

COVER STORY

Cover Story - Corporate Espionage.

We have all heard the stories and seen the movies but how many of us really know anything about corporate espionage? In this issue's cover story, we go inside the cloak and dagger world of corporate spying with one of Australia's leading investigations and security consulting firms to find out who is at risk, why and how they are being targeted.



Corp



Tania Bateman

Corporate SPYING



*We have all heard the stories
and seen the movies but how many
of us really know anything about
corporate espionage?*

*In the issue's cover story, we go inside
the cloak and dagger world of corporate
spying with one of Australia's leading
investigations and security consulting firms
to find out who is at risk, why and how
they are being targeted.*

The term "industrial espionage" used to conjure up image of black and white photographs and "shady" individuals dressed in black, passing on secret information in plain brown envelopes. Old movies would often depict stereotypical figures walking the streets under the cover of darkness, hugging the walls like warehouse rats, waiting for the opportunity to gain entry surreptitiously into an office for the purpose of illegally gathering information for either personal gain, or in the corporate world, market share advantage. What many people do not realise is that these cloak and dagger images were largely founded in fact, and that the use of James Bond type equipment and clandestine meetings were just a part of the very real world of industrial espionage.

In the current era, the term "industrial espionage" has mutated into what is now known as "corporate espionage" which is practised globally - every day and in every type of business. Whether it be basic manufacturing of non-descript product consumables, or blue chip information technology, the competitive edge within the corporate world is far more important now than it was 40 years ago. Furthermore, with the huge advances in modern technology which have occurred over the last few decades, collecting information has become much easier. However, the risk of exposure if caught in the act can be detrimental to an organisation that has naively taken this chance.

Whether a company manufactures designer label clothing of fashion, produces CD's, or manufactures general foods, there will always be competitors who wish to gain an advantage by discovering what the business is producing in the way of a new developments and impending releases. Obtaining advanced notice of such developments will enable them, the competitor, to prepare a counter attack with a product of their own, therefore gaining a 'jump' on new market business. In the business world, information is power.

Other businesses may choose to engage in some form of corporate espionage to simply gain knowledge about their competitors and their business practices. Those companies then use that information to improve their own



business but have no intention of competing on an even keel against the company from whom the information was stolen. For example, a small to medium enterprise (Company A) gains information from a corporate heavyweight in the same industry (Company B). That information may pertain to Company B's manufacturing or business processes or even quality control methods. However, given the disparity between the size of the two companies, Company A may never be as big as Company B but will, nevertheless, use the information obtained to grow their own business.

In most cases, corporate espionage is a premeditated, deliberate act often taking the form of a well thought out plan of attack executed by senior members of an organisation. Consider the following example. A marketing team for a food manufacturer, Company Y, was constantly being beaten to the supermarket shelves by a competitor, Company Z, who somehow released new product lines that were similar to theirs but which had not been released yet. Company Y were planning to release a tropical theme to a product and had developed a fun and exciting marketing campaign. Two weeks prior to their launch, Company Z released a Hawaiian theme with a coincidentally similar marketing campaign. Company Y's prediction of winning market share for this product line was dramatically sledge hammered. Unbelievably, this occurred for three different product lines in the same year. The way this was uncovered will be discussed later in this article.

However, corporate espionage may not always be a deliberate act. In some cases, corporate espionage can be the unintentional by-product of an eager new employee, keen to scale the corporate ladder. In the quest to achieve success, the employees may use ideas and strategies which are not entirely their own. Such ideas may have come from previous employers or may even be passed on by friends and colleagues within other rival companies.

Some company directors may even find that they have been the unwitting accomplices to acts of corporate espionage. There have, in the past, been instances where senior personnel within an organisation have exploited a vulnerability within a competitor's company

with a view to stealing that competitor's proprietary information. They do this to gain an advantage for their own company.

However, they are acting without the knowledge or consent of the members of the board. Yet, despite the fact that the board members of the offending company claimed to be unaware of what senior management had been doing, they were, none the less, held partly responsible for those actions once exposed. While financial gain might seem the most obvious motivation for acts of corporate espionage, it is by no means the only motivation.

Certain vocal lobby groups conduct surveillance, pretext inquiries and even gain undercover employment within corporations they are seeking to expose. Whether it is to discover an environmental issue, a planned policy change or simply to uncover a corporate deception, these groups can be and have been very successful in the past.

depth and aggressive undercover investigation.

Companies seeking to gain information may also identify and target certain middle management employees who might prove to be a beneficial source of information. This tactic often involves the use of a skilled investigator who befriends the target employee outside of his/her work environment, at a local football match, party or club when that person's guard is at its lowest. When drinks are flowing freely and the focus is on socialising, not business, the unsuspecting employee can be vulnerable.

Generally speaking, these people are only too happy to speak about a top secret project to someone they would consider to be a total stranger with a view to either impressing or boasting. Unfortunately, no matter how friendly these new acquaintances may be, the unsuspecting employee has little or no knowledge of the detrimental impact this casual pass of information could have on the employer's business or product.

In most cases, corporate espionage is a premeditated, deliberate act often taking the form of a well thought out plan of attack.

Method

Information can be gathered from an unsuspecting company in a variety of ways. It can be as easy as simply asking a staff member of a competitive company if their employer has a new product that is ready to be released. Even when employees have been instructed about confidentiality and told that the company's information should not be given to unauthorised persons inside or outside the company, there are often staff members who are enthusiastic and pro-company who do not understand the consequences of loosely discussing the company's upcoming marketing plans or proprietary information. Often, these people are only too happy to talk about their company's pending expectations or achievements.

Should a staff member mention in passing that new product or initiative is due to be released, a simple phone call to the target company with a series of pretext survey questions could at the very least, confirm that the release of a new product is imminent. This, in itself, can lead to a more in-

Another method used to gather information is to have students apply for work experience with an unsuspecting company. Such people may come across as a Year 12 student or university student but may, in fact, be three or four years older and could even be a licensed inquiry agent. A corporate spy, acting in the guise of a student, may request a guided tour of the plant for a project claiming that they are writing a thesis. There have even been occasions when individuals operating under a similar guise have secretly video taped the creation and design of a new product.

Some companies will also attempt to obtain competitor information by headhunting specific employees with lucrative job offers. Desirable individuals are offered substantially greater salary packages with attractive benefits. However, once the employee has been "lured" into the fold, they are milked for any and all information they may possess about their previous employer, which is then used by their new employer.



Typically, studies have shown that these new employees do not last long in their new organization. Once the valuable information is obtained, the employee either leaves, as he or she realizes what has happened, or the new employer discards them as a by-product on their way to gaining valuable market share with their new 'innovative product'.

Action

One way to prevent such breaches of security is to have a professional assessment conducted. During this process, disgruntled employees who would willingly and knowingly leak top-secret information to create problems for senior management may be identified and can be handled accordingly.

One method for handling such employees may be to have them sign some sort of non-disclosure agreement pertaining to company information and practices (if they have not already done so). Surveillance is a tool which is also commonly employed in cases of corporate espionage.

Watching key members of an organization with a view to ascertaining whom they visit and who is visiting them can give valuable insights into, and an understanding of, a company's relationships and networks. This information can be analysed and a determination can be made as to what this company may be trying to achieve.

This was evident in a case in the US where

a steel manufacturer of a certain type of aluminium screen had surveillance conducted on a competitor who was involved in the manufacture of other non-aluminium steel products. After a week of observing aluminium being delivered, it was quickly determined that this company was intending to manufacture a similar product and therefore compete.

The company which authorised the surveillance quickly made some decisions, which led to the securing of long-term contracts with customers, which virtually rendered the competitor as non-

threatening. The competitor cut its losses and ceased its proposed plan to introduce the similar product line.

In most jurisdictions it is not a criminal offence to obtain information by request, or the hiring of a competitor's employee with knowledge of the company's proprietary information. Civilly, however, breaches of confidentiality agreements and non-compete clauses in contracts can be aggressively pursued and fought out in courts.

However, not all of the methods used to obtain information in the name of corporate espionage may be considered entirely legal. There are, unfortunately, some unscrupulous operators who would advertise themselves as professional investigators. Such companies may resort to tactics such as the theft of files from staff vehicles, homes and offices, all of which are criminal acts. Investigators who promote this type of illegal behaviour leave not only themselves but also the company they are advising at high risk of prosecution.

Surveillance has, in the past, been extremely effective in determining where security breaches have been occurring within specific organisations.

The old fashioned "break in" was once common amongst this type of company. However, with the modern era of high tech security and proactive guard forces, there is less chance of this type of activity going unnoticed.

Prevention

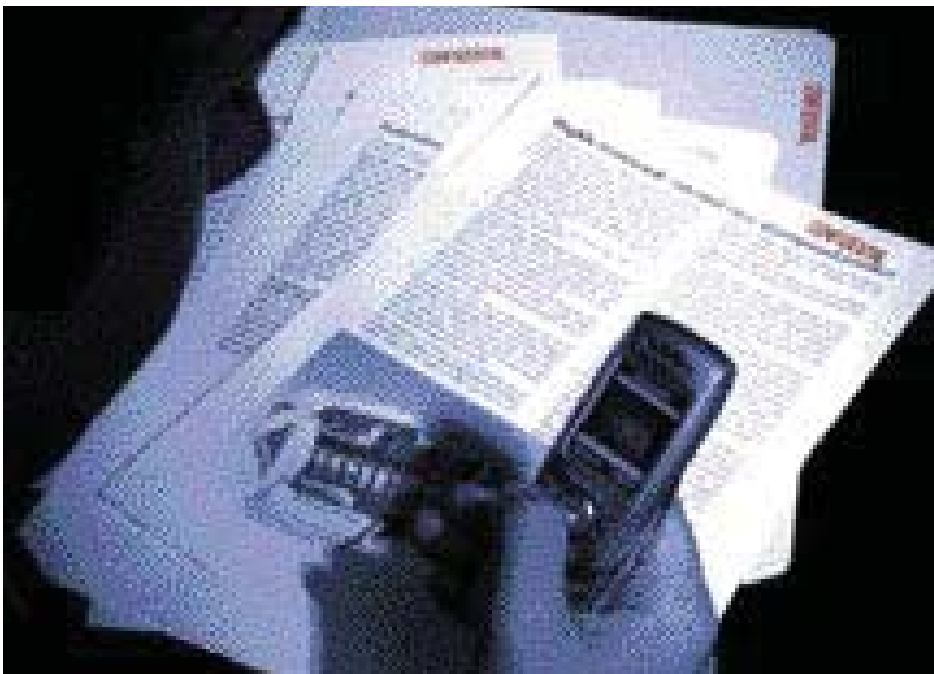
According to Andy Chambers, the Managing Director of Pinkertons Australia, one of the country's largest security consulting and investigation firms, good corporate security begins before an employee even walks through the doors.

"Background checks and pre-employment vetting are the first step in preventing security breaches. Even then there is no guarantee

...ensure that one has an ironclad confidentiality agreement in place, as its this subtle reminder that is often enough to curb any loose lips.

that the person you are employing is who they claim to be but at least you have minimised the possibility of employing someone with a dubious background or ulterior motives."

The next step, according to Mr. Chambers, is to ensure that one has an ironclad confidentiality





agreement in place (and where applicable, a non-competition agreement) and that all employees sign these documents prior to the commencement of employment. These documents are extremely important for a number of reasons.

First of all, they prevent staff from disclosing proprietary information about a company once they leave. They also give a company a means by which they can control the flow of information. For example, if an employee has been offered another job by a competing company with a view to milking that employee for information, upon leaving, that employee can be reminded that he/she has signed a non-disclosure agreement. Further, that if any information of a sensitive nature pertaining to the former employer, is divulged, there will be serious legal consequences.

Non-disclosure agreements are also useful at the beginning of a new project. In addition to advising staff of the sensitive nature of the project and informing them that they are not to discuss the project with anyone other than their immediate project team mates, managers can remind staff members that they are bound by the non-disclosure agreements which they signed at the commencement of their employment. This subtle reminder is often enough to curb any loose lips.

In addition to staff vetting and non-disclosure agreements, it is important that any company

dealing with sensitive information provide some sort of security and asset protection training to their staff. If your company is lacking a suitably trained asset protection professional, it is worth considering engaging the services of a company who specialises in asset protection.

Electronic security measures such as access control and CCTV systems play an important role in preventing the theft of sensitive information.

These companies can not only provide specialist training in how to deal with the types of security threats often associated with corporate espionage, but can also act on the company's behalf to identify the source of the information gathering attempts and deal with the offending company appropriately.

Awareness training should be the main thrust of any asset protection training package. In order to thwart the types of social engineering attacks mentioned earlier in this article, (such as telephone surveys and verbal probing at social events,) staff need to be aware of the methods employed in these types of attacks - as the old saying goes, "A tactic known is a tactic blown."

With regard to telephone surveys, staff should be alert to any people being overly friendly while

asking questions of a personal or sensitive nature.

They should also be aware of what may appear to be extraordinary coincidences. For example, if a receptionist has a Croatian accent and it just so happens that the person on the phone, during the course of the conversation, discloses that his

mother is from Croatia, be alert! This may just be a coincidence.

However, corporate spies will often try to build rapport with a person in an attempt to get that person to lower his/her defences. Flirting is another way in which corporate spies will attempt to get around a person's defences. Staff should also be wary of callers who, when questioned, refuse to leave a name or contact number where they can be reached.

Once staff members are aware of such tactics, ask them to keep a log of any such calls received

Mobile phone cameras have become a valuable tool in the arsenal of the corporate spy.





and if possible, refer the caller on to an in-house asset protection manager if one exists and if not, a senior manager who can deal with the situation appropriately.

Once again, should a person attempt to elicit information from a staff member at a social event, knowing what to look for and being aware of the tactics used for information gathering will be that person's greatest defence.

According to Andy Chambers, "Simply being aware of these tactics and making staff aware of such tactics makes it that much harder for any potential corporate spy to elicit information. In fact, if someone begins asking probing questions in a social environment, a staff member alert to the tactics, with the right training, could even take control of the situation by turning the questioning back on the person attempting to gather information perhaps even gathering information about that person."

The theft of files and or sensitive information for the office should be addressed by way of good house keeping policies. These might be a "clean desk" policy, which dictates that at the end of each workday, all work, including sensitive files and materials, must be cleared off an employee's desk.

Any and all sensitive documents or material should be either returned to a secure storage area, such as a lockable filing cabinet or file vault, or destroyed. If documents of a sensitive nature are to be destroyed, ensure that staff use only crosscut or "confetti" type document shredders as documents shredded in normal strip shredders can be recompiled and read with relative ease.

It is also a good idea to implement a policy whereby sensitive documents are not to be taken out of the office. Furthermore, any computers should be protected by some sort of encryption program to prevent unauthorised access. This protection should also extend to computer files taken from the office. If printed documents are to be taken out of the office, it is also recommended that they not be left unattended in vehicles.

As is the case with new staff members, any potential work experience candidates, cleaning and or contracting staff (such as trades people) should be subjected to appropriate background checks and vetting procedures prior to allowing those people access to company premises.

Ensure that anyone presenting themselves as a

student or work experience person shows photo identification prior to being given access to the company. Furthermore, ask for references and ensure that any references provided are contacted and checked. Also ensure that the organization or school this person represents is contacted to ensure the validity of their request for work experience.

Finally, it is a good idea to install some sort of security system comprising access control, CCTV and intrusion detection. This will help minimise any unauthorised access during non-business hours.

An organisation that is aware of its critical information and takes appropriate steps to protect it is the organisation most likely to succeed against corporate espionage. There are many steps which need to be taken in a proper protection program and the information provided in this article represent only tip of the proverbial iceberg.

Ongoing planning and testing of both physical and procedural security measures needs to be adopted. There is little point in creating a hard target with state of the art technology when the old saying of 'loose slips sinks ships' is still very much in vogue. A well thought out plan to provide protection for all sensitive information must be put in place over a period of time. Security professionals should carry out a security survey to assess the level of risk and overall vulnerability of the organisation. A security management plan should take care of the major issues such as access control, CCTV, security guards, provision of document safes and vaults.

Most importantly, security management plans should incorporate corporate policy relating to proprietary information. As discussed, confidentiality agreements, staff background checks, internal control, auditing and regular security awareness training should support a company's proprietary information and intellectual property protection policies. Pinkerton's technical security measures team (debugging) have located listening devices in boardrooms, chairman's offices and executive's homes during security audits. These eavesdropping devices have been installed by unscrupulous individuals who are fully prepared to 'cross the line' for a client who will pay whatever it takes.

In relation to staff security procedures, the importance of proper training provided by professionals with demonstrated experience cannot be stressed enough. Companies and their

employees require regular reminders of corporate pitfalls if relevant company information is not adequately protected. In addition, security auditors should carry out regular reviews of operational procedures. These should also include integrity testing of the systems in place.

In conclusion, let us return to the example of Company Y and Company X mentioned earlier in this article. After a security audit was conducted at Company Y's headquarters, it was revealed that draft marketing plans, including photo boards of the new products, were obtained by Company X from Company Y's rubbish bins of all places. It was revealed that Company Y did not utilize shredders in relation to relevant and important company documents, and their paper waste was placed in communal dump bins in their industrial estate. A counter espionage program was embarked upon, and covert surveillance cameras were strategically placed focusing on the bins in question. Unauthorized persons were recorded removing papers and company information. Further investigations revealed that these papers had been removed by staff employed by Company X. Too easy.

Companies serious about protecting what is rightfully theirs and who understand the enormity of misplaced proprietary information or confidential upcoming new company marketing trends, need to vigorously ensure that they have an effective and efficient countermeasure program in place. As an international investigations and security consultancy, Pinkerton has provided proprietary information and intellectual property protection programs to a variety of businesses worldwide. However, there are a number of companies in Australia capable of providing this type of advice. Those who believe they could be at risk of being targeted by industrial or corporate espionage and who feels they may lack the necessary expertise to combat such a problem is encourage to contact professionals and seek further advice. ■

Tania Bateman, is a Director of Pinkerton in Australia and consults to Pinkerton's global clients on security awareness and countermeasure programs.