

Competitive Intelligence: An External Threat and an Internal Requirement

by Naomi R. Fine, Esq., President, Pro-Tec Data

A Fortune 500 company authorizing an illegal entry into a competitor's network? Tapping phone lines? Intercepting confidential faxes? Highly unlikely. It's illegal, reputation-shattering, and just plain poor business sense. But what about a competitive intelligence review? It's legal, cost-effective, and often results in acquiring more valuable information about competitors than many illegal approaches. Actually, it's a routine practice for many companies, including a majority of the Fortune 500.

Information is now more accessible than ever. Companies around the world are taking advantage of technology to actively research their competition. A growing number of companies are spending hundreds of thousands, sometimes millions of dollars to acquire competitive intelligence. Their investment is aimed at gaining an advantage from your company's information.

What is Competitive Intelligence?

Competitive intelligence (CI) involves gathering and analyzing information that helps companies better understand their competition. Information about a competitor's capabilities and intentions provide a solid basis for improving market position and crafting strategic plans. The sought after information includes customer lists, price and cost information, production processes and R&D developments. All of this information, which is extremely valuable in the right hands, can be disastrous if put in the wrong hands: the hands of competition.

“The line between competitive intelligence and corporate espionage is the line between legal and illegal, ethical and unethical. This line is often blurred.”

Most companies involved in competitive intelligence begin by conducting online database searches to obtain detailed profiles of their rival companies. Databases and search services have become extremely prolific. The efficiency of the automated process makes these services an easily accessible source for up-to-the-minute details about almost any competitor.

Competitive Intelligence: An External Threat and an Internal Requirement

For many companies, online searches are just the beginning. The core of competitive intelligence comes from the target company's employees, customers, vendors, contractors and consultants.

How Do They Do It?

How does a company get product, pricing, cost, timing, engineering and sales information from a target company, its customers, and its suppliers?

By hiring a competitive intelligence professional from one of the many consulting firms around the world that provide this service.

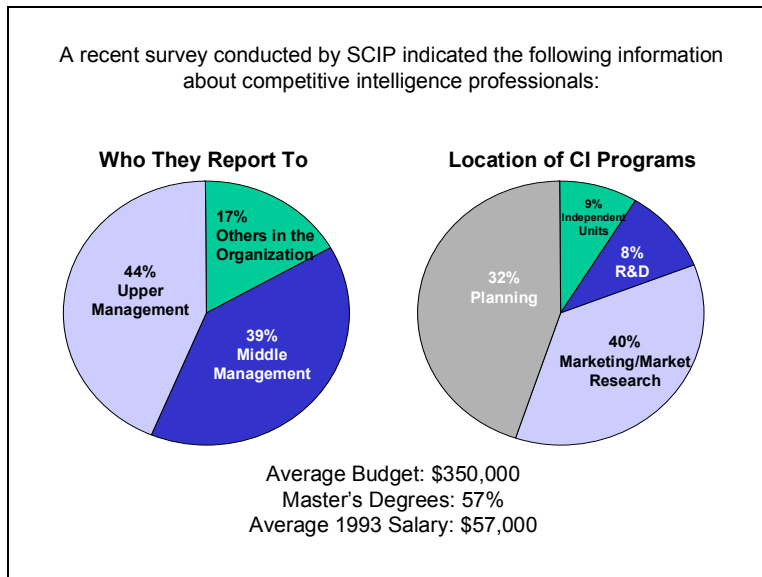
They call themselves "Competitive Intelligence Consultants," "Market Researchers," or even "Information Brokers". Whatever the name, they are experts at eliciting detailed strategic and tactical information from a target company's employees. These firms brag that they can "obtain any information from any company", "tap the knowledge and experience of key players in the market", "provide competitor's costs, product plans, profits and other secrets" and "gather anything you need to know." Their tools are the telephone, excellent communication skills, and unrelenting persistence. They achieve the results they promise, often by simply asking for what they want. CI professionals provide their clients with an in-depth perspective into a target company's future.

The Society of Competitive Intelligence Professionals

How big is the threat? Is there a "...method to this madness?" There is not only a method, but a well established organization that supports the competitive intelligence industry whole-heartedly.

The Society of Competitive Intelligence Professionals (SCIP) which aspires to "serving professionals engaged in collection, analysis, and management of information on competitive and business strategies" was founded in 1986. Today, this highly regarded organization boasts over 5000 active members. This number represents employees from some of the world's most prestigious companies with titles like Market Analyst, Research Analyst, Project Manager, Manager of Corporate Development, and Director of Corporate Strategy. Other members are the consultants representing several hundred firms that persistently wage war on companies' secrets, armed only with a telephone and a friendly voice. The chart below summarizes findings about competitive intelligence professionals.

Competitive Intelligence: An External Threat and an Internal Requirement



Should You Be Concerned?

Computer hacking and electronic interception have been, and may always be, threats to all companies. Unfortunately, reducing these threats may do nothing to alleviate the most damaging source of information loss: unsuspecting employees. CI professionals laugh at the immense resources expended by companies to secure computers and electronic communication, particularly when companies have employees so willing to talk.

Likely targets of CI are in competitive markets, utilize valuable proprietary information, are in a state of growth or change and do business in a way that makes their information accessible.

The most effective way to reduce the risk of loss to competitive intelligence is through employee awareness. An effective employee awareness plan includes a strategy to educate employees regarding:

- The motivation that drives a CI project
- Actual tactics that CI professionals use to gather information
- The damaging results of a successful CI initiative
- Preventative measures an employee can take to keep illegitimate researchers from getting the information they want
- Guidelines on reporting suspected CI inquiries and information vulnerabilities to the appropriate department (e.g. Information Security or Public Relations)

Competitive Intelligence: An External Threat and an Internal Requirement

Employee awareness of information protection issues often does as much to protect a company's proprietary rights as physical, technical and electronic access controls.

It's Closer Than You Think

Competitive intelligence is not just an outside force against which a company must defend itself. Rather, CI is also a valuable asset cultivated within a company. By tapping into internal intelligence resources, such as the sales force, marketing teams, and purchasing departments, a company can obtain valuable knowledge about the competition.

Sales representatives are constantly gathering information from customers, trade shows, association meetings and even 'casual conversation.' Marketing departments are monitoring the industry, looking for patterns from which to forecast. Purchasing departments evaluate different suppliers to decipher who can best fit their needs.

Companies that recognize the value of CI set up communication channels to take advantage of internal as well as external sources of intelligence. Typically a person or group is responsible for collecting and analyzing intelligence from online database searches, CI consultants and internal sources. They then distribute it within the company to the person or group that can benefit most from the information.

Using Competitive Intelligence to Your Advantage

Competitive intelligence is not only valuable for strategic and tactical decision making, it is also a helpful tool for improving information security.

At Pro-Tec Data we have had a number of clients use competitive intelligence initiatives to assess information vulnerabilities. We arrange for companies to hire a CI firm to conduct a competitive intelligence "audit" on their own company. This entails a CI firm conducting an investigation by attempting to retrieve confidential and sensitive information from the company that hired them, as though they had been hired by the competition.

In this process, the CI firm is examining the critical flows of information and uncovering the sources of vulnerability within the company. In one case, we were able to get the spell-bound attention of a company's entire executive staff. The embarrassing evidence of information the company had freely given to a CI expert was more convincing than any hypothetical threat or incident experienced by another company. Following a presentation about the information the CI

Competitive Intelligence: An External Threat and an Internal Requirement

expert was able to gather, we presented a proposed comprehensive information protection program based on priorities indicated by the "audit". The executive staff immediately committed to implementing the program we proposed.



Summary

Protecting proprietary information as it is processed, stored, and communicated requires a comprehensive approach that reduces all risks of loss. Computer security is just one component of an effective plan. Employee education is another. Competitive intelligence is a growing threat to all companies in today's competitive market. CI is also a valuable resource recognized and cultivated by many companies. Understanding both sides of CI is a requirement of staying competitive and critical to planning and implementing an effective information protection program for your company.

About the Author:

Naomi Fine is an attorney and the President of Pro-Tec Data, a consulting firm dedicated to helping companies identify and protect confidential information. Pro-Tec Data develops and implements information protection programs that incorporate legal, computer security, human resources, and audit protections. Pro-Tec Data's clients include many Fortune 500 companies. An innovative leader and team player, Ms. Fine has helped thousands of executives and managers incorporate information protection into their corporate vision and business objectives. Ms. Fine is the author of hundreds of information protection policies, procedures and standards, employee handbooks, training programs and employee communication materials. Ms. Fine is a member of the Information Systems Security Association and the American Society for Industrial Security. Ms. Fine is also a member of the Society of Competitive Intelligence Professionals, which proves her information to help Pro-Tec Data's clients take advantage of the offensive advantages and defensive requirements of CI initiatives.
