

Corporate Espionage

Defense Against the DarkArts

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

<http://www.darwinmag.com/read/060101/defense.html>

JOHN NOLAN, A FORMER U.S. 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 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."

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."