TIPS ON TOOLS

Ethical Business Intelligence Is NOT Mission Impossible

by Bill Fiora

Business intelligence is one of the fastest growing disciplines in corporate America. To many, however, the words conjure up images of trench coats and meetings in back alleys. Unfortunately, recent events only serve to reinforce these fears. Earlier this year, for example, Volkswagen agreed to pay $100 million to General Motors after the U.S. firm alleged that VW used documents pilfered by an ex-GM executive to its competitive advantage. More recently, Johnson & Johnson and Boehringer Mannheim settled out of court after trading accusations of improper activities, including infiltrating company meetings and taking confidential documents. Even more unsettling to some may be the passage of the Economic Espionage Act in 1996.

"Simply stated, legal and ethical guidelines are the ground rules that all employees must follow in carrying out their business intelligence duties, be that speaking with suppliers, customers, or even direct competitors."

Bill Fiora is a senior consultant in the business intelligence practice at The Futures Group, a Glastonbury, Conn., firm that focuses on helping companies manage the uncertainty of planning for the future.

The law makes it illegal to steal any material that a business has taken "reasonable efforts" to keep secret, and if the material derives its value from not being known. The Act imposes fines of up to $5 million and 10 years in jail for domestic cases, with greater penalties for cases in which the theft is committed on behalf of a foreign government.

What's the manager of a new business intelligence unit to say when the chief executive officer or president declares, "We don't need this kind of publicity. Leave the espionage to the CIA." The appropriate response is to agree wholeheartedly, of course. Espionage is too risky and, surprisingly, unproductive. Business intelligence, however, has proven itself too powerful a tool in today's competitive marketplace to be ignored. These recent cases not only show the difference between espionage and business intelligence, they also demonstrate the need for clear ethical and legal guidelines to guide the intelligence effort. (See sidebar: Business Intelligence vs. Corporate Espionage.) Rather than dismantling their intelligence units or restricting them to searches of published literature, top management should instead ensure that their intelligence activities conform to stringent legal and ethical standards and that these guidelines are conveyed clearly and frequently to all employees.

Simply stated, legal and ethical guidelines are the ground rules that all employees must follow in carrying out their business intelligence duties, be that speaking with suppliers, customers, or even direct competitors. Whatever form the guidelines take, they must reflect and reinforce your company's corporate ethical guidelines—with added specificity about intelligence activities. Clients of The Futures Group have spanned the range in terms of how detailed they make their guidelines—from a simple statement of the company's commitment to the highest ethical standards to a multi-page document of specific guidelines and examples that leave little doubt in the reader's mind about what is and is not permitted. Whatever method you choose, it is critical that the guidelines mirror the ethical culture of the organization.

What's the best way to institute such guidelines? Perhaps the most critical element is the support of top management. This ensures two things: that the guidelines will be followed and enforced, and that they are seen to apply to all employees, not just those in the intelligence unit. Any guidelines that lack top management's support will soon be forgotten or ignored.

Secondly, it is crucial to enlist the help of your company's legal department early on. Just the mention of business intelligence can give some lawyers the shakes, conjuring up a host of fears and misconceptions. Meeting with your lawyers early will allow you to fend off these misconceptions and gain your attorneys' input before you begin drafting the parameters. In return, by engaging the legal department you can help elevate the status of the intelligence unit. If your guidelines are "blessed" at the corporate level, a clear signal is sent that the intelligence unit is an integral part of the organization that's here to stay. Too, you can begin to forge a valuable relationship between your company's intelligence and legal units, which often have information of value to each other. Corporate lawyers often know first about pending legislation or regulatory issues that could affect company strategy. For its part, the intelligence unit can often provide early warning of potential takeovers, as well as input on mergers and acquisitions and anti-dumping cases.

Business Intelligence vs. Corporate Espionage

Business intelligence professionals often face a myriad of stereotypes, including the perception that they engage in espionage. Corporate espionage is unethical and often illegal. In contrast, business intelligence is a series of systematic techniques to collect, validate, analyze, and deliver public information and expert insights about the competitive environment to those in your firm who can act upon it. Here are some sample guidelines to help employees realize the difference:

DO

- Share public information gleaned from published materials, factory tours, trade shows, etc.
- Talk to suppliers, vendors, or customers if they are willing to share information about a third party.
- Speak with new employees if they are willing to share public information about their former employers.

DON'T

- Misrepresent your identity or corporate affiliation.
- Ask your contacts or outside consultants to share information that is confidential or privileged.
- Make employment or business negotiations contingent upon providing competitive information.

Remember, no piece of competitive information is worth more than your firm's solid reputation—or worse yet, worth risking a lawsuit or prosecution. Public information, coupled with insights from your own employees and analyzed in a systematic way, is more cost-effective and more valuable than any information obtained through unethical or illegal means.

Third, the guidelines should be introduced with a short training program. It's important that everyone know the limits of legitimate business intelligence from the outset. Equally important, the guidelines should not frighten employees into ignoring the valuable information they come across daily. A short training program can help strike this balance. In it, there should be a discussion of the inevitable gray areas employees may encounter. What is a salesperson to do, for example, if a contact volunteers a document from your competitor that is clearly proprietary and reveals some valuable insights? The answer to this will vary by firm, and it is important that your employees recognize the potential for such situations. It's important at this point, therefore, to give your employees a single point of contact to call if they have questions or concerns. This person could be in the legal or security department, but it's best to designate only one contact point to avoid confusion.

What specifically should your intelligence guidelines include? First, they should refer directly back to your corporate ethical guidelines. Doing so makes it clear that this is an extension of your corporate guidelines and not a new task or initiative. Like involving the legal staff, this is also a good way to add the corporate imprimatur to your intelligence efforts as a way to boost their status and recognition.

The guidelines should include specific examples as necessary. Obviously, illegal activities like theft, bribery, and wiretapping should be clearly prohibited. In more ambiguous situations, however, examples can go a long way in explaining your corporate standards. Some firms use video tapes of employees in questionable situations in their training sessions and stop the tapes for discussion at the end of each segment. The debate that follows is often lively and always informative. Some possible situations to include are the proper use of outside consultants, guidelines for interviewing former employees of your competitors, and proper conduct at trade shows and conferences.

There are a number of benefits to having such guidelines—beyond the obvious of staying out of court and out of prison. First, clear, explicit guidelines can help alleviate any concerns among employees that their firm is engaging in espionage or other skullduggery. On a more practical level, should an errant employee engage in illegal behavior, guidelines can help protect a firm's management from legal harm by demonstrating that this was clearly outside the bounds of acceptable behavior and not sanctioned by management.

Corporate managers, therefore, need not fear the recent anti-espionage lawsuits and legislation as long as a firm's intelligence activities remain within the bounds of a well-crafted set of legal and ethical guidelines. Neither should they worry that such guidelines will "straight-jacket" their intelligence units and prevent them from collecting timely, actionable intelligence. These latest accounts of business espionage gone awry present an opportunity to maximize and strengthen the business intelligence unit's place in corporate decision-making. It is surprising how much good intelligence can be gleaned and analyzed from public information—some of America's leading companies have been doing this legally and ethically for years. So put away your trench coat and spy camera and turn to your telephone and your computer. The information you need to compete is out there—in the minds and reports of your own employees and those with whom they work. Your mission, should you choose to accept it, is to find it and make sense of it before your competition does. ■