Competitive Intelligence

By John A. Nolan, III

It's the Third Millennium: Do You Know Where Your Competitor Is?

Executives at a major pharmaceutical company learn that one of their primary competitors is about to introduce a new product that will directly challenge their leading over-the-counter pain reliever. They learn that the rival will launch the product in two months with a major media blitz that will emphasize savings of a dollar a bottle off the leader's price, with the same ability to reduce pain.

As a result of this forewarning, the executives are able to blunt the new entry through a creative blitz of their own and to take other actions to completely disrupt the new product's introduction for well over a year. In fact, they're so able to retard the new entry, and to defend their own share, that when persons unknown start poisoning people via their product, they are able to withstand all the negative publicity and remain America's number one pain reliever.

Surely you recognize Tylenol in this example, but have you ever heard of Datril?

Johnson & Johnson employed competitive intelligence (CI) in identifying the projected Datril entry, and that CI allowed Johnson & Johnson to take the initiative. In fact, that's really the foundation for all good intelligence: getting the necessary information to the decision maker in time to make a difference, in time to take the right actions.

On the other hand, had Bristol-Myers done some homework to protect that entry during its development and test marketing, it may very well have been able to replace Tylenol in the hysteria that surrounded the cyanide poisonings. And by protection, we're talking about more than the "gates and guards, guns and dogs" orientation that many companies unfortunately set as limits for themselves.

A counterintelligence approach to protection, in the Tylenol/Datril matter, would have been anticipatory, business-oriented, and pro-active. To place this into proper perspective, it might be instructive to look at how Johnson & Johnson actually got the information that allowed it to trump Bristol-Myers.

J&J's intelligence strategy included no midnight skulking, no waste archeology (what some call dumpster diving), no loitering about waiting for a marketing plan to appear in a lobby unattended, no burglarizing, no hacking, no bribery, nor any of the myriad things that might come to mind. Instead, Johnson & Johnson determined that Bristol-Myers had traditionally tested new products in Albany, N.Y., and Peoria, Ill. It was a fairly simple matter to insinuate observers into the test marketing populations in those two cities, and, on the basis of their reports, identify the penetration strategy and dates.

If Bristol-Myers had a counterintelligence strategy, it's hard to discern from the result. Even if it had simply recognized that it had established a pattern to its test marketing activities—and changed the city locations accordingly—Bristol-Myers would have made J&J's CI collection job much more difficult. As my colleague at The Centre for Operational Business Intelligence, Bill deGenaro, is fond of pointing out, "You don't have to make it easy, you don't have to make it fast, and you certainly don't have to make it cheap for the other guy to find out what you're doing."

CI, as an approach that employs legal, ethical, and non-fattening meth-

ods to gather competitively valuable information, is an increasingly common business practice. Thousands of companies around the world use it to find out what their business rivals are planning and to avoid being surprised in the marketplace, or, at least, to reduce those uncertainties that every business finds unpleasant.

What Is Competitive Intelligence?

CI is not a euphemism for industrial espionage or economic espionage. These tactics—CI's evil twin cousins—represent altogether different approaches to information collection and reporting. Practitioners commonly use illegal and unethical means to gather the information—approaches that include bribery, break-ins, computer penetrations, outright theft, and manifold other wholly inappropriate means.

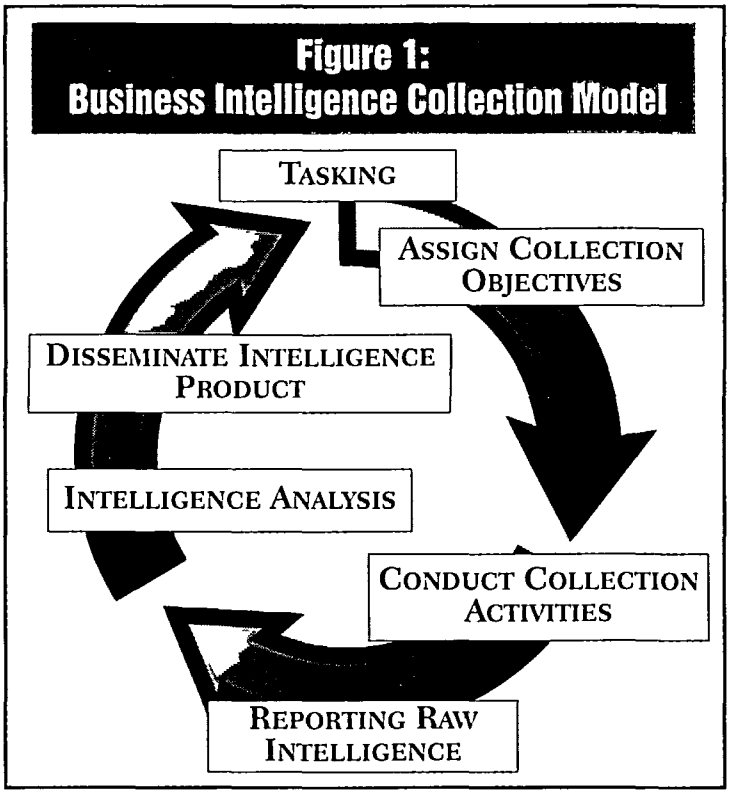
Unlike its cousins, who are more like domestic and international smash and grab artists, CI is an organized, rigorous, and coherent approach to information collection, analysis, and reporting. The CI process, which is illustrated in Figure 1, consists of the following discrete elements:

Tasking: A CI professional's first order of business is to determine what kind of information is needed. That is, together with the firm's leaders, they must decide the scope of the intelligence gathering. The leaders should have a specific goal in mind—to gather information about a product under development, or to obtain information about a competitor's planning in a certain area, for example.

Collection Objectives: Once those responsible for competitive intelligence understand the task, they can refine it into the particular sub-components that together represent the principal collection requirements. They can then identify the sources of information—both primary (knowledgeable individuals, including suppliers, customers, or even their own or their rivals' employees) and secondary (published in both print and electronic media)—that will begin to satisfy the collection objectives.

Collection Activities: Secondary sources—the open and publicly available media such as the trade press, help wanted ads (which can help pinpoint the areas in which a competitor is staffing up), and technical papers—are a good starting point for information gathering. They are not necessarily the best sources of current and reliable information, but they provide valuable background data as well as the means to identify those primary, human sources who have the most up-to-date, and reliable, information.

Figure 1: Business Intelligence Collection Model



Interim Reporting and Initial Analysis: As they collect the information, the CI experts regularly check and measure it against known or postulated data, assessing its accuracy and validity.

Analysis: Once the collection activities are complete, the CI professionals subject all of the information to rigorous analysis, particularly as it relates to established assumptions. They are careful not to force the data to fit the assumptions, however, because that would undermine the integrity of the project.

Furthermore, there are often unexpected yet very valuable discoveries when the Law of Unintended Consequences goes into operation. As the CI process goes forward, inevitably there are pieces—sometimes even whole blocks—of information that come into the hands of the collectors. They can open whole new lines of inquiry, identify whole new products or product lines, or provide early notice of heretofore unknown acquisition activity.

Reporting and Dissemination: At this point, the intelligence gatherers present the results of the collection activities and analysis in both an oral presentation and in a written report that provides greater detail.

What Is Counterintelligence?

Irrespective of whether your competitor is using the legal means of CI or the illegal means of the other approaches, the simple fact remains that the best way to protect yourself is to employ a counterintelligence process. Simply defined, business counterintelligence consists of: "Those active measures undertaken—sometimes in conjunction with federal

agencies—to identify and neutralize the information collection activities of business rivals."

Why sometimes? After all, wasn't the Economic Espionage Act of 1996 specifically enacted to deal on a federal level with this kind of problem? Isn't the FBI there to protect us? Hardly. And the reasons many firms avoid becoming involved with federal agencies are many and varied. Some are simply skeptical that "the guy from the government is here to help you." Others are concerned about the effects of publicity, especially if exposure decreases shareholder confidence. And still others fear losing through the discovery process that accompanies litigation the very information they took such pains to protect. In short, the EEA is simply not the answer to every maiden's prayer.

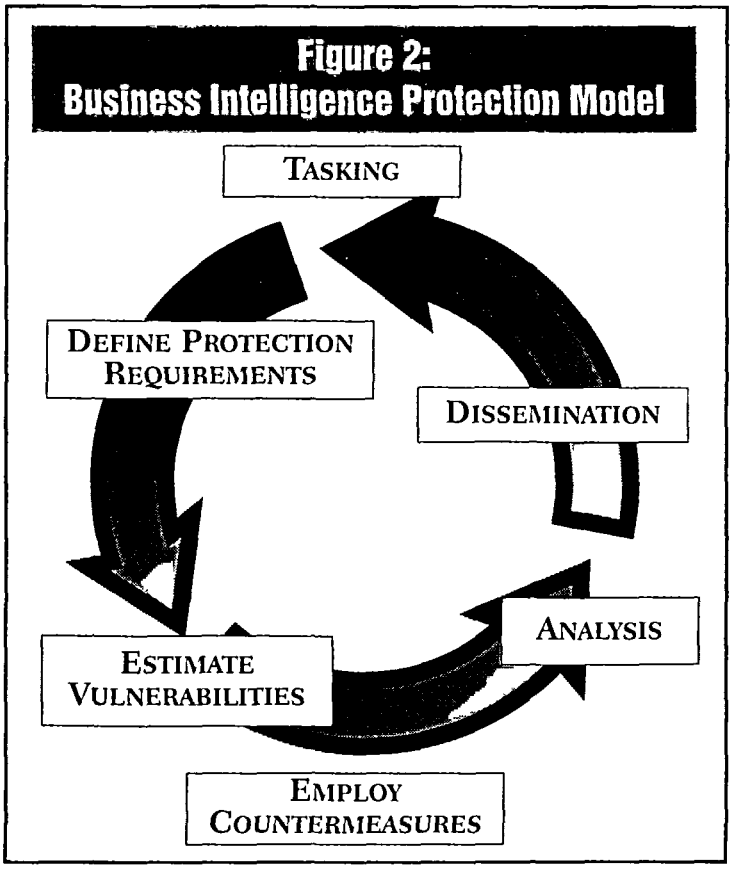
For more and more businesses, a counterintelligence approach makes a great deal of sense because business leaders are becoming more attuned to, and greater consumers of, intelligence products. Indeed, when executives discover how much accurate information they can get legally, ethically, and quickly, they often begin to wonder just how vulnerable *their* company is. They begin asking themselves the two questions that most leaders and strategists ought to be asking themselves every morning as they gaze into the mirror: One, "Why is our competition making money at our expense?" Two, "What is there about us that allows us to make money at their expense?" The first question drives the intelligence collection cycle, the second drives the counterintelligence and protection cycle.

The Counterintelligence Cycle

Counterintelligence is far more than a Barney Fife wannabe sitting around eating jelly donuts, waiting for something to happen. It's far more than someone hitching up his pistol belt and telling Betty Sue at the all-night diner "Well, Darlin' tonight I had to roll on a 459 and it really got hairy out there for a while." Instead it's a formal and rigorous process that is nearly as old as the collection process.

Tasking: Figure 2 depicts an organized counterintelligence approach. At the top of the process, gaining clear and specific tasking about what to *protect* is just as critical as clear and specific tasking about what to *collect*. Just as no CI professional in his or her right mind would accept an assignment to "go out and get me everything you can on XYZ Company," no counterintelligence practitioner is going to accept an assignment to "protect everything in sight."

Figure 2: Business Intelligence Protection Model



In defining what needs to be protected, the counterintelligence professional is not interested in wasting time, effort, or energy on the things that the security force is already doing. The security management team has already taken measures to prevent thefts, break-ins, and other criminal and illegal acts. But rivals' CI practitioners aren't trying to steal the crown jewels—they're collecting numerous disparate pieces of information that will provide competitively valuable insights once all the pieces have been gathered and analyzed. A platoon of armed security officers and the most effective locks in the world won't protect sensitive information from this kind of attack.

Requirements Definition: The counterintelligence professional needs to know what needs to be protected, for how long, and from whom. Then, he or she must break those sensitive plans, strategies, or projects down into individual components to identify those critical ingredients or elements that the competitor's CI professional is after.

Assessing Rivals' Competitive Intelligence Capabilities: Once he or she understands what needs to be protected, the counterintelligence practitioner focuses on assessing rival firms' CI capabilities. This includes becoming familiar with the information sources and information collection methods rival firms customarily use, as well as identifying those in the industry who "stop at nothing to get what they need." The process coincidentally reveals quite a bit about what the competition is trying to collect. This becomes major advantage of the

CI/counterintelligence integration: Knowing what the competition is asking is often an early indicator of where *they're* going as a company.

Understanding how a rival firm goes about collecting against the company leads to the next step—trying to emulate the rival's behavior. In essence, this means that the counterintelligence people attack their own company as if they were actually working for the rival firm. And they often work backward from a postulated loss of information to determine how a rival got the information in the first place.

Assessing Vulnerabilities: The next step in the protection model is to test the firm's vulnerability to the collection methods that the rival firm is known or believed to use. Quite often, clues about these methods come from the security department's records of other types of losses, investigations, and reports from line employees when they field unusual or suspicious questions from someone outside the firm. Further, once the firm understands its weaknesses, it can decide—long before sensitive information is compromised—how it will manage the vulnerability.

The concept of "managing" a vulnerability perhaps more clearly than anything else illuminates the difference between security and counterintelligence: Security would close the vulnerability as if it were a hole in a fence; counterintelligence would seek to find what opportunities the vulnerability presents. For example, a firm might decide to put certain kinds and classes of information purposely at risk. That is, it might allow a rival access to certain facts along with false information that can encourage the rival to draw erroneous conclusions about where the firm is really headed or when it anticipates getting there. Or, in a variation, the firm may capitalize on what it has learned that the competitors *think* they know. This, in turn, leads directly to the identification of what vulnerabilities the rivals' CI collectors and analysts have that may be exploitable.

As an example, there is the well-known business case of Johnson Controls and Honeywell, both manufacturers of building control systems. Johnson Controls had spent about $20 million and three years developing a digitized control system for use in the U.S. and Europe. Johnson had code named its project Loba. Honeywell's salespeople, who didn't have an organized CI system, heard about and reported a new system from Johnson Controls that was called Lobo. Just a one-letter difference, but it made all the difference when Johnson Controls decided to confuse Honeywell about what was actually happening. It renamed a relatively minor control system Lobo and invested a couple hundred thousand dollars in a fairly splashy ad campaign. When Honeywell recognized Lobo for the low-level product that it really was, it abandoned its interest—just long enough for Johnson Controls to finish its development and beta testing of Loba; just long enough for Johnson Controls to gain first-to-market advantage and significant share in the multi-billion dollar market.

When executives discover how much accurate information they can get legally, ethically, and quickly, they often begin to wonder just how vulnerable their company is.

Countermeasures Development: Developing countermeasures is perhaps the most interesting and intellectually stimulating of all the aspects of the counterintelligence process. Countermeasures not only help protect what needs to be protected, they may also provide the means to change the value and character of the information that the firm's rivals are collecting—in order to influence how those rivals will react to that information.

Countermeasures can be simple or complex, long-term or short-term, and they can be designed with specific rivals in mind. Consider how a defense and aerospace supplier we'll call Zygote Technologies dealt with its much larger rival, Allegro Aerospace. Allegro's well-developed and highly functioning CI unit was highly respected for the great work it did in helping win in excess of 80% of its competitive procurements, often at the expense of such firms as Zygote. With Allegro's capabilities in mind, Zygote developed a fairly aggressive employee awareness program, complete with a system for reporting questionable contacts from outsiders. Zygote identified the sources Allegro's CI team was contacting—and had been contacting over time—that had provided details of competitive pricing proposals. Selected Zygote employees were provided certain key elements of an overall concept that Allegro was allowed to collect, elements of which fit in with Allegro's leadership's known biases and prejudices.

Through five separate procurements over an 18-month period, Allegro's CI team collected all of these elements and reported them to its leaders. But when that information always led to the precisely wrong conclusion, Allegro's leaders decided that they were spending a lot of money on a CI unit that simply wasn't answering the mail. Zygote was thus doubly successful: Using the intelligence equivalent of martial arts, they allowed Allegro to use its CI strength against itself to reach erroneous conclusions and to lose several millions of dollars worth of business, and concurrently helped create the conditions that led the once highly respected CI unit to be disbanded. It effectively blinded Allegro's leadership by taking

away its eyes and ears, and it effectively neutralized its main competitor's CI organization.

Perhaps it would be well to ask yourself at this point about the last time that your security organization, confronted with a business issue such as this, assisted in ways that allowed you to cash in on business opportunities.

Once the firm selects the most appropriate countermeasures, it must analyze how well they are working and whether they should be modified. It is at this point that the integration of CI and counterintelligence begins to pay off. CI practitioners, who have been following the company that is the target of these countermeasures, provide important insights into how that rival is responding.

Analysis and Dissemination: When integrated, competitive intelligence and counterintelligence give senior executives a clear and complete intelligence picture of the marketplace and significantly improve their ability to reach decisions on the basis of the best and most comprehensive information available.

The Well-Honed Edge

Much of strategy and tactics—whether political, social, or business—is rooted in the history of military operations. When corporate strategists study Sun T'zu and Genghis Khan, Clausewitz and Schwarzkopf, and attempt to apply those leaders' concepts to the business battlefield, they become exceptional consumers of intelligence. They know what to ask for to support their plans, they know how to get it from their collectors and analysts in time to make a difference, and they know when and how to take action.

This is the essential function of the intelligence process: Allow the leader to take the right actions for competitive advantage. Indeed, in more and more companies, leaders are developing intelligence and knowledge cultures. These cultures are committed to protecting the assets, operations, and processes that constitute the company's competitive edge—and to protecting the sources and methods that help them keep that edge. ◆

John A Nolan, III, is chairman and managing director of Phoenix Consulting Group, a Huntsville, Ala, firm that provides integrated business intelligence solutions to firms across a variety of industries. He is the author of the recent book CONFIDENTIAL: Uncover Your Competitor's Top Business Secrets Legally and Quickly—and Protect Your Own *(HarperCollins, 1999). He may be via e-mail at jnolan@intellpros com.*