

Trade secrets

Claire Shoesmith

Mon, Sep 10, 2007

SECURITY: With more job movement and better technology than ever before, it is much easier today to carry out acts of industrial espionage.

If you thought spying on, or copying from a rival was a pastime reserved for the classroom it seems you were mistaken. In fact, according to industry insiders, the developed world wouldn't be where it is now if it weren't for the human desire of needing to know what your rivals are up to.

As far back as the sixth century, the Byzantine emperor Justinian sent two monks to China, at the time the global leader in silk production, to steal silkworm eggs and mulberry seeds. A few years later, Byzantium had replaced China as the world's leading producer of silk.

In another such incident, it has been said that the industrial revolution, which turned America into a global economic power, grew out of a single act of industrial espionage, whereby a Boston merchant travelled to England in 1811 and stole the plans for the Cartwright power loom.

He brought it back to America and thus launched the textile industry that sparked its industrial revolution.

While these incidents may be a long time ago, old habits die hard, and believe it or not, such acts of spying and theft aren't confined to the history books. In fact, even as you read, some company somewhere around the world will be hiring a new starter who has been employed by a rival organisation with the sole purpose of stealing confidential information.

"At these levels it is a business, and one that can be likened to drug smuggling," says Rosemary Turley, head of marketing at Dublin-based technology group Norkom. "As in the case of the person carrying the drugs through the airport, the individual stealing the data will very often not know who they are working for and in some cases even what they are stealing."

However, this is not how all cases play out. According to Michael Harrington, commercial manager at Risk Management International in Dublin, industrial espionage - the act of spying on one's rivals to gain a competitive advantage - can refer to anything from stealing confidential data to simply finding out when a rival is planning to launch a new product.

And while it isn't talked about much here, Harrington is in no doubt that it happens in Ireland and the extent to which companies are at risk depends on the importance and sensitivity of the information they have at their disposal.

Andrew Harbison, senior manager of enterprise risk services at Deloitte agrees. "Information is power," he says, adding that in today's technological age, where about 98 per cent of company documentation is computerised, stealing information isn't something that's difficult to do.

"It's no longer a case of print it out, check no one's looking, and carry it out of the room," he says. "It's possible to lift an entire organisation onto a piece of hardware that you can carry in your pocket."

Admittedly headline-making incidents like that of a Coca-Cola employee trying to sell trade secrets to rival PepsiCo for \$1.5 million (€1.1 million), or Formula 1 team McLaren obtaining confidential information from rival Ferrari in a bid to get ahead on the racing track are few and far between here in Ireland, but Harbison and many others in the industry are in no doubt that theft and fraud relating to confidential information does go on.

In fact, the simple fact that most of the large law firms here in Ireland have experts experienced in the areas of misuse and misappropriation of commercial confidential information and intellectual property assets is a sign that it is an issue for Irish business.

However, the very nature of the activity and the potentially large financial losses that can be incurred as a result - it is estimated that US companies lose an estimated \$50-100 billion (€36-73 billion) a year in the theft of trade secrets and Europe can't be far behind - mean that people are reluctant to speak about it. In fact, according to Gregory Glynn, a partner at Arthur Cox, if such an issue does arise, most companies are keen to keep it out of the courts in order to protect their share price.

According to US statistics, about 85 per cent of all industrial espionage crimes are perpetrated by an employee and the situation doesn't seem to be any different here in Ireland. Glynn and his colleague Pearse Ryan, a technology law partner at Arthur Cox, agree, saying that while they haven't encountered any cases of one company rifling through a rival's dustbin in search of confidential information as Procter & Gamble did to Unilever back in 2001, they have definitely come across employees who "misbehave".

"There have been plenty of cases where employees leave to go to work for a rival and seek to take information with them," says Glynn, adding that he has also seen situations where employees start up dummy companies with the aim of taking money from their employer or even set up an operation to rival their employer.

He has also been in meetings where he has been required to take the battery out of his phone to ensure that unauthorised individuals can't listen in.

Paul Lavery, a partner in the Technology Group at McCann FitzGerald, says that given the amount of confidential and sensitive information that a company may need to provide to its employees in order for them to perform their functions properly, it's not surprising that while they are a significant asset of a company, they are also a potential source of misuse of information.

This may occur through disclosure of the information to competitors or through its use by employees in competition with their employer after they leave employment.

However, he does believe that companies in Ireland are becoming more aware of the issue and that today most employment contracts or confidentiality agreements contain clauses addressing such potential problems. He also says the increased awareness has coincided with a switch to a more knowledge-based economy. "The most valuable attribute of many companies is now their knowledge," he says. "That is something that is hard to protect."

While there has been an economic espionage act in the US since 1996, there is currently no specific law dealing with the issue here in Ireland. In the case of any alleged wrongdoing, injunctions will usually be sought to prevent someone who has allegedly obtained information illegally from using it to their advantage, and cases can be brought under laws relating to breach of confidence, data protection and criminal damage. Between them these can command fines up to €100,000, as well as damages to cover any losses suffered by the wronged party and even order the destruction of any items made with misused information.

Still, there is also a risk of taking things too far, says Grace Smith, intellectual property partner at McCann FitzGerald. "There's no point in being precious about the key to the photocopier," she says. "It is about knowing what is valuable and considering how best to protect it."

One thing that both Smith and Lavery are quick to point out is that it is important to ensure that people are made aware of what information is confidential and what isn't. If any problems should arise this can then be used as a defence in court.

Ryan, at Arthur Cox, says that as well as having corporate policies and procedures in place to deal with misuse and misappropriation of third party information and IP rights, it is important that employers ensure they take reasonable steps to implement them as this will assist in protecting the company should a third party allege misuse or theft of their assets.

While the dawn of the technology age has without doubt made it easier for some information to be stolen, it has also improved the situation for investigators. Luckily for them, computers are a bit like elephants - they never forget. Pressing the delete key, removing a website from the browser favourites list or moving a document to a recycle bin may seem to make something disappear forever, but in reality the way computers are designed to store information means that traces of the data still remain in the empty spaces of a hard disk.

So while there is no doubt that incidents of industrial espionage are going on here - in fact a former CIA agent recently claimed that both Dublin and Belfast are major centres of industrial espionage, an allegation that is currently being investigated by the Data Protection Commissioner's Office - companies appear to be becoming more aware of the issue and taking the appropriate measures to protect themselves. As one industry source said, no one is immune, so you'd better pay closer attention the next time you see James Bond in action.

High-profile Industrial Espionage:

Ferrari versus McLaren

In this most recent of cases, the FIA world motor sport council found McLaren guilty of possessing confidential information owned by rival Ferrari but said there was insufficient evidence that the team had used it to its benefit.

It is believed the documents were obtained from Ferrari's now-sacked performance director.

Coca Cola versus PepsiCo

A former employee of Coca Cola was sentenced to eight years in prison last year after being found guilty of conspiracy to steal the soft drink giant's trade secrets and try to sell them to rival PepsiCo. The sale never succeeded as PepsiCo informed its rival that the recipe it had kept secret for more than a century was being offered for sale.

Lockheed Martin versus Boeing

In 2003, Boeing was punished by the US Air Force for resorting to espionage to better its defence rival Lockheed Martin.

Unilever versus Procter & Gamble

In 2001, P&G undertook a corporate-espionage programme by hiring a consulting firm to rummage through Unilever's rubbish and steal the secret formula for a new hair-care product. The two companies eventually reached a settlement, with P&G agreeing to pay \$10 million (€7.4 million).

Lucent

In 2001 the FBI arrested two employees of Lucent Technologies (Lucent chief executive Patricia Russo is pictured below). The employees were arrested for conspiring to steal Lucent trade secrets and sell them to the Chinese government.

General Motors versus Volkswagen

In 1996 General Motors sued Volkswagen, charging that GM's former head of production had stolen trade secrets and turned them over to VW. This resulted in a landmark intellectual-property case, at the conclusion of which GM was able to obtain a very large settlement from VW.

France and England versus the Soviet Union

The Soviet Union was accused of industrial espionage in the development of its ill-fated TU-144 aeroplane in the late 1960s. Although the TU-144 flew before Concorde, its development was alleged to be connected with industrial espionage after two different Soviet representatives were found to be in possession of detailed plans about Concorde's development. The TU-144 had a short life however, after crashing at a Paris air show in 1973. The issues surrounding its creation were never really resolved, but did result in several imprisonments.

© 2007 The Irish Times