Private Intelligence Service - Cobra Systems LLC
Information Broker - Private Intelligence Service – Counter-Espionage

www.cobra-systems.com/intelligence marketing@cobra-systems.com

"Know your enemy, know yourself"
Sun Tzu (ca. 520 B.C.)
Chinese military general, strategist, and philosopher

Our era is being called "information age" for a reason. Our world and even our lives have become more and more digital, both private and business. "Data", or information – sometimes being referred to as "intelligence" - has become almost a currency, and a very important one at that.
Obtaining and protecting such data is now a core task for any business, government, and organization.

The importance of "intelligence" is by no means news. About 2500 years back, the above mentioned Sun Tzu wrote a manual about the art of war, comprising the rules for espionage and the use of spies, and these rules are still valid to this very day. **Espionage is the MOST IMPORTANT single activity of governments and security services. Espionage is also the MOST ECONOMIC way to secure both military and business success**. No government in the world can do without taking care of espionage and counter-espionage, nor would any government have the intention to refrain from it. **Even the Vatican has an intelligence service, a very effective one, too, and one of the oldest still existing ones in history**.

Naturally, corporations are the main target of industrial and corporate espionage, thus no company, with even a medium importance to their own branch of industry, can simply ignore espionage, counter-espionage, protection of data and company secrets or with the process of vetting staff, clients, partners, associate and suppliers. **At the very LEAST, all this MUST be done in order to protect one's own company, the jobs and the staff**.

For a whole number of reasons, managers and business owners do not like to take their problems to the authorities in order to solve problems with corporate intelligence and espionage. At the same time, most businesses do not have the capabilities to maintain their own specialized counter-intelligence department; it is simply too costly. **And so it happens very often that the whole matter of espionage and counter-espionage is simply and eagerly being ignored, overlooked, put aside**.

Given the annual losses in the BILLIONS of dollars, due to industrial espionage, this kind of action by the corporations is not optimal at all. Each year, the economy of the important Western countries lose industrial secrets to the countries most active in espionage. Industrial secrets are being lost, whole companies go down, jobs are destroyed forever. And all this is fully unnecessary.

Of course companies are trying to cut down costs wherever possible. Unfortunately, many, if not most companies save on important security measures. **This type „saving money" can in fact become extremely costly...** Most managers and business owners do not like to take advice, and when a security counsel talks about "security", managers most often think exclusively of „costs" and try to avoid this matter completely.

With a very high percentage of likelihood, given your company has any real meaning in your line of business, you can almost be CERTAIN that in some way you have already been the target of espionage, in one way or another. Your competitors, intelligence services, criminal gangs and groups,

and possibly even terrorists, as well as a plethora of groups and organizations spy against basically ALL business at one point. **If your business possesses goods or knowledge that can be SOLD or if your business has a strategic value of any kind, it is extremely likely that one of the above mentioned groups have already at least attempted to spy on or infiltrate your company**.

The other side of the same coin is almost just as much being neglected: **the use of professional methods to obtain data and information that is needed or can be useful to your own business**. The largest part of all businesses does not use all available methods to the full extend in order to obtain data, and thus leaves money on the table. This goes for obtaining intelligence, for counter-intelligence and for the right kind of training of staff and key personnel.

A business owner and/or manager simply MUST be very aware that each member of staff, and particularly the key members of staff, are the bearers of the company secrets.
This goes both ways; the key staff of your competitors also are in possession of valuable information. This is why there's almost a war going on in regards to headhunting (and **just look at that expression in itself!**)...

Thus, your employees MUST be trained to detect attempts of espionage, know about the methods used by the various attackers, and be able to act accordingly in order to prevent espionage.
If done right, your OWN FULL STAFF becomes your security department!
Do NOT just consider the guard at the entrance being your security staff. **EVERYONE of your staff should be part of your security system**!
Even in today's digital world, espionage happens not only via computer and internet. There are MANY more methods available. You and your staff should know them all and know how to counteract. **Both the methods of obtaining data and the protection of your data should be on your list of priorities**.

Of course, as always in business, cost reduction is a main concern, and this is only natural to any business. It is thus very important to conduct all the areas of corporate intelligence in a cost effective way.
The extreme risk of NOT dealing with the subject, and NOT using corporate intelligence to your advantage and protection, must not be overlooked in this equation. One should NOT ignore the possible risks and the damages caused by successful espionage. Whole businesses are being destroyed each year, hundreds and thousands of jobs lost forever, stockholder values diminished in almost frightening amounts.
Also, **one should weigh the BENEFITS of the use of corporate intelligence against the costs of it**. Surprisingly to many business owners, the mid- or long-term **benefits are much higher than the costs**!

We KNOW that the whole area of corporate intelligence is somewhat dubious to most business owners and managers. Why? Because espionage is an abstract threat.
Successful espionage is not being discovered. Only unprofessional activities are being discovered. Thus, if in YOUR business there are professionals spying on you, you will not notice, or only when it's too late.
Espionage against or within your own business is like a cancer. If you have no prophylactic measures in place, it will be discovered only when it's possibly too late to remedy.

Again: if your business has any kind of meaning in your branch of industry or if you possess knowledge or if your products are of high or superior quality, you may very well be almost 100%

certain that your business is the target of corporate intelligence, of espionage. This applies to your staff as well. Key staff will be enticed to leave your company to work for competitors; should that occur, they will take their knowledge and their share of your company secrets with them and USE them against you. **Key staff will ALWAYS be targeted by espionage, in in MOST cases without even being aware of it**.
As a business owner or manager, you should be CERTAIN if and possibly how your company is being targeted and how to protect your company and your staff.
To stay in the picture of a cancerous disease: **an annual check-up should be put in place, precaution should be the a top priority**.
Those are the only ways for early-detection and for averting losses, risks and damages. **In the long run, this will lower your costs and heighten your security**.

Let's get back to the use of corporate intelligence for your own company.
This is a quite delicate and very confidential subject. The use of concealed measures to obtain all useful and important data is a gray area at times. There are business owners who feel it being "immoral" to use all available methods. From the point of view of the above mentioned Sun Tzu, that would be a mistake. ***"Know your enemy, know yourself"***, in his strategy, is always TOP priority – he means this: do NOT act, UNTIL you have ALL the pertinent info.
According to his maxim, to NOT use corporate intelligence to the full extend would be failure.

There frequently also is a misconception about the use of intelligence measures. **Obtaining EVERY available information concerning your business should not be a question; it's just a chore on the to-do list**.
It is, however, **the responsible USE of such data** where possibly moral questions come into play. In real, daily life, here's an example: I am in my garden, trimming the roses, I overhear a conversation of my neighbors about some compromising fact or other. The RIGHT moral thing would be to walk away and to NOT eavesdrop, maybe. But maybe I find this conversation intriguing, so I listen in. Is this immoral? I don't know, possibly; but it's human and it's not illegal, plus given the fact that the neighbor isn't careful enough to not talk about it where others can listen in. Now, if I were to GOSSIP this info or use it to slander my neighbors name, THAT would be immoral and possibly illegal.

So: **obtaining data and information as such is not necessarily immoral. Using it in a criminal or illegal way would be**. YOU NEED all pertinent data about ANYONE who is in contact with your business. But you are NOT forced to use it in an immoral way; however, **you can use the data in order to PROTECT your business which would NOT be immoral. It is your duty**.

Ethics and questions regarding morality are much more anchored in the **USE of information**. It is a simple fact of life that there will ALWAYS be the one competitor or perpetrator who will not operate according to ethics and moral thinking. Every business must and should be prepared for that situation. **Governments ask of businesses to act ethical, but the governments themselves do not, nor will they ever refrain from the use of intelligence services. They simply CAN'T**.

The other fact is: **there are a plethora of governments, who live according to this principle: why pay for research and science, if we can STEAL corporate secrets**? Having dealings with certain countries will raise the risk of espionage against your company immensely.
Yes, ethics are important, no question about it. But ethics should not cross the line to being naive, for that would endanger companies and countries.
Thus, it is important to HAVE ACCESS to all and any information needed; it is a question of ethics and also of laws and regulations to properly USE such information.

Not every business owner can afford to run his or her own intelligence department, and not every business owner has the right training, knowledge, skill and TIME to do it properly him/herself.
Many companies are using security services or even employ their own security staff. However, **in order to truly and effectively protect your business, you should NOT use the regular security staff in order to check on your internal security**.
Be aware that both intelligence services and criminal organizations, and even TERROR GROUPS, run security companies and cleaning services as a front in order to infiltrate companies!

The use of security guards and cleaning personnel is one of the most often used ways to infiltrate companies. Why? Each companies uses these services, thus infiltration is easy; these workers can spy on you very easily and at the same time make money off of you.
They will monitor the comings and goings of your staff and clients, they know who your suppliers are, they rummage through your desks and waste bins, they can even very simply get access to restricted areas without raising suspicion, and obtain a wealth of data; they can place surveillance devices almost anywhere in your business, and all that while being on YOUR payroll.

Also, **do not forget that by lowering costs** (and security and cleaning staff ARE the lowest paid in your company probably) **you do possibly indirectly tempt these workers to steal information or become susceptible to recruitment by intelligence services and criminal gangs for a little easy earner on the side**. Cometh the hour,cometh the thief
You should be aware of this, as it would be a grave mistake to ignore this real-life fact. There are information brokers out there, intelligence services, criminal gangs, terrorists. They all are looking for easy targets to obtain your company data, and they usually FIND such targets within a day among the security guards and cleaning staff. We know that first hand...
And many of your competitors do NOT have the scruples that you have.

So, due diligence demands that your staff be vetted thoroughly, included all staff from outside companies that service your company. **Obviously, this vetting process cannot be done by your own security staff, be that in-house or external**.
By the same token, it is much safer AND more cost effective to use external professionals for your own needs of corporate intelligence, for instance certain legal considerations in regards to privacy regulations and others. Also, your company should not store certain sensitive data in-house, for the same reasons.
Finally, the training of your staff or candidates for employment can go along with the background vetting process – this is cost reducing and more effective and avoids certain privacy matters, and is thus all in all a much better way to proceed.

And that's where COBRA SYSTEMS LLC comes into play. With individual professional experience of between 25 to 30 years, our senior counselors and staff are experts in the fields of intelligence, counter-intelligence, obtaining information, counter-espionage, undercover operations worldwide, and the pertinent training of staff and security personnel.
Our own specialized network includes high ranking contacts to security organizations in all important countries. We are one of the very few institutes to offer extensive private intelligence and undercover training, including subjects such as infiltration, exfiltration, high risk operations and many more.
We are successful information brokers and are intimately familiar with the market.
We can provide the information you need and at the same time ensure the safety of your company and key staff.

If you have any need of private intelligence services or counsel in such matters, as a private person or business, Cobra Systems LLC can provide you with professional services worldwide.
Obtaining or protecting data, matters of corporate espionage, background vetting of staff, clients or associates, training of your staff as regards counter-intelligence, as well as internal security services and penetration tests, and any related service are what we can offer to you.
We guarantee you absolute confidentiality and are at your disposal.

Knowledge is power. Thus, obtaining such knowledge and protecting your own data is of paramount importance.
We are the right partner for you in these important matters; **if** you have any needs in this regard, we should make an appointment shortly**.**
Corporate intelligence is and should be discussed on the highest management level and on a need-to-know basis, thus, it should not be delegated or only to the necessary degree**.**
Contact us any time to make an appointment.
Best wishes from
Yossie Blumberg
Cobra Systems LLC

Overview Services

We offer you all services needed in the area of private intelligence services, such as

- **Obtaining data and information**
  - procurement of all pertinent data and information
  - intelligence operations
  - infiltration by short- or long-term informants
- **Counter-Intelligence**
  - all measures of counter-espionage
  - use of intelligence methods e.g. to defeat product piracy
- **Security and Protection**
  - background checks (vetting) of staff, candidates, suppliers, associates, new investors
  - penetration tests – security checks, identifying possible security problems, leaks, threats, conduct loyalty tests, test the reaction of your key staff as regards counter-espionage techniques
  - Assessment if your company data is already being dealt on the “information market” and if so by whom and to which extend
- **Training**
  - Training of staff in general – turn your staff into your extended “security system”
  - Training of key staff – awareness and professional counter-espionage, counter-surveillance, early-detection and more
  - Professional counter-intelligence training
  - Emergency action plans in the case of any attack by means of espionage methods
  - Training of security operators in the areas of intelligence, counter-intelligence, undercover operations