By Fred Burton and Scott Stewart

As anyone with a stock portfolio knows, it is a rough time for the markets. With many portfolios down 50 percent or more, this large loss of equity and wealth has been very difficult on individuals and corporations. The problems, of course, have not been confined to the stock markets. With property values plunging and variable-rate mortgages ballooning, many homeowners are also caught in a bad situation -- the number of homeowners behind in their mortgage payments has been increasing and the number of foreclosures has grown. Unemployment is also an issue. According to the Bureau of Labor Statistics, in January 2009 there were 2,227 mass layoff actions in the United States involving 237,902 workers.

Significantly, the financial crisis is not just restricted to the United States -- it is a global event that is also having a severe impact on economies in Europe, Asia and the developing world. Things are tough all over, and this financial strain will create some large security problems for corporations and governments.

Threats to the Bottom Line

During times of financial hardship, companies often have to make cuts like the aforementioned layoffs. When companies plan cuts, they often focus on eliminating those corporate functions that do not appear to be contributing to the company's profitability. And one of the first functions cut during tough times often is corporate security. A security department typically has a pretty substantial budget (it costs a lot for all those guards, access-control devices, cameras and alarms), and security 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 in an effort to balance the profit-and-loss statement.

This view of security is due to a number of factors. First, it must be recognized that there are certainly some security programs that are indeed bloated and ill-conceived that have consumed far too many corporate resources for the results they produce. Furthermore, there is a long tradition of corporate security directors who are not good communicators and who do not take the effort to educate upper management about ways their programs contribute to corporate goals. However, even when a security director has an effective program and is a good communicator, it can be very difficult to quantify the losses that the corporation did not suffer due to the presence of effective security measures. The lack of losses and incidents due to a robust security program 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, a paradox we have also seen in the historical pattern of U.S. go

vernment security funding -- a pattern that has resulted in a number of disastrous attacks against U.S. embassies.

In times of economic hardship, the relentless focus on operating expenses and even corporate cutbacks can lead to definite security challenges. As we discussed last November, 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

Espionage is always a problem corporations must face. Competitors, criminals and even foreign governments often seek ways to gather proprietary information from companies, sometimes to boost their own operational capacities (e.g., to apply critical or emerging technologies to their weapons programs) 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 the targeted company's operations. If the required information is readily available, there is no need to undertake a time-intensive and costly operation to retrieve it. Indeed, it is shocking to see the amount of sensitive and critical information that is openly available on the Internet and in research libraries, or that is 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 using other technical surveillance measures.

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 working within 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 sources in the government sector. (The risks associated with obtaining unclassified proprietary information from private companies are often far less than those associated with obtaining classified information from government agencies or national research laboratories.)

The first step in the human-intelligence process is called spotting. This is when the human-intelligence practitioner attempts to identify those workers who have access to the required information. Then the practitioner conducts a thorough examination of the backgrounds and situations of the employees who have that access 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 or to support drinking, drug or gambling habits, or those who are hiding

extramarital affairs or other secrets 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 the product their company makes or the process the company uses to produce it. Finally, there are the employees whose egos are so big that the

y might be willing to risk committing industrial espionage just to prove they can get away with it. Robert Hanssen, an ex-FBI special agent accused of selling secrets to Russia, was motivated by the belief that he was above the system and could commit espionage without being caught.

Of the four major motivations for committing espionage -- money, ideology, compromise and ego (known to security officials as MICE) -- money has proven to be the No. 1 motivation, though two or more motivations can be used to turn an employee. More often than not, simple bribery is sufficient to obtain the desired information, especially if the employee is living beyond his or her means for one reason or another. Outside agents looking to turn an employee can also use blackmail ("compromise" in the MICE acronym). Demanding proprietary information in exchange for not exposing a personal secret, for instance, 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 than other means and make the source more likely to rebel. However, sexual entrapment and blackmail is still widely used as a recruitment tactic, one that has been used with great success in recent y

ears by the Chinese government against targets such as Japanese and Taiwanese government officials, FBI special agents -- and foreign businessmen.

Emphasizing the 'M'

Once the practitioner has identified the weakest link, decided on the approach to take and made a specific plan on how to proceed, the next step in the human-intelligence process is to actually approach the employee and "pitch" him or her. This step is often a gradual effort to establish a relationship of trust between the practitioner and the employee, and 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 favors. The requests gradually become greater in scope until the targeted information is obtained. Other times, the pitch is far more blatant and the human-intelligence practitioner does not take the time to establish a relationship or gradually recruit the target. Instead 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, with many 401(k) plans now more like 201(k)s, stock options severely underwater and homeowners facing foreclosure, cold hard cash -- the M in MICE -- is an even more attractive approach. In fact, with employees seeing their investment accounts decline dramatically, and perhaps even facing the possibility of home foreclosure, it is not at all unreasonable to anticipate that companies and foreigners will face a windfall of walk-in

sources who will volunteer to sell critical information -- and in such a buyer's market, information can often be bought at fire-sale prices. Employees attempting to sell proprietary information are somewhat common; one of the most publicized examples of this in recent years was the disgruntled Coca-Cola Co. employee who was arrested in July 2006 after attempting to sell Coke's recipe to rival soft drink company Pepsi.

Mass layoffs also complicate the equation, especially when some of the employees being laid off have access to critical information. If measures are not taken to ensure that the information is protected, the information could easily find itself in the hands of competing companies or even foreign intelligence services.

Not Just a Corporate Concern

The current financial crisis -- and vulnerability to espionage -- is not just confined to the private sector. There are many federal government employees in the United States who have watched their investments in the stock-based funds of the government's Thrift Savings Plan wither on the vine over the past two years, and judging from the performance of foreign stock exchanges, the investments of employees in other governments have followed suit. Additionally, government employees tend to live in places with very expensive real estate, like Washington, London, Paris and Tokyo. This means that a foreign intelligence officer armed only with a briefcase full of dollars, euros or yen can make a substantial amount of money. With many corporate security departments being cut to the bone, many internal security services focused on the counterterrorism 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.