PROTECTION OF INTELLECTUAL PROPERTY AND TRADE SECRETS

- Article & Interview by De Wet Potgieter

In this day and age the *protection of information* should be the foremost priority of any Corporate Company to prevent the theft of its most valuable asset - its *Intellectual Property*.

The danger of Espionage is an Alarming Reality, and as *South Africa* is regarded as one of the five most targeted countries in the world, the protection of information should be *at the top of the agenda in security planning*.

Gone are the days when people thought of espionage as the work of State Intelligence Agencies like the CIA, British MI6, the KGB or the Chinese ministry of state security. They were the experts specialising in espionage, analysis and covert operations, but the invisible face of espionage has changed significantly.

As the field of Intelligence has changed dramatically and as Technology has advanced it has become significantly privatised. *Private Intelligence emerged as an important part of the new world Intelligence Order*, but at the same time, the *threats of Intellectual Property theft* also increased at an *alarming rate*.

But strangely enough, despite this shift change in the murky world of spies, many companies are still in denial about this new sophisticated threat to their businesses.

Corporate Managers should realise that the *risk of Espionage is real and evident in all organisations*. In most cases incidents of espionage, when exposed by counter-espionage measures, remains a secret because companies regard such security breaches as reputational damage that should be kept under the wraps.

Few South African Companies really grasp the enormity of the problem and fail to take *provisional precautionary steps* with *pre-emptive action* to safeguard their Businesses. Hostile intrusions by Industrial Spies equipped with high-tech surveillance equipment for the job, has become a common phenomena in the South African corporate environment.

In most cases Companies *act after the fact* and retrospective damage control is in fact a losing battle trying to repair the losses incurred.

A good example of the huge damages a company could suffer if they do not have *pre-emptive measures* in place is the classic case of the sad demise of the once powerful British motor manufacturing industry.

A Chinese woman was paid 1,7- million British pounds as a consultant to MG Rover, but at the same time she was having an affair with one of its directors. It later turned out that the woman's father was in fact a senior official at a Chinese motoring company who bought up MG Rover's assets for a song and a dance when it collapsed, and shipped this major British asset to China.

More than 6000 British workers lost their jobs and Britain lost a part of one of its most precious heritage- thanks to the ignorance of company directors in safeguarding their Intellectual Property.

It is almost impossible to calculate the damages when an organisation loses control with the destructive impact that espionage may cause to its effective operations. Apart from the fact that confidence is seriously jeopardised, such an incident may also *affect share value* and compromise Businesses' Client Security and Confidentiality resulting in its *losing its competitive edge*.

A *spokesperson* for ***Advanced Corporate Solutions (ACS)*** warned that the driving forces behind espionage are continuously upgrading their high-tech spying equipment using micro-electronic devices that have been developed to minute specifications making them virtually undetectable by visual search.

"It requires *professional counter-espionage experts* like ***ACS*** to find these devices," he added. "Whenever you have important information you want to protect, we are the right people to secure it for you."

This means that **ACS** *will stop any unauthorised monitoring* of its clients in the Corporate World and *protect important information* you have. "Espionage Techniques could be deployed by anyone who wants to find out what information you have ensuring they stay a step ahead of your business." *the **ACS** spokesperson explained.*

Information has become the currency of this modern Global Economy and while some companies are still ignorant about the trade secrets they have, they may not be aware of the theses valuable secrets until it's too late.

For spies always on the prowl for valuable information to peddle, it is an organisation's commercial strategy plans, or financial reports, or latest breakthrough in new developments that will earn him a few bucks enabling a competitor to gain that edge in the very competitive international market arena.

*Part of the comprehensive services offered by the team at **ACS** are the outlining of an operational plan for the best techniques, products and services to facilitate each client's unique needs in safeguarding its assets against industrial espionage.*

ACS *was established in 1995* and has, as a *global player* in Corporate Intelligence and Countermeasures, been involved in investigations with clients ranging from business to industry and government agencies.

"The overall objective of Corporate Intelligence Management is to protect a company's day-to-day intangible assets".

Therefore ***ACS*** *is duty bound* by its mission and vision in life to protect its clients taking all possible pro-active measures that could be enforced to ensure and guarantee client safety and confidentiality.

Although many organisations have their *offices swept / debugged* for Eavesdropping Devices once or twice per year, ***ACS*** suggest that the sweeping of premises should be increased in times of a heightened risk like the period prior to pre-results announcements.

ACS *also recommends that Corporate EXCO'S arrange regular espionage awareness briefings for their employees- in particular senior managers and board members.*

"The threats of espionage and its affects should be an integral part of the risk management and business strategy of every organisation, ***ACS*** advises their clients".

Apart from the usual search for eavesdropping devices during the routine operations at clients' premises, ***ACS*** also recommends to have a permanent Counter-Surveillance plan in place.

This would ensure that additional problem areas would be identified where *information* may be lost through IT, Bluetooth, Unencrypted Systems and Broadcasting Equipment.

"What we strive for is to establish a clear change in the mindset of our clients on board level sensitising organisations to this ever growing threat to sound and clean management in the Corporate and Industrial environment," the spokesperson said.

He also stressed the point that directors of companies should be *personally liable for Corporate Governance issues* (The King III Report King Code of Governance Principals 2009 and King Report on Governance 2009) and that espionage takes an important space on any responsible board's agenda. For further information please visit: **www.acsolutions.co.za**

De Wet Potgieter is a free lance investigative journalist and the author of Contraband, South Africa and the International Trade in Ivory and Rhino Horn (1995), Total Onslaught (2007) and The Eleventh Hour (2013).