of learning what your competitors are up to, and they run the gamut from searching the web to hiring spies who will lie or steal to get what they want. How far would you go to get information that could make your company the market leader? How far is too far?

and even legal boundaries on behalf of corporate clients both here and abroad.

Such spooks—many of them former government spies who migrated to the civilian sector after the Cold War ended—will resort to every dirty trick in the book. They'll lie, misrepresent themselves, steal phone records and do anything they can to wiggle their way into your confidence. Perhaps even now they are shopping their specialized talents to your competitors. So, listen up and remember that forewarned is forearmed.

The Espionage Price Tag

Earlier this year, in a report to the European Parliament, a British investigator asserted that both U.S. and European companies routinely engage in corporate espionage. And many foreign corporations regularly receive help from intelligence-gathering networks in their own governments, which use the latest in information monitoring technology to keep abreast of supposedly private Web communiqués. According to the U.S. Chamber of Commerce, corporate espionage costs U.S. shareholders at least \$25 billion a year in intellectual property losses.

"The Internet has made it so much easier to gain access to information. It has actually made people and companies more open," Nolan says. "It's getting harder and harder to protect your assets from the bad guys."

Consider, for example, the recent unpublicized case of a California biotech CEO who got a call from someone claiming to be a reporter from a foreign television company. The "reporter" wanted to interview him, and the CEO was happy to oblige. "One of his crew had a shoulder video camera, and they walked with the CEO around his R&D lab with the camera running," says Alan Brill, a senior managing director at investigative firm Kroll Associates who is familiar with this case. "They were able to steal a number of secrets by videotaping the equipment, the settings on the equipment, and papers and notebooks that were lying around. And this CEO was so busy trying to be a star that he never noticed what they were doing or validated who they were."

Some companies, like the biotech CEO's, are at a competitive disadvantage because they are simply unaware of the spies among them. Others know what's going on but are afraid to take the steps necessary to protect themselves. "Most companies don't like to get embarrassed, and they don't want to risk the bad press that comes from doing the James Bond stuff," says Nolan, who worked for the Defense Department's intelligence agency for 22 years. "We can't even use the term counterintelligence with the business community; they think of torture and assassination when we use that term. So we call it competitive assurance."

Competitive assurance may not involve torture. But it does sometimes involve lying or misrepresentation. There's the old headhunter trick, for instance, or

the potential investor who just has to know a company's R&D plans. The ruses are endlessly varied (see "A Ruse by Any Other Name," right), and what many executives may not realize is that they are perfectly legal. Lying to obtain information is not even cause for a successful trade secret lawsuit—unless the imposter has signed a nondisclosure agreement. Ironically, the only party who can legitimately be charged with a trade secret violation is, in many cases, the employee who unwittingly shared the crown jewels. "It's not illegal to misrepresent yourself," says R. Mark Halligan, an expert on trade secret law and a principal with the Chicago law firm Welsh & Katz. "And the pretext itself is not actionable."

A Ruse by Any Other Name

Protect yourself against the devious tricks that some folks in the business employ (whether they'll admit to it or not) [Read More](#)

Making matters worse, many corporate executives have a faulty understanding of just how to go about doing the kind of intelligent intelligence gathering that will keep them one step ahead of the competition. While corporate CI units need to know the arsenal of dirty tricks competitors might use against them, specialists say they should also understand that good competitive intelligence can often be accomplished without resorting to such shenanigans. If you know what you're doing, they say, the information you seek about your competitor's plans can usually be obtained by legitimate "open source" means.

"You don't have to do the Mickey Mouse stuff to get proprietary information," Nolan says. "We get that kind of thing all the time just by calling the right people, going through public records and putting the pieces of the puzzle together."

That doesn't mean, however, that there aren't bad guys out there. CI insiders say that certain Fortune 500 companies regularly rely on subcontractors to do their dirty work. "The fact of the matter is there are independent contract relationships," says Halligan, referring to what happens when a CI firm turns around and hires a subcontractor to do the work they don't want to get caught doing. The subcontractor "comes back with a report, and [the contractor] doesn't really inquire how you got the results of that report. You can call that plausible deniability; the fact is the corporation's relationship is with the first person, not with any subcontractor he may have hired."

Interview with the Vampire

Marc Barry is one of the bad guys. He says so himself. A cocky fellow from Dorchester, a working-class section of Boston, Barry won't

Marc Barry is a self-styled bad guy whose "highly manipulative" nature helps him unearth business intelligence.	say how he learned to do intelligence work or which agencies he may or may not have worked for in the past. "I basically developed my skills working undercover for years against Asian organized crime networks that were manufacturing counterfeit stuff" is all Barry will acknowledge in a long phone interview from his office in New York City. But he readily confesses that people who do the kind of work he does have to be "highly manipulative" and "borderline sociopathic." (Barry is also quite
friendly. After two brief print interview phone conversations, he invited this reporter, a perfect stranger, to his loft in Manhattan to see his priceless collection of modern furniture.)	
Barry, who is a founder and president of a CI firm—C3I Analytics—in New York City, says he regularly uses false pretenses to get information on his clients' competitors. And he knows a lot of other intelligence gatherers who do likewise. "The Society for Competitive Intelligence Professionals [SCIP] claims that all of their members abide by ethical rules, that they do everything by open source," says Barry. "You know, information you can pull down from a company's 10K, patent searches, Internet searches, pollution permits, that sort of thing. But that's simply not true. And the reason I know this is because I have been hired by SCIP members to engage in some very dubious activity	

on their behalf."

Barry claims he once (illegally) obtained the phone records of a West Coast defense contractor at the request of a prominent CI firm whose founder is on the SCIP's board of directors. "We do as much open-source stuff as anyone else—and if you know where to look, you can get a wealth of information without resorting to deception and trickery," he notes. "But when it comes to things like profiling a competitor's R&D—like finding out Pfizer's formula for a drug it's developing for arthritis—you're not going to get that without deception or trickery."

A Cereal Killing

Consider, for example, the job that Barry undertook on behalf of a cereal manufacturer that directly competes with the Quaker Oats Co. His assignment was to uncover Quaker Oats's R&D strategy. The first thing Barry and his crew did was conduct a thorough Internet scrub (search) of people and institutions affiliated with the cereal company. In this way, they discovered the names of several prominent professors whose research Quaker Oats was funding. At which point the games began.

"We would pose as just about everything," says Barry. "[We'd act as] grad students writing papers; we'd set up front companies and talk to these professors about the possibility of also funding their research. It's all a matter of knowing how to get the guy to open up to you."

Barry and his minions were also able to penetrate a supposedly secure facility in Chicago where Quaker Oats scientists were doing all kinds of genetic research. "We posed as journalists from an agriculture magazine interested in developments in genetics as it related to crop production, and we were able to meet with key researchers and interview others over the phone."

How did they carry off the deception? "The first thing we did was set up a bogus voice mail box and fax-forwarding line and e-mail address. And the phone lines all had the corresponding area code; so when the [target] called back," Barry proudly explains, "they would think we were in the area when, in actuality, we were talking to them from New York City."

Barry's investigators also canvassed job sites such as Monster.com and Headhunter.net, punching in "Quaker Oats R&D," to find people with that credential on their posted résumés. "Half of these people were still working at Quaker Oats and looking for a job, or had recently left," Barry says. "So we interviewed them." The interviews were done under false pretenses, or the sources were hired as consultants and paid for the information they provided, he says.

His company was soon able to report back that the main focus of Quaker Oats's R&D was to introduce the genetic material from corn into oats to improve crop yield, among other things. The information proved quite valuable to Barry's client. "By honing their own R&D to replicate what Quaker had already done, they were able to bypass millions of dollars in research," he says.

To this day, Barry says, "Quaker Oats doesn't know what happened. It's what we call a clean extraction." Barry insists that none of the techniques his company used in the Quaker Oats job were illegal or cause for a successful lawsuit. "I know exactly where the line is," he brags. "I can dance on the line, but if I get caught behind the line, that's when I get in trouble."

Barry—who recently coauthored the controversial book *Spooked: Espionage in Corporate America*, in which he elaborates on these tricks of the trade—says his clients span the spectrum of Fortune 500 companies. And as a result of publicity from the book, he adds, "I've picked up some new clients."

Working with Raytheon, Barry is trying to land \$12 million in funding to create a new intelligence-gathering "war room" facility to be known as Intelogix. According to Michael Davis, who now works for Raytheon and formerly worked for the National Security Agency, Intelogix will help American corporations use online and offline means to go after counterfeiting operations that market fake products such as ersatz Gucci bags and Rolex watches. The venture, for which Davis holds the title of vice president of business development, will also provide companies with real-time monitoring of information on the Web so that they can stay up to speed on what's being spread about them

or their product.

"Let's say, for example, a rumor starts in a chat room that one of [a company's] products has been tampered with or is defective," Davis says. Company sales have already been hurt by such false rumors, "which spread at the speed of light on the Web. This is a way for companies to see what's being said in real-time and counter it immediately—before it has a major impact on their stock price or market share."

Intelogix, of course, won't be the first to use sophisticated technologies to help companies protect themselves. Investigative firms such as Kroll Associates already offer this service, and a number of vendors sell surveillance software, including "sniffers" designed to ferret out unwanted visitors to a particular company's website and divert them to a look-alike site that contains only superficial information.

Raytheon is also marketing to the civilian sector a covert monitoring software package that it developed for national security agencies. Nicknamed Silent Runner, the software monitors ingoing and outgoing e-mail in real-time as well as whatever websites employees are or have been surfing. "It's like Carnivore [the controversial FBI e-mail filtering technology]," says one CI expert. "It monitors the traffic on a company's network so trade secrets don't go bopping out on e-mail. And it can be programmed to intercept sensitive e-mail."

Despite the barrage of new electronic tools and the well-publicized threat from hackers, intelligence experts say that so far electronic break-ins have been far less frequent and damaging than the more traditional means of securing information through human intelligence. "In four out of five situations, we have found that the compromise occurred by word of mouth, as opposed to sophisticated cyberpenetration," says Alden Taylor, a managing director and practice head of the business intelligence service at Kroll Associates.

The same holds true for corporate efforts to gather competitive intelligence. Dozens of vendors sell software packages that purport to help companies collect and analyze data about their competitors. But according to a recent study by Fuld & Co., a leading CI outfit based in Cambridge, Mass., these technological tools are only one part of the answer. (See "Most CI Software Flunks the Fuld Test," right.) "Technology alone is not the solution to intelligence gathering," says Leonard Fuld, the company's founder. In other words, the old gumshoe approach still prevails.

Most CI Software Flunks the Fuld Test

□. Some offerings help more than others, but nothing does it all

[Read More](#)

Doing It on the Up-and-Up

Located on an industrial backstreet in Cambridge, Fuld & Co. is hard to find, tucked between a larger brick edifice and a mysterious-looking research facility

Leonard Fuld scorns cloak-and-dagger approaches to competitive intelligence. You don't have to "lie, cheat and steal," he says, to serve clients well.

that is surrounded by a barbed-wire fence. But penetrating the yellow brick building that contains the headquarters of Fuld & Co. is as easy as walking through one glass door and pressing a button that automatically opens another glass door. The founder of Fuld & Co. is similarly unimposing, a graying middle-aged man sporting a frumpy tweed jacket and a friendly, puppylike demeanor. But appearances can be deceiving; when it comes to gathering information, knowledgeable people in the field say that Fuld and his team are seasoned pros. In the past 22 years, the CI company has done more than 3,000 investigative assignments for companies here and abroad, and Fuld insists that most of it has been done on the up-and-up.

"We're not angels, and we're not naïve. But there are ways to do this very honestly and ethically," says Fuld, who bikes the few miles from Brookline to work when the weather permits. "And we encourage our corporate clients to stay within legal and ethical boundaries."

Consider the case that Fuld took on a few years ago on behalf of a U.S. food manufacturer. The company was losing market share to a rival, and executives were suspicious that the rival was a money-laundering front for the Mafia. So Fuld's company did what any good CI outfit does first: The staff searched the Net for any and all news articles about the rival company and also checked various computerized databases that make supposedly private information

□- available for a price. "We saw from a credit report that the rival had paid their bills on time, which indicated that they were not starving for cash and were in fact making money," Fuld recalls. Then, his crew went to the planning department at the local town hall and obtained a floor plan of the rival's factory—public information for anyone who knows where to find it.

They showed the floor plan to an engineering expert in the food industry and soon figured out that the rival had five production lines up and running, compared with their client's two. They also talked to the rival's equipment suppliers, who helped them unravel the company's production process.

"There was no putting on false names or glasses, or whatever," Fuld says. "We identified ourselves as a consulting firm. Not everyone talked to us, mind you. But this is a business where you have to do more with less."

They quickly discovered that the rival manufacturer was simply doing a more efficient job than Fuld's client of producing the same basic product. That was why they could sell it at a lower price. "There was no money laundering going on," he says.

Fuld is openly contemptuous of investigators like Barry who routinely cross the ethical divide. "We can find the same information this guy says he finds, but we can do it legitimately," he insists. "Most professionals in this business don't have to lie, cheat and steal" to serve their clients.

They may not have to, but there are a growing number of investigators who do. And if it made the difference between winning a lucrative contract or protecting your company's assets, wouldn't you?
