



[www.compusafe.co.za](http://www.compusafe.co.za) / [info@compusafe.co.za](mailto:info@compusafe.co.za)

## INDUSTRIAL ESPIONAGE

"Who says industrial espionage is a relatively new thing? Man has always recognised technology as a means to gain power over another, so they guarded their secret carefully. Alchemists of the medieval period all had their secret notebooks full of coded lists, ingredients and amounts that pointed towards the synthesis of gold." In our modern world industrial espionage is rampant and methods include making use of casual employees working as undercover agents, hackers, hired teams of burglars, trash-picking, exploration of dumpsters, bugging, etc.

### Definition

Industrial Espionage is the discreet gathering of intellectual and sensitive data in an unethical and/or unlawful manner in order for the gatherer of such information or someone else to get the edge in the market place in unlawful competition.

Some South African companies are unaware of industrial espionage practices. In South Africa there is no law prohibiting industrial espionage per se. However acts of espionage could be accommodated under theft, trespassing, etc.

The underlying philosophy of industrial espionage is, why spend years and millions of rands on research and development and developing a customer base when you can bribe an employee in the competitor's camp for a few rands, tap their telephones, or bug their offices, etc.

According to the American Society for Industrial Security (ASIS), occurrences of industrial espionage in American business have grown by more than 260 percent since 1985 which could amount to as much as \$63 Billion per year. The FBI estimates that espionage costs corporate America more than \$50 Billion per year.

Industrial Espionage in South Africa is regarded as an acceptable way of doing business, with no danger of legislation to deter it. In South Africa it has been attempted to use various criminal statutes to counter espionage when the perpetrator is caught, but as said these laws do not specifically cover the theft or improper gathering of proprietary information.

Clearly, in today's business arena, information is more valuable than ever. Every organisation is vulnerable to information theft. Companies can not simply sit back, whilst a fortress mentality of hiding behind fences, locks, alarms, access controls and guards is also not the answer. The enemy most often is already inside the fortress as about 85% of espionage crimes are perpetrated by employees. Your security may be great to keep the outsiders out, but does nothing to prevent

insiders exporting company secrets.

In this regard companies must change the way they think "security". They must identify their valuable information resources and who might be interested in them.

They must decide where defenses are needed and where to find the right people who can provide them. OF&A encourage companies to conduct background checks before bringing in the team of supposedly qualified software professionals. Besides having immediate access to the arsenal of company information, unscrupulous programmers can be bribed to plant a Trojan horse in the corporate computer system, and in doing so build a 'backdoor' offering them repeated access to company data. The laptop of a high ranking executive on the road is also loaded with the company's latest and most vital activities and plans, and is often left in the hotel room during lunch or dinner. It is the easiest thing to access a room, boot up the laptop, copy the data on the hard drive whilst a partner armed with a cell phone keeps the executive under close surveillance while the other leaves the premises without anyone being any the wiser.

Even sitting aboard an airliner may not be safe. It is alleged that the French have been accused of bugging seats in the first class section of their airliners. The same for French hotel rooms frequented by executives.

Legislation is, however, not always the answer because should a company catch the spy and resort to civil or criminal prosecution, the nature of the confidential information stolen, is commonly made public during the trial which is an ironic consequence of legal rules that in order to obtain justice, the victim will have to make public the very same information it is trying to protect, making the value of the confidential information far less. The secret therefore is to protect confidential information in such a manner that the spy can not get it in the first instance!