INDUSTRIAL ESPIONAGE THREAT IN CORPORATE SOUTH AFRICA

Rabelani Dagada

University of the Witwatersrand, Johannesburg

Private Bag 3, Wits, 2050, South Africa

Rabelani.dagada@wits.ac.za

Seth Mukwevho

University of the Witwatersrand, Johannesburg

Private Bag 3, Wits, 2050, South Africa

smukwevho@gmail.com

ABSTRACT

The widespread presence of industrial espionage in South Africa could be an indicator that domestic corporate security frameworks have so far failed to neutralize the threat. It is nevertheless unfortunate that South Africa's firms do not have adequate security frameworks in place to protect themselves from industrial espionage. It is therefore, the aim of this study to understand the manifestation of industrial espionage and recommend security measures that firms in the country can adopt to fight against the threat. The data was collected using qualitative methods and was analysed using a thematic approach. Analysis of the study shows that industrial espionage is one of the major risks of business operations. Business rivals apply a number of instruments including human and technical sources. The human and technical sources of intelligence are believed to be the most preferred means of perpetuating this criminal activity.

KEYWORDS:

Security, industrial espionage, Information communication technologies, South African firms, techint, humint.

1. INTRODUCTION

Industrial espionage is the least-known concept within the intelligence compendium although many agencies are now involved in this activity. France, the United States, China and Israel now have intelligence units responsible for collecting and co-ordinating industrial intelligence [1]. Private businesses such as Jacobs Barnard Mellet [2], F1 racing team Vodafone McLaren Mercedes-Benz [3]

and the South African Reserve Bank (Financial Mail, 2001) have been mentioned in cases involving illegal theft of commercial information. This attests to the fact that in modern societies, as was the case in earlier centuries, economic intelligence is an integral aspect of business, albeit as a business risk. This study is intended to analyse industrial espionage and propose a security framework for South African business to secure their interests.

According to Chama [4] industrial espionage in South Africa is on the rise. A variety of covert and overt instruments exist to enable competitors to acquire business information to increase their competitive advantage; it is argued that South Africa's businesses do not have adequate security frameworks in place to protect themselves [5]. Industrial espionage easily succeeds with the aid of information communication technologies and when there are no proper security measures to prevent the stealing of business information. The widespread presence of industrial espionage in South Africa could be an indicator that domestic corporate security frameworks have so far failed to neutralize the industrial espionage threat.

In view of this reality, it is the objective of this study to understand the manifestation of industrial espionage and recommend security measures that firms in the country can adopt to fight against the threat. That is, the attempt to improve the understanding of modern corporate security perspectives in South Africa. The study tries to answer the questions:

- What are the manifestations of industrial espionage?
- How can South Africa improve business security protocols?

A qualitative research approach was employed whereby interviews were used to collect data to assist in the answering of the questions. The data was analysed using a thematic approach. Analysis of the study shows that industrial espionage is one of the major risks of business operations. Business rivals apply a number of instruments including human and technical sources. The human and technical sources of intelligence are believed to be the most preferred means of perpetuating this criminal activity.

2. INDUSTRIAL ESPIONAGE

Intelligence refers to information that has been collected and analysed about a target [6]. This information is assembled through overt and covert methods, including collection from grey sources, which are diplomatic and overt government documents. Industrial espionage entails purposeful gathering of information of economic and business value related to trade secrets, product formulae, concealed business strategies, trade negotiation strategies, business plans and product development of industry competitors [7]. Industrial espionage is not restricted to collection from open sources; the gathering of concealed strategic business secrets is also highly prized. This activity is nonetheless, carried out by both private entities and government agencies.

Industrial espionage presents a serious business risk. It is estimated by Ernst and Young (South Africa) that industrial espionage is a $67 billion a year industry [8]. This figure indicates that illicit industrial espionage is a substantial business. South African-specific accounts of industrial espionage are mostly contained in business publications. An assessment of reported cases indicates that the nature of industrial espionage is predominately an inter-organizations activity where rivals steal information from each other using private agencies. For example, in 2003 *The*

Star reported that British American Tobacco South Africa (BATSA) conducted spying activities on its rival, Apollo Tobacco; and Finsettle, a subsidiary of Barnard Jacobs Mellet, stole business information secrets of CST Outsourcing [9]. The considerable scale of industrial espionage is not only apparent in South Africa, but exists in international markets as well. For example, a report to the United States Congress in 2004 on Foreign Economic Collection and Industrial Espionage estimated that theft of business information cost the American economy between $100 and $250 billion annually[10]. The total international market for industrial espionage is not known because many victims choose not to disclose when they have incurred a loss. Be that as it may, the conclusion is that industrial espionage is a huge economic activity involving both state and private business entities.

Global integration and advancement of information communication technology is fuelling the exponential growth of industrial espionage. Previously disparate societies have integrated through globalisation and the network knowledge economy. The combination of globalisation and information communication technology has led to a huge surge in industrial information crime. From its humble beginnings 40 years ago, Internet technology has developed exponentially. Its ability to link people, organisations and enterprises is the major advantage for the commission of industrial espionage. This connectivity enables hackers and other criminals to carry out their operations with ease. The same technology allows for stolen information to be easily concealed from *de jure* authorities and illegally transmitted to clients. The conclusion is that the rise of information communication technologies (ICT) in a globalised environment has seen a concomitant rise in the rate and spread of industrial espionage [11].

Ineffective counter-industrial measures are also responsible for the growth of industrial espionage [12]. Most business enterprises do not seem to be conscious of the importance of having high quality security measures in place. Many corporate entities continue to use old and outdated security management infrastructure that prioritises physical security whilst oblivious of the need to protect information in accordance with modern techniques. Physical security-based approaches to security are often rudimentary and inadequate. Competent anti-espionage security systems should, amongst others, target ICT infrastructure, ICT end-user security awareness, and electronic recording and information transmission devices [13].

3. RESEARCH DESIGN

A qualitative research approach was employed whereby semi-structured interviews were used to collect data to assist in the answering of the questions above. Eleven purposively selected participants representing a broad spectrum of experiences were interviewed. Those who are very knowledgeable about the phenomenon under scrutiny in this paper were contacted to participate in the study. To protect the participants in the study, no names or the firms with which the respondents are affiliated are mentioned in this paper.

The study opted for face-to-face interviews owing to the sensitive nature of the subject of the research exercise [14]. Information related to espionage should always be communicated on secure platforms. This means that emails and telephone interviews could not be acceptable as they are often relayed on non-secure electronic

infrastructure. Secondary data was also used in the process. The data was analysed using a thematic approach. Engaging various sources of information for triangulation has significant advantages. Byrne [15] observes that the usage of multiple sources of information increases the credibility and reliability of research findings.

4. FINDINGS AND DISCUSSIONS

From the analysis of the primary and secondary data collected about industrial espionage in South Africa, the following themes became evident:

i. Employment of multi-layer security measures
ii. Employing the principle of 'need to know'
iii. Securing email communication
iv. Securing mobile devices' data
v. Employing quality and skilled human resources

4.1 **E**mployment **o**f **m**ulti-layer **s**ecurity **m**easures

According to one respondent who works for a technology consulting company focusing on website auditing, organisational technology concerns and leveraging technology in business, 100 per cent security may not possible to attain, nevertheless, using a combination of measures can improve business security significantly. The respondent introduced the word 'multi-layer security' in this study. The question is: given South Africa's industrial espionage record what should its multi-layer security strategy be composed of? Other respondents are of the opinion that it should be composed of education. This point is informed by the belief that "employees for us are the biggest danger", hence "the only way that we have been able to minimise that risk is by training." The training module is very global, and touches every aspect of security. For example, he points out that his company encourages executives to shred all documents as a security measure. Unfortunately, people do not value the benefits of these shredders. There are three areas identified that training should be focused on, namely physical security, the technical aspects and social engineering. Accompanying education is the testing of employees to assess whether they are internalising security lessons. The intention of training is to build awareness of business security and ensure that security is deeply entrenched in the human resources component of the business organisation.

4.2 **E**mploying **t**he **p**rinciple **o**f **'n**eed **t**o **k**now**'**

According to the respondents such training mentioned above should inculcate the principle of 'need to know', related to computer/technical security. Access to electronic and non-electronic communication systems should be extended to only those who need to know them and who will use them. Advancing the theme of 'need to know', which is actually grounded in compartmentalisation, information communication technology applications such as email should be encrypted and should have high strength passwords. Encryption should be applied to crucial company strategy documents as well. The theme that is emerging is that education makes employees more alert to security issues and the equipment they use should conform to that level of security.

4.3 **S**ecuring **e**mail **c**ommunication

Emails are the major source of malware in any computer system. Business information is also communicated to espionage agents through this medium. In some instances

people store crucial business information on emails, sometimes using web-based email service such as Yahoo, Webmail and Gmail (Google). This is a major risk to the integrity of business knowledge management, and encourages industrial espionage. According to an expert, one of the solutions is to ban outgoing email systems completely. Accordingly, officials of the organization do not send emails out and in turn they do not receive information from external emails. Such an organisation only has an internal email system (at times hosted by an intranet). He asserts that "the Post Office is actually a good example; you cannot get anything (email) from them, and you cannot email them anything." What he refers to is a secure information communication system. To enhance security, secure and insecure information communication systems should never interface. One of the ways of advancing secure information is to proscribe conventional emails. Literature review showed that interface compromises communication lines, hence the existence of US-CERT. It is recognised that a lack of outgoing email can retard business, especially when dealing with business constituencies not used to this culture. However, the huge cost of industrial espionage in certain industries such as aerospace, military hardware development, and security software supplant any possible inconvenience brought about by lack of emails. The central theme the study is embracing is that security should be central to business operations, even if security strategies may be unusual and unfamiliar in the current ICT world.

4.4 **S**ecuring **m**obile **d**evices' **d**ata

Business information is also easily stolen from hand-held, mobile devices such as laptops and cell phones. Business leaders use these instruments to communicate and for some, to store information. However, business information peddlers easily steal information from these devices, especially when they are linked to a cordless source of data such as wi-fi. In South Africa most techint takes place in this manner. From the data analysis, it was noted that a security strategy appropriate for this type of electronic attack is what is known as an 'air defence product'. Respondents recommend the 'information wiper system', produced by Research In Motion (manufacturers of Blackberry). Information wiper is an automated information erasing system activated when a Blackberry is lost. The 'air defence product' does two things. Firstly, it serves as an electronic sensor instrument around organisations and reports to the server all illegal intrusion. Secondly, it provides detailed intelligence to the server administrator of all the activities of the malicious hacker. Therefore, the air defence system provides early warning reports whenever techint intrusion takes place. The main emphasis is that business security systems should contain an effective early warning capability, as in traditional intelligence organisations. One respondent argued like:

> *So the ideal security system is one that is fairly monolithic in its overall structure, and will have as many overlapping layers of security, and is structured in a way that informs when a (security) breach comes about, because often no security system can stop people from breaching it.*

4.5 **E**mploying **q**uality **a**nd **s**killed **h**uman **r**esources

Early warning calls for immediate response. Thus calls for quality human resources to deal with techint methods of industrial

espionage. Analysis shows that South Africa should invest in quality computer security personnel in three areas, namely prosecutors, police officers and the corporate sector, all of which are presently inadequate. Lack of capacity among police and prosecutors means that cases involving techint such as eavesdropping, bugging and industrial espionage are not being prosecuted efficiently. It is also observed that court cases involving techint are difficult to settle in South Africa: "*it is just that there is nobody in South Africa (the legal system, police and prosecutors) that deals with that*." Others are of the opinion that 'cyber cops' and laws to prosecute business crime offenders should be introduced as a matter of urgency.

The corporate sector also lacks advanced knowledge with regard to problems related to technical intelligence. Referring to the limited number of computer security experts in corporate South Africa, one respondent said:

...it is still difficult for us to find talent that we are looking for; we know Dominic White [computer security expert] because the community is so small.

The picture that emerges from consulting with various experts is that South Africa is extremely vulnerable in dealing with electronic methods of intelligence collection.

Unfortunately, information about security breaches reach businesses when much of the damage has been done. Furthermore, many chief financial officers are not educated in security and find it difficult to invest the huge financial resources needed to install effective multi-layer security systems. Most security managers still have a strong focus on physical security rather than the intrusive technical intelligence methods of espionage.

5. CONCLUSIONS

Industrial espionage is one of the major risks of business operations. Business rivals apply a number of instruments, and at times hire intelligence services to steal strategic business information. In the domestic environment, human and technical sources of intelligence are the most preferred means of perpetuating this criminal activity. The application of human and technical intelligence has attracted academic debates. Insofar as humint is concerned, the debate centres on the most ideal human sources of information. The dominant school believes that human sources are indispensable in intelligence collection. There should not be discrimination as to who should be recruited; any human source with access to information should be recruited regardless of moral standing. On the other hand, there is a view that only those of high moral standing should be recruited for espionage operations.

Nonetheless, the ideal human intelligence source is the one with direct access to information regardless of moral competence. In the technical intelligence arena there is an over-reliance on technical intelligence which can be misleading for several reasons. Technical intelligence is unreliable, is easily undermined by quality of recording instruments and the technological competence of the user. The conclusion is that technical intelligence should be used as a back-up to human intelligence.

In spite of some criticism, human intelligence and technical intelligence methods are very popular in industrial espionage. The combination of the two methodologies of espionage is promoting

the entrenchment of business spying in South Africa. Many people believe industrial espionage can be significantly frustrated by improving security, especially by concentrating on security screening of human resources in an organization. However, a number of people interviewed have strongly recommended virtual security strategies as an effective mechanism for addressing business information crimes. Strategies like air defence products, information wiper software, computer security firewalls, amongst others, are recommended as effective security tools. Again, the importance of security consciousness, education in computer security for the judicial and police communities, implementation of legislation and creation of a law that prosecutes industrial espionage as crucial to stemming the tide of industrial espionage in South Africa is emphasised. Their contributions overwhelmingly indicate that the upgrading of virtual security to meet 'new economy' security needs is integral to defeating domestic business espionage. Entry-level security measures such as physical security and shredding are also very important, but should be applied together with virtual security protocols to attain a robust, effective, and responsive multi-layer security system for corporate South Africa.

REFERENCES

1. Jones A. 2008. Industrial Espionage in a Hi-tech World, Elsevier Ltd http://www.sciencedirect.com/science 25/11/2009

2. Gilmour C, 2005. BJM Company Sued, Financial Mail, Johannesburg

3. Parsons, A. 2007. "F1 'Spygate' Q&A", BBC Sport http://news.bbc.co.uk/sport2/hi/motorsport/formula_one/6992011.stm 25/11/2009

4. Chama K. 2006. "Take Cyber Crime Seriously – Says E&Y http://www.compustaff.co.za/news.asp 30/04/2008

5. Chama K. 2006. "Take Cyber Crime Seriously – Says E&Y http://www.compustaff.co.za/news.asp 30/04/2008

6. Platt, W. 1957. *Strategic Intelligence Production*. Frederick A Praeger Publishers, New York

7. Crane A. 2003. *In The Company of Spies: The Ethics of Industrial Espionage*. International Centre for Corporate Social Responsibility

8. Chama K. 2006. "Take Cyber Crime Seriously – Says E&Y http://www.compustaff.co.za/news.asp 30/04/2008

9. Gilmour C, 2005. BJM Company Sued, Financial Mail, Johannesburg

10. TSCM. 2009. *What is TSCM?* http://www.tscm.co.za/whatistscm.html

11. Nasheri H. 2005. *Economic Espionage and Industrial Spying*. Cambridge University Press, UK

12. Nasheri H. 2005. *Economic Espionage and Industrial Spying*. Cambridge University Press, UK

13. Nordquist M. 2002. *Towards improved security management practice*, Dissertation.com

14. O'Sullivan, E. & Rassel, GR. 1989. *Research Methods for Public Administrators*. Longman, New York

15. Byrne MM. 2001. *Evaluating the Findings of Qualitative Research*. AORN Journal http://findarticles.com/p/articles/mi_0FSL/is_3_73/ai_72272010/19/10/2009