Institut für Strategie- Politik- Sicherheits- und Wirtschaftsberatung, Berlin

# The Fight against Corruption, Industrial Espionage and Economic Crime

by Maxim Worcester

## Corruption

Current estimates place the cost of bribes paid to gain business advantage at US$ 1 trillion annually; the embezzlement of public funds or theft of public assets by corrupt officials is unquantifiable. The World Bank also estimates that tainted procurement amounts to US$ 1.5 trillion, with an unquantified volume of fraud in the private sector. The result of this development is a reduction of Foreign Direct Investment, reduced growth rates and a significant reduction of tax revenues with a consequent reduction in state spending on infrastructure and public services. The cost associated with corrupt practices is not only a financial cost – the reputational damage to companies which have been associated with corrupt practices, such as Siemens, continue to dominate the press.

The scale of global corruption shows no sign of abating. Companies readily engage in corrupt practices to maintain market position and share. Transparency International has highlighted that it is companies from emerging market economies such as Russia, China, India and Brazil that are more prone to pay bribes in return for contracts, with clear implications for Western companies where corruption controls are significantly higher and more effective. Some argue, incorrectly, that they can only compete against such companies by behaving in a similar manner.

International initiatives to combat corruption continue to struggle. Such initiatives include the UN Convention against Corruption, the OECD Convention on Combating Bribery and the US Foreign Corrupt Practices Act. Despite this, awareness levels remain low with many companies, including those in the OECD, unaware of the legislation or unwilling to implement measures to combat corruption. It can however be assumed that awareness will grow as the implications of non compliance with such initiatives become more apparent. Global media coverage has made companies increasingly sensitive of the needs to protect their reputations worldwide and has also lead to growing public awareness of the cost of non compliance. The key challenge for companies will be that they can no longer operate by one set of standards at home and by another abroad. However, companies will find it increasingly difficult to compete given that rivals from less well regulated and controlled jurisdictions will continue to play by different rules. As a consequence it can be expected that Western companies will revert to “name and shame” tactics in order to overturn commercial decisions which have been taken due to corrupt practices. Greater awareness of the economic costs of corruption and associated social costs will boost reform agendas at a national and international level. It will also mean that companies will have to invest increasingly in

programmes to fight corrupt practices within their own companies in order to avoid damaging their reputation and in order to be sought after as a reliable and clean business partner. Companies not adhering to compliance guidelines will in future no longer be asked to tender for contracts by an increasingly number of governments, international organisations and private companies.

Of all the measures the Foreign Corrupt Practices Act (FCPA), which governs all US-listed companies and their overseas subsidiaries, is currently the most actively enforced and implemented anti-corruption instrument. The emphasis is on US companies (and foreign companies listed in the US), but cases against foreign companies have increased, underlining the extraterritorial reach of the FCPA. Besides making it unlawful for any US-listed company to make or offer a payment to a foreign official to influence that official to assist in obtaining or retaining business, it also requires companies to maintain an adequate system of internal controls. The recent decision of the US government to impose a fine of $ 400 Million on the British arms giant BAE for knowingly and wilfully impeding the US authorities by making certain false, inaccurate and incomplete statements in relation to compliance with anti corruption standards, thus defrauding the US, is a milestone in the fight against corrupt practices and bribery of foreign officials in order to win contracts. BAE was also fined around $ 47 Million in the UK for withholding information in relation to a deal in Tanzania. As a result of these payments, and for having admitted to wrong doings, BAE is not to be disbarred from tendering for defence work in the US and UK, but the monetary and reputational cost was and remains significant.

European companies are slowly waking up to the fact that they still have a long way to go in building up internal controls to both prevent corrupt practices and satisfy regulators and Governments. The screening of future employees (pre-employment screening) is rudimentary at best in many companies and the “know your customer” approach adopted by Anglo-Saxon companies is considered by some to be an attack on the privacy laws. Pre employment screening is frowned upon as it is considered to be too intrusive. As corrupt practices are conducted by employees it makes sense to investigate the past of future employees in order to weed out those with a corrupt past or tendencies to turn a blind eye to illegal behaviour. Data protection laws will have to be looked at very carefully in the future in order to ensure that legislation does not aid the criminal.

The way forward is going to be very varied with many countries increasing their anti corruption efforts in order to attract foreign investors. Many others, however, will continue in a “business as usual” mode, not least because many emerging markets have benefited from high investment flows even where they are known to have high levels of corruption. Resource-rich African countries are reluctant to embrace anti corruption measures given that they are wooed by countries such as China which is known to turn a blind eye to corrupt practices, providing the resources continue to flow. Such practices do little to combat corrupt business practices.

## Economic and Industrial Espionage

Economic espionage has been around ever since nation states have existed and since there has been competition between nations and companies. The ancient Egyptians ran an intelligence service developed to gain information about their rivals, the Chinese attempted to protect the secret of porcelain, the method of production was, however, discovered by a French Jesuit and so reached Europe.

Today nations and companies spend a huge amount of money every year on trying to discover secrets their competitors attempt to protect. The overall economic cost of espionage cannot be calculated as the budgets for Intelligence Agencies who are the main practitioners of economic espionage, are a closely guarded secret. It is however known, that the Chinese Intelligence Services employ over one million people to both protect the country from within and unearth the secrets of others. The economic damage caused by the loss of information is also unquantifiable. The FBI estimates that economic espionage costs the US around 100 Billion $ per year, the German Ministry of the Interior estimates the damage to Germany at around 20 Billion EURO.

Industrial Espionage, unlike Economic espionage, is conducted by private companies. Aims and methods are similar; however government agencies have the advantage of being able to employ highly sophisticated technical means in order to gather information. Increasingly however, private organisations working for the private sector are using equipment and methods which only a few years ago would only have been used by intelligence agencies. The rapid increase in cyber attacks on companies is also due to the fact that unscrupulous "consultants" are now also using electronic means to gather confidential information, or are seeking to disrupt the systems of the competition in order to gain an advantage for their clients. Such cyber attacks on businesses can be expected to increase.

Companies are quite rightly investing significant sums of money in order to ensure that their EDP systems are as robust as possible in order to protect confidential information. The weakest link is however the employee and not the hard and soft ware. Security does not begin and end in the computer department, it is an issue which affects all departments within a company and is a top management issue. The firewalls and CCTV systems can be state of the art, if however an employee is willing to pass on confidential information or reveal passwords, the best wall can be broached with relative ease.

Shady consultants and foreign agents are well schooled in the art of social engineering. This process, which can take time, is designed to ensure that a target is sufficiently manipulated to reveal the secrets of a company. This can take the form of creating friendship, usually by providing a life style the victim could otherwise not afford. In the first instance information of little real value is asked for, gradually the stakes are raised until the informant is so deep into the role of informant that he cannot escape. At this point the real information the agent is seeing is requested, accompanied by the threat of revealing what has taken place should the information not be handed over. Most persons in such a position hand over the information.
The outcome for the informant is not very bright. If the person is a low level employee, recruited to get hold of one specific piece of information, they will be discarded. Only sources at a decision making position might be retained and further induced to reveal information.

Open Source Intelligence (OSINT) is frequently used both to gather information on companies but also on people who might be targeted as a source. There is a huge amount of information in the Web and in publications. This can be further refined by legal visits to companies, seminars, trade fairs and social gatherings. The latter has the advantage of combining both social engineering methods and the gathering of information. Whilst OSINT will not replace Human Intelligence (HUMINT), the rapid growth of freely available information and computer programmes which allow analysts to rapidly sift through gigabytes of electronic information has increased the vulnerability of companies. The willingness of people to provide private information on such sites as Facebook is alarming as it offers those who seek to target weak links in companies an easy way to identify likely candidates.

A recent penetration test in the US gives a good example of how OSINT and HUMINT methods can result in the loss of information. A High-Tec company asked a security consultant to test the defences the company had constructed to counter the loss of information. The consultants, using OSINT methods, managed to place a part time employee in the company using a false name and a fictitious background. By using social engineering skills this person was able to gain access to top secret information relating to the configuration of the fire wall and also to pass words. This information was passed on to external hackers who were able to gather sensitive information which, if it had been passed on to competitors, would have resulted in a loss to the company of around 1 Billion$. The company had built up a robust defence from attacks from outside; it had simply forgotten that the enemy can also come from within.

Given that many companies are networked and expect their senior management to be electronically reachable at all times, the dangers of loosing information are greater outside the office rather than within. The use of hand held devices or lap top computers when on a business trip represent a major threat to the security of data. Computers or other electronic devices left in bed rooms or in meeting rooms can be compromised and land line calls as well as calls on mobile phones intercepted. Such threats are barely recognised and many executives endanger their company by not sticking to simple precautions. One should simply assume that all information carried with one in electronic form can be accessed and should avoid if at all possible taking any such information on a business trip and leaving it unguarded. A further threat is blackmail – many a piece of hot information has come out of entering into a compromising position far from the marriage bed.

## Economic Crime

Some 45 % of all companies fall victim of some form of economic crime, according to international consultancy KPMG. Large companies report an average of 12 incidences per year; many incidences remain unreported as companies do not want the general public to be aware of the problem. Retailers, affected by numerous low value losses even factor the economic cost of theft into their pricing structure.

IP theft and counterfeiting also show no sign of abating. The global trade in illicit goods is increasing: the number of counterfeits has grown at eight times the speed of legitimate trade according to Interpol, resulting in global commercial losses in the region of 500 Billion $, equal to around 7 % of world trade and is largely built around the same global complex distribution chains associated with legitimate trade flows. Organised crime has built increasingly dense infrastructures to smuggle goods such as cigarettes, alcohol and drugs.

Such groups are becoming increasingly sophisticated through international links, the use of legitimate business structures and violence. They will become increasingly entrenched through growing influence (via corruption) and their associated level of social and economic infiltration and integration. In some countries, such as Angola or Russia, organised crime can account for up to half the national economy.

These networks conduct criminal activities varying in structure, length and complexity, but most groups will continue to possess a core membership around which there is a cluster of subordinates, specialists and transient members with a network of dispensable associates or low level criminals used to carry out logistical and criminally related tasks. Such groups use a risk based approach to activities by threatening violence in the case of betrayal and by transferring risks to lower level criminals or using specialists on a need only basis. As a result

of the latter, we now have highly specialised criminal service organisations offering quality services in the field of IT, finance, forgery or logistics. Such specialists offer criminal organisations the possibility of cyber attacks rather than old fashioned robbery and furthermore the possibility of using the Internet to launder the proceeds of their illegal activities. Economic crime has both gone global and increasingly electronic.

Many observers believe that the links between transnational organised crime and political violence will continue to grow. There have been or are numerous examples of armed groups resorting to smuggling to finance their violence: narcotics have been smuggled by the Kosovo Liberation Army, the Kurdish workers Party. The Islamic Movement of Uzbekistan the Taliban and the Irish Republican Army. Thus organised crime will increasingly corrupt and undermine effective governance from the local to the state level and in some cases replace the legal government. The list of countries considered to be failed states or failing states is growing in Africa but also in Latin America, Asia and the Middle East. The problem of this development is more dangerous than is generally understood. The human security implications of state failure include armed conflict, famine, disease outbreaks, mass migration and an acceptance of organised crime. Such an environment is hardly one companies would like to do business in, certainly not without taking robust measures to mitigate the associated risks involved.

## Conclusion and Recommendations

Whilst globalisation has acted as a facilitator of growth, it also serves to increase susceptibility to risk through interconnectedness between business, markets, people and nations. At the same time, the pace of change has increased dramatically, meaning that the consequences of a risk event may become wider and more immediately felt by companies than previously envisioned.

As threats manifest, they will have a widespread impact on business activities through the interplay of multiple factors. The loss of information to a competitor has an impact of the financial performance of a company and also is damaging to the reputation, which in turn can result in a declining share price. For the board of such a company the implications can be serious if it is shown that the company had not taken the necessary steps to protect the company from the loss of information. Thus the loss of information becomes a compliance issue with all the consequences for those responsible at board level. An incidence of corruption within a company can in the same way damage the company financially and have compliance consequences for the board if it can be proven that due care to avoid such incidences had not been taken. It can furthermore result in companies who have tolerated corrupt practices from being barred from tendering for contracts in certain countries or for international organisations. Siemens, for example, was not allowed to bid for a contract for a mass urban transportation system in San Diego following the recent investigation into corrupt practices in relation to bribe paying in return for contracts.

At the root of the problem is not an exogenous factor such as a pandemic or breakdown in infrastructure or even a natural disaster. Such risks are outside the control of companies and organisations can prepare for such an event in order to mitigate the impact on the company. The main risk is the employee who, for whatever reason, is induced to act in a manner which is criminal and thus damages both the reputation of the company and causes economic damage. The enemy might be outside the company but the way into the company requires inside help. Companies can protect themselves from exogenous threats such as electronic

monitoring, tapping of phone calls or from burglary by using technical means. Such measures, however, do not protect companies from being exploited by employees.

Senior executives or owners of companies are reluctant to believe that employees can be disloyal. In investigations of such cases one often hears that “we don’t have that kind of problem”. Alas, that is not the case and as in society any company also has its share of individuals prone to take rules and regulations lightly. Companies need to become aware of this and need to screen those in positions of responsibility closely prior to them joining the company. Such pre employment screening is commonplace in many Anglo Saxon companies, but in continental European countries screening is the exception rather than the rule. The monitoring of persons on a regular basis once they have joined the company is one fraught with problems in countries with high levels of personal data protection. However, controls need to be introduced in accordance with local laws in order to keep up the pressure on employees to perform to agreed guidelines. Such measures also include job rotation in the purchasing departments in order to prevent the creation of corrupt networks or the practice of two or more employees signing off on contracts. At the same time companies need to screen their business partners on a regular basis in order to prevent the company from doing business with corrupt partners.

Not all information can be protected, nor does it need to be. Companies therefore need to decide what information is confidential or secret and even top secret. Confidential information is normally the kind of information all employees can share. If such information is leaked to competitors the consequences are not usually damaging. A leak of confidential information can however result in later damages to the company as it could reveal avenues for a future attack. Examples of this are internal phone lists which could allow a hacker to impersonate an employee in the computer department and thus gain access to valuable data in internal databases. There need to be clear rules about the circulation and destruction of such information and these rules need to be enforced. Secret and top secret information needs to be protected by restricting access to those who really need to know and by the establishment of clear paper trails in order to easily identify possible leaks rapidly. Rules on copying such information and on encryption need to be established. Any hard copy of such information needs be held in a secure place and shredded rather than disposed in locked containers for shredding by external service providers. It should be remembered that the easiest way of gathering data is by examining the waste a company generates, it is known as “dumpster diving”.

Such measures will make it more difficult for competitors or even foreign intelligence agencies to gain access to company secrets. However the main weakness remains the employee who is willing to break and circumnavigate such rules. Besides ensuring that no clearly rotten apples are employed by screening candidates in advance and on a regular basis, the real key to fighting information loss and any criminal activity within a company is by laying down clear rules and communicating such rules. Employees need to understand why such rules are enforced and what the consequences are if these rules are broken. There has to be a clear zero tolerance policy for those breaking the rules which is enforced from the top down as rigorously as it is from bottom up. Many companies have such programmes, most of them are however not effective as they tend to be computer based multiple choice questionnaires which are seen as a necessary evil. In some cases employees are required to sign off on the rules governing information protection and other compliance issues, more often enough such declarations are signed without understanding why the rules have been drawn up. More effective are regular face to face workshops where senior management explain in detail the reasons behind such rules and the consequences of not living these rules. If this is done professionally and often enough then such measures, combined with other

security measures, will result in a high degree of protection from criminal behaviour in the company and a higher degree of business protection.

The risks companies face have increased significantly in the past years due to globalisation and the advent of the internet and networked systems. Risk levels are likely to increase and new risks will emerge in the future. At the same time national and international law is requiring companies to run their operations in a manner compliant with such laws. Increasingly, companies are being investigated for infringing and breaking such laws, with significant financial and reputational consequences.

The fight against corruption, industrial and economic espionage and other economic crime is as much a battle against those wishing to attack your company as it is a fight for the hearts and minds of the employees.

***

*Remarks:*

Opinions expressed in this contribution are those of the author.

*Maxim Worcester*

Since January 2010 Maxim Worcester is Senior Advisor at ISPSW. Before, he was Senior Manager for Advisory Forensic at KPMG International. In the past he was Managing Director of Control Risks Germany, and held senior positions at the Economist Intelligence Unit, the Frankfurter Allgemeine Zeitung and Deutsche Börse AG.