CGF
RESEARCH INSTITUTE
(PTY) LTD
Corporate Governance Framework

ARTICLE

CORPORATE ESPIONAGE: LETHAL BY INTENT
Johannesburg
27 June 2014

Article by Terrance M. Booysen

It may sound remnant of a bygone era in the movies; however corporate espionage in the workplace is alive and well and is estimated to be costing organisations a great deal of money. Recent reports suggest that the local economy may be losing up to R80 billion each year, and these losses are primarily being perpetrated by employees through fraud, theft and corporate espionage. Corporate espionage -- more commonly referred to as Industrial Espionage -- is a type of espionage that involves the secret collecting of confidential information and intellectual data from an organisation through various direct and or indirect means, and which is then used against the organisation. The considerable scale of corporate espionage is not only apparent in South Africa, but exists in international markets as well.

The effect of corporate espionage on an organisation is clearly detrimental, and most often it leads to substantial monetary losses, including competitive disadvantages in the marketplace. There are various spying tactics that perpetrators use to conduct corporate espionage. Some of the most common tactics include covertly extracting sensitive information from employees of an organisation through to intercepting telephone calls and e-mails; these being some of the more basic examples. Expectedly, corporate espionage has many other negative effects for an organisation. Once confidential proprietary information of a particular organisation has been handed over by an employee of the organisation to its competitor, it is easy for the other organisation to erode that organisation's competitive advantage, credibility, profit margins and so on. Perpetrators within an organisation will typically gather data and information which has commercial value and usually this relates to their organisation's trade secrets, product formulae, business and trade negotiation strategies, client lists, product development plans and supplier agreements.

Unlike the type of legislation found in the United States, namely the *Economic Espionage Act of 1996* and their more recent *Foreign and Economic Espionage Penalty Enhancement Act of 2012* which strictly prohibits any form of corporate espionage in the government and private sectors; notably South Africa has no specific legislation that deals with corporate espionage. At this point in time, the cold comfort South African organisations are provided against unscrupulous employees acting as internal spies for other organisations may arguably be found in Section 14 of the Constitution of the Republic of South Africa (1996). It states that; "Everyone has the right to privacy, which includes the right *not to have* –

(a) their person or home searched;
(b) their property searched;
(c) their possessions seized; or
(d) the privacy of their communications infringed."

In other words, by following the Constitution's very broad provisions, it means employees may not tap phones, make use of discreet cameras and or any other instruments that violates the privacy of the employer, amongst other. Clearly these provisions will not deter the perpetrator and unfortunately, even legislation such as the legendary Protection of Personal Information Act (2013) (POPI), the Electronic Communications and Transactions Act (2002) ('ECTA') and the Regulation of Interception of Communication and Provision of Communication-Related Information Act (2002) offers no real deterrent to eager employees who may have criminal tendencies.

That being said, it is interesting to note that whilst the ECTA is a highly regarded piece of legislation internationally (in respect of dealing with information security), studies reveal that not all its provisions are implemented by both the government and information security practitioners in corporate South Africa. Whilst the ECTA advocates the appointment of cyber inspectors who have powers to inspect, search and seize through a court order, in reality, little has actually been done to give this legislation the teeth to prevent employees who infiltrate the organisation's databases for valuable information.

To emphasize the extent of this 'rogue' employee problem; a local company that specialises in employee background tests (GriffithsReid) reported earlier this year that about 16% (sixteen percent) of all South African job applicants have criminal records and about 25% (twenty five percent) of all job applicants in South Africa contain claims to qualifications which are fraudulent. Clearly if these reports are anything to go by, organisations should be very concerned about the manner in which their information is being protected against these potentially unscrupulous employees.

"Clearly, in today's business arena, information is more valuable than ever. Every organisation is vulnerable to information theft. Companies cannot 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."

Website: www.ofa.co.za

In the past, corporate espionage was restricted by the fact that an individual could only access a limited amount of organisational information, or smuggle out a limited amount of prototypes and equipment. These were lengthy processes that required months of preparation work. With the recent boom in informational and technological advancements, the susceptibility to theft of confidential information and other forms of intellectual property is far easier and much greater. Today, hackers have the potential to access a large amount of company information almost instantaneously.

Numerous products, tools and devices are used for corporate espionage and these are becoming more widely available. For example, various products are available that allow an individual to record meetings, listen to private conversations, track a courier and see the contents of an envelope without even having to open it. Basically, any person -- no matter their age or location -- has the means to attack and or spy on any organisation so long as they have the tools to do so. Essentially, the perpetrator requires a personal computer, access to the internet and some technical savvy. Some popular tools used by perpetrators of corporate espionage include:

- CDs, DVDs and USB drives are common tools for transferring data into and out of a particular system;
- parabolic dish microphones are available to sieve unwanted background noise in order to hear a conversation or a meeting in another room;
- ordinary-looking pens and watches with integrated flash memory capable of 8-9 hours of covert digital voice recording;
- "tracksticks" are used for transmitting real-time GPS movement of vehicles;
- X-ray envelope sprays can be used to turn opaque paper translucent for 30 seconds allowing an individual the ability to view the contents of an envelope without opening it; and
- 'key loggers' are tools used to capture and email the keystrokes of a computer to another's email address.

In South Africa, corporate espionage is wrongly viewed by many organisations as an 'acceptable way of conducting business' and many South African organisations do not see the need to have adequate frameworks in place to protect their business from this scourge. Corporate espionage can be reduced and eradicated by organisations, by significantly improving their security strategies and implementing effective

business mechanisms to reduce the associated exposure and risk. Entry-level security measures such as document shredding and physical security of key company information should be added to virtual security protocols to achieve a robust and effective security system for organisations. Of course, even more basic preventative measures such as screening prospective and existing employees with proper background checks could also be applied. To this end, organisations may well also perform exit interviews with 'honesty testing' of their outgoing employees and consultants to determine the real reasons for their departure.

ENDS

Words: 1163

This article was reviewed by Hogan Lovells for its accuracy only. Hogan Lovells have not furnished advice as regards the content of this article.

More information regarding CGF can be found at www.cgf.co.za
More information regarding Hogan Lovells can be found at www.hoganlovells.com

For further information contact:

CGF Research Institute (Pty) Ltd
Terry Booysen (Chief Executive Officer)
Tel: 011 476 8264
Cell: 082 373 2249
E-mail: tbooysen@cgf.co.za

Hogan Lovells Attorneys
Ayanda Nondwana (Senior Associate)
Tel: 011 286 6900
E-mail: ayanda.nondwana@hoganlovells.com