The Corporate Spy: Espionage in America

By: Matson Breakey

It's probably not news to you that Larry Ellison, CEO of Oracle Corp., is a self-made billionaire. But did you know that this man is so competitive that he hired a couple private spy types to steal garbage from his biggest rival, Microsoft, the world's number one software firm?

And did you know he's not alone? Millions of dollars are spent every year in a very secret part of corporate America's research and development (R&D) effort: Corporate Espionage.

The cold war may be over, but the men with the skills are still around. Today they are not looking for government secrets - there's no money in it - they are looking for the next big, money-making, mouth-watering, high- (or low-) tech breakthrough from GE, 3M, HP or any other part of corporate America. What's their goal? Profits!

The Legal

Before we dive into the dark world of corporate espionage, it is important to understand that not all research of your competitor is considered illegal. There is a legal and respectable way to obtain information on your competitors, and it is called, appropriately enough, competitive intelligence.

By definition, competitive intelligence encompasses only the legal aspects of data collection and analysis. It is the culmination of a legal and ethical effort that leads to a company's successful product launch or perfect timing in the marketplace. Every company that has had success has utilized competitive intelligence in one form or another. Some larger firms like Palm not only have a CEO, CFO and CIO, but they also have a CCO, a chief competitive officer.

According to Business Week Online, competitive intelligence encompasses everything from "scouring securities filings and news reports to database research to schmoozing with representatives of rival companies at trade shows." In addition "many large U.S. companies spend upwards of $1 million a year" following and understanding their competitors every move. So much so that the resultant information is built "right into their sales strategies."

And this, by all accounts, is perfectly acceptable practice for any company anywhere, because, according to Business Week, "companies of all sizes need to know what the competition is doing, planning, thinking about and worrying about."

Many times, the legal information and analysis is generally obtained from the area of intelligence known as Open Source. Open Source is exactly what it seems. In today's wide wired world there are a millions of bits of data literally surrounding us and following our every move. If you have the time and patience, and like putting together puzzles, what you can find on the Net or in the news media would astound you, shock your parents, and scare the heck out of your grandparents.

And then there's the point where the research crosses the line.

The Illegal

Procter & Gamble hired spies to check up on their chief rival Unilever but shut down the program when one of the spooks was caught doing a little more than dumpster diving.

Larry Ellison hired detectives to steal Microsoft garbage in a desperate effort to obtain evidence in court.

And somewhere, right this very moment when your reading this article, a bribe is being passed or a computer is being hacked by a would-be agent of espionage in a veiled attempt to obtain juicy tidbits of information for his or her boss.

Corporate espionage, in a definition provided by Business Week Online, is the "theft of trade secrets through illegal means such as wiretaps, bribery and cyber intrusions."

According to Corporate Espionage 101, a report by Shane Robinson of the SANS Institute rr.sans.org corporate espionage is "a threat to any business whose livelihood depends on information." Corporate spies look for any kind of information whether copies of signed contracts, vendor lists, thumbnail notes from a corporate meeting - any data that could give the aggressor firm an upper hand.

With the advent of the Internet, corporate America opened itself up to even greater threat of information theft by permitting a direct line into its systems allowing hackers and crackers to join the ranks of the corporate spook. In addition, the insistent pursuit of the great paperless society has left more of corporate America's most vital documents and secrets on every office computer or laptop being used. It is estimated that corporate espionage costs corporate America hundreds of billions of dollars per annum.

According to a SANS Institute report, the illegal corporate spy can be "classified into two basic categories": those on the inside and those on the out. Insiders, or employees, are estimated to be responsible for over 85 percent of corporate espionage. The immediate access to information and the temptation for getting back at the grumpy boss can lead to some serious losses.

Hired spies, private dicks, hackers and script kiddies are all outsiders. They enter from outside the firm and attempt to use their skills to obtain any "proprietary information" from the target company.

In one example, two large companies were each putting forward a bid on a $900 million dollar deal. Using the well-practiced tools of a hacker, one company hacked into the other, discovered its e-mails relating to this bid, downloaded them and, therefore, underbid its competitor and was awarded the large contract.

Straight from James Bond's handbook is the kite, or expendable agent. This agent is directed to find information and in the case that the gig is found out, the client cuts the "string to the kite" and lets him or her deal with the authorities on their own. Plausible deniability is the catch phrase here.

An example from the SANS files is the case of a company executive who was traveling

with his laptop. The laptop contained key information on the firm's most pressing and important programs. Leaving his room for dinner, the executive innocently left his laptop in the room. During his absence a consultant (a.k.a. kite) to one of his competitor's entered the hotel room while the maid was turning down the bed and downloaded the information without anyone ever suspecting a thing. His partner was casually watching the executive in the dining room prepared to use his cell phone if and when the executive chose to return.

To paraphrase, all's fair in love and business. But, what if the kite wasn't hired by a competitive company; what if the contractor was a country?

The Downright Dangerous

From Russia to India. From France to China. They all want a piece of it. They all dream of it. Yet they can't quite grasp it. It's our American ingenuity and it's the envy of the world over.

The desire to know what we know, to have an upper hand on our economic superiority, has led to massive investments by sovereign nations into the realm of corporate espionage.

The leader of the pack is our good friend the People's Republic of China. For decades, China has been infiltrating American firms. According to United States Senator Richard Shelby in a statement to Forbes magazine, the PRC is "trying to make the great leap forward, technologically speaking." And they are doing so by stealing the information from us.

China's MSS, or Ministry of State Security, has been reported to recruit college students and employed professionals to be agents within the United States. They are given instructions on the type of positions they should seek within companies and are ordered to work their way into sensitive areas.

State-sponsored corporate espionage is very socialistic in nature. Governments like China utilize their extensive state resources to target information, gather information, and then pass the resultant information into the pockets of its industry leaders. The idea is to boost its economy by creating a competitive advantage.

It is estimated that at least 23 countries are actively pursuing programs of espionage in corporate America.

According to Forbes magazine, before China dominated the playing field, Japan was the big boy in the playground. In the eighties, Hitachi was accused of stealing secret information from Big Blue (IBM). And just a few years ago France was accused of using the Paris Air Show as a national convention for its spy agency, the Direction Generale de la Securite Exterieure (DGSE) causing several contractors to pull out.

While some may find economic espionage to be part of our global marketplace, we must remember that the further entrenched they become, the greater chance they have to simply screw things up. The same hackers that China might use to gain access to GE for a not-so-innocent look at e-mail, can also plant a Trojan horse that could simply destroy GE's system and cost the company millions of dollars.

Then There's Us

I must confess, I too am a sponsor of corporate espionage, I mean, competitive intelligence. As the President and self-appointed CCO of Design Dögs, I have just established a program of competitive intelligence to include research and observation of all our competitors, learning the services they offer, the prices they offer it for, and whether or not they order sushi on Fridays.

Dumpster diving anyone?