Security implications of t

By Fred Burton and Scott Stewart

THE global financial crisis is likely to create some new security problems for corporations and governments. Companies facing financial hardships often have to make spending cuts and layoffs. When companies plan cuts, they tend to focus on eliminating the corporate functions that do not appear to be contributing to their profitability. Corporate security can be one of these. A security department typically has a substantial budget and is usually viewed as detracting from, rather than contributing to, the company's bottom line. The "fat" security budget is seen as an easy place to quickly reduce costs.

Certainly some security programmes are indeed bloated and consume far too many corporate resources for the results they produce. Also, corporate security directors may not be good at educating management about ways their programmes contribute to corporate goals. Even when a security director has an effective programme and is a good communicator, it can be very difficult to quantify the losses that the corporation did not suffer due to the effective security measures so that the lack of losses and incidents due to a robust security programme can be interpreted by some to mean that there is no threat to guard against. Indeed, effective security can make it appear that there is no need for security.

In times of economic hardship, the relentless focus on operating expenses and even corporate cutbacks can lead to definite security challenges. One of these problems is workplace violence, but during times when people are hurting financially, issues such as employee theft, fraud and product theft by non-employees must also be carefully monitored. However, while the theft of a tractor-trailer full of computers or flat screen televisions can quickly get someone's attention, there is a far more subtle, and no less dangerous, threat lurking just under the surface. That threat is espionage — both corporate and state-sponsored.

The human-intelligence process: Corporate competitors, criminals and even foreign governments seek ways to gather proprietary information from companies, sometimes to boost their own operational capacities and sometimes to sell on the open market. Once a company has been identified as having the information sought, the first thing the human-intelligence practitioner will do is look for weak links in its operations. If the required information is readily available, there is no need to undertake a time-intensive and costly operation to retrieve it.

It is shocking to see the amount of sensitive and critical information openly available on the Internet and in research libraries, or freely given out at technical conferences. When open source collection efforts fail, more invasive measures must be employed. Sometimes the required information can be obtained via technical surveillance. A faulty information technology system, for example, can expose the company's secrets via remote electronic intrusion conducted from a continent away. Other times, information can be obtained by eavesdropping on telephone calls made by corporate leaders or by other technical surveillance measures.

> There are the employees whos
> be willing to risk committing i
> they can get away with it. Of t
> money, ideology, compromise
> proven to be the No. 1 motiva
> simple bribery is sufficient to

However, technical surveillance has its limitations, and sometimes critical information must be obtained through human intelligence, which means obtaining the required data from an employee in the targeted company. Due to human nature, human-intelligence practitioners use the same time-tested principles in the recruitment of corporate sources that they use when recruiting

the global financial crisis

W. E.O. - Financial Crisis

sources in the government sector.

The first step is "spotting". This is when the intelligence practitioner attempts to identify the workers who have access to the required information. Then a thorough examination of the backgrounds and situations of the employees who have that access is undertaken in an effort to determine which employee is most vulnerable to exploitation. Employees who are in dire need of extra cash to maintain extravagant lifestyles

se egos are so big that they might
ndustrial espionage just to prove
he four major motivations —
and ego (MICE) — money has
tion. More often than not,
btain the desired information

or to support drinking, drug or gambling habits, or who are hiding extramarital affairs that can be used for blackmail, make prime candidates.

A background check might also reveal that a certain worker is angry with his or her employer over issues of salary or placement in the company. There also are employees who disagree ideologically with a product their company makes or the process the company uses to produce it. Finally, there are the employees whose egos are so big that they might be willing to risk committing industrial espionage just to prove they can get away with it. Of the four major motivations — money, ideology, compromise and ego (MICE) — money has proven to be the No. 1 motivation. More often than not, simple bribery is sufficient to obtain the desired information, especially if the employee is living beyond his or her means. Demanding proprietary information in exchange for not exposing a personal secret, too, is a cost-effective approach that also allows the agent to return again and again to the same source. This method is a bit riskier, however, since it can cause more resentment and make the source more likely to rebel.

Emphasising the 'M': The next step is to actually approach the employee and "pitch" him or her. This is often a gradual effort to establish a relationship of trust. Contact can begin gradually with requests for small, seemingly harmless bits of information such as internal phone numbers. In this approach, known as the "little hook," the employee is offered "gifts" in exchange for these favours. The requests gradually become greater in scope until the targeted information is obtained. Other times, the pitch is blatant; the practitioner makes a flat-out cash offer for the required goods or shows the target the evidence that will be used for blackmail.

In the current economic environment, cold hard cash is an even more attractive approach. In fact, it is not at all unreasonable to anticipate that companies and foreigners will face a windfall of walk-in sources who volunteer to sell critical information. In such a buyer's market, information can often be bought at fire-sale prices. One of the most publicised examples of this in recent years was the disgruntled Coca-Cola Co. employee arrested in July 2006 after attempting to sell Coke's recipe to rival Pepsi. Mass layoffs also complicate the equation because some of the employees being laid off may have access to critical information.

Not just a corporate worry: Vulnerability to espionage is not confined to the private sector. With many corporate security departments being cut to the bone, many internal security services focused on the counter-terrorism mission and many law enforcement agencies chasing white-collar criminals, it is a good time to be in the intelligence business. One day we will look back on this time through a counterintelligence lens and see that, although it was a time of bear stock markets, it was a tremendous bull market for practitioners of human intelligence. COURTESY STRATFOR