INTRODUCTION
Espionage is the collection, collation, and analysis of illicitly gained information. In the case of industrial espionage, the most common objectives are to determine competitor activities with regard to new products, formulations, research areas of interest, production methodology, production quantities, promotional programs, distribution, and economics. Corporate espionage is also used to examine products or ingredients for perceived or actual risks, to time markets, and to establish pricing. All too commonly, companies find themselves the targets of such activity without the knowledge or methodology to effectively counter it.

As we move further toward an information-driven society in which information is traded and brokered, knowledge will become more powerful than ever. Knowledge theft is becoming an increasingly important and influential crime, and one that has become increasingly difficult to combat.

The business world has become more vulnerable than ever before to corporate espionage as we move information systems from paper-based to online. Now that many companies are moving their corporate information to the Web, they need to realize that most computers systems were never intended to be secure, and that should be a cause for concern.

CORPORATE ESPIONAGE
The landmark National Debt Clock in New York City was recently shut
down due to the fact that the debt is now decreasing. But if there were some type of device to measure the losses due to corporate and industrial espionage, it would be an enormous calculation. And it would be increasing at a dramatic rate.

Did you ever wonder why the Russian supersonic airplane, the TU-144, looks dramatically similar to the European-built Concorde? Coincidence? Twist of fate? No way. The Soviet-built look-alike, nick-named the Konkordski, was built during the Cold War when the Russians, Americans, and Europeans were in a fierce battle for profit and honor to build the first supersonic aircraft. What was unique about this battle was that it was fought not only in the skies by the world’s top aircraft designers, but also on the ground by secret agents of Communist Russia. The Konkordski is one of the classic examples of industrial espionage.

The pilfering of the Concorde’s designs was a top priority for the Kremlin and the KGB. While the Russians were able to succeed somewhat (the TU-144 flew before the Concorde, but never made it into mass production), their espionage required a large network of spies located in many different countries. Such requirements necessitate huge budgets, logistics, and personnel. Too bad for the Russians that the Internet was not around then; it could have saved them immense effort. But while the end of the Cold War put many spies out of work, they are now finding new jobs in the area of corporate espionage.

Some of the effects resulting from compromised corporate information include:

- Loss of market share
- Loss of profits
- Loss of business
- Weakened balance of trade

Ira Winkler, a former analyst with the National Security Agency and author of Corporate Espionage: What It Is, Why It Is Happening in Your Company, What You Must Do About It, asserts that American companies lose billions of dollars each year as a result of corporate espionage. What is ironic is that a significant portion of such losses is preventable.

Corporate espionage is known to a certain degree as competitive intelligence. While competitive intelligence is a legitimate and strategic business tool, when taken too far, it becomes corporate espionage. The problems of unlawful corporate espionage were so severe that they led to the passage of the Economic Espionage Act (EEA) of 1996.

The EEA is one of the most significant pieces of criminal intellectual property legislation in history. This act was designed to combat the theft of American intellectual property by foreign governments and foreign companies. The EEA makes industrial espionage a criminal offense as opposed to a civil crime (which is how it was dealt with previous to the
Prior to the EEA, if an act of corporate espionage had occurred, recourse for such wrong was generally limited to instituting a civil action against the party misappropriating the trade secrets, and perhaps involving state authorities through an unfair trade practice statute. Protection of trade secrets through federal criminal prosecution was exceedingly unlikely.

Specifically, the EEA:

- Makes it a federal criminal act for any person to convert a trade secret for his or her own benefit, or for the benefit of others, intending or knowing that the offense will injure the owner of the trade secret
- Makes it a federal criminal offense to receive, buy, or possess the trade secret information of another person knowing the same to have been stolen, appropriated, obtained, or converted without the trade secret owner’s authorization
- Defines the term “trade secrets” to mean all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether how stored or compiled, memorized physically, electronically, graphically, photographically, or in writing; and a federal offense has been committed if the owner thereof has taken reasonable measures to keep such information secret and the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means to the public
- Imposes up to a ten-year prison term and/or a maximum fine up to $250,000.00 on any person, and a $5 million fine on any organization
- Requires the forfeiture to the U.S. Government of proceeds or property derived from economic espionage and may require forfeiture of property used to commit economic espionage

A prime factor in the creation of the EEA was as a reaction to the conflict between General Motors (GM) and Volkswagen (VW). The case involved the alleged theft of intellectual property, including numerous designs and trade secrets by Jose Lopez, a former GM executive. VW lured away Lopez, along with his voluminous stockpile of intellectual property, in an effort to learn more about GM’s design plans for new products and existing technology. GM sought to take action against VW in the United States but found its remedies limited. Criminal action was basically foreclosed by the absence of criminal trade secrets legislation. GM was left fighting a protracted civil action with VW in the United States, while Lopez spirited GM’s secrets to Europe. Only in late 1996 did the German government take criminal action against Lopez and others.
COMPETITIVE INTELLIGENCE METHODS

There are numerous legal methods of competitive intelligence, such as the review of public information. But once eavesdropping and dumpster diving are carried out, such activities generally cross the line into illegal activities.

As an example, the National Counterintelligence Center (http://www.nacic.gov) offers the following suggestions to assist companies in safeguarding their corporate information:

1. Obtain support for information security from senior management.
2. Do not waste resources protecting that which does not require protection.
3. Identify what information should be protected and for how long.
4. If extremely sensitive, information should be hand-carried or transmitted using encryption techniques.
5. To dispose of sensitive information, shred it or make it unreadable.
6. Valuable company information must not be left unattended in hotel rooms; this includes printed copies and removable media.
7. E-mail and voicemail passwords must be protected and changed frequently.
8. All sensitive materials must be removed from conference rooms, and chalkboards and whiteboards must be erased after meetings.
9. Where possible, conduct back-ground investigations on all individuals with access to sensitive information.
10. Obtain nondisclosure agreements from employees, vendors, and others with access to proprietary information.
11. The disgruntled employee is the greatest threat to your organization.
12. Telephone conversations, both fixed and mobile, are vulnerable to intercept.
13. Information regarding the movement of your company aircraft, including routes and destinations, is available for sale on the Internet.
14. Be knowledgeable regarding your organization’s physical assets, information assets, and vulnerabilities.

Additional steps to prevent information release include:

15. Physical security: while some companies obsess on using 4028-bit encryption keys, they neglect to lock the doors to the data center. Passwords alone will not prevent determined infiltrators from stealing.
16. Shred all paper documents before trashing them.
17. Do not discuss company secrets in unsecured environments.
18. Do not assume your consultants and temps are necessarily working on your behalf.
19. A little, well-placed paranoia could save your company from financial calamity and public humiliation.
Competitive Intelligence and the New Economy

Intelligence and surveillance have in the past required significant resources. In the past ten years, intelligence and surveillance have gone mainstream and migrated into a discipline known as competitive intelligence. Competitive intelligence is the act of gathering information about competitors’ activities.

Competitive intelligence has become vital in the Internet age because the nature of the new Internet-based economy often lowers barriers and entrance times. This new paradigm, combined with systems being rolled out in “Internet time,” means that companies must react to their competitors and business partners in record time.

In the rush to get on the information superhighway, many companies have often entered blindly into the myriad security risks involved. This has resulted in organizations spending money on physical security while not properly budgeting for information systems security.

Tom Jones, General Manager of the Cookeville, Tennessee-based Research Electronics International (www.research-electronics.com) notes that people are using the Internet to see what is going on at their competition. Jones notes that there are many, many ways to gain information on another company’s activities. These methods can range from digging through trash, to compromising the competition’s employees, to actually planting bugs. And this barely scratches the surface on how to gain competitive information.

The double-edged sword, Jones notes, is that if revenues are down and budgets have to be cut, security is often the first to get the axe. The problem is that there may be active espionage occurring, and when security is the first to get cut, the remainder of the organization becomes even more vulnerable. Jones notes from his experience that money must be spent on security, irrespective of the economy.

“I believe in many environments it’s almost impossible to catch somebody who is good enough,” states Richard Power, editorial director for the Computer Security Institute (www.gocsi.com) and author of Tangled Web: Tales of Digital Crime from the Shadows of Cyberspace. Power comments that, “One of the great blunders in the defense of cyberspace is that the threat is juvenile hackers. They end up in the headlines because they get caught. But professionals most often don’t get caught.”

Preventing Information Release

One of the first steps in attempting to protect data is information management. The basic idea behind information management is that to the degree data has value to an organization, it has comparative value to the competition. As an organization’s intellectual property moves from the filing cabinet to the network, it becomes much more difficult to manage using traditional protection methods.
The first recommendation to prevent information release is that every company, no matter how small, needs to have a structured business intelligence effort. Part of this business intelligence effort is a comprehensive risk analysis and assessment. Without a complete risk analysis, security endeavors will exist in a vacuum. An effective risk assessment and analysis ensures that organizations are worrying about the right things.

A risk assessment should define items into categories of threats, vulnerabilities, and risks. At a high level, they can be broken out as:

1. Threats:
   a. What are they?
   b. Who are they?
   c. What techniques do they make use of?
2. Vulnerabilities:
   a. How sensitive is your information?
   b. How valuable is that information?
3. Risks:
   a. How well is your infrastructure currently protected?
   b. Is the protection adequate?
   c. If it is not adequate, how do you plan on rectifying it?

Taking the aspect of a risk analysis further, in *Economic Espionage: An Information Warfare Perspective*, Dr. Myron Cramer details five approaches to preventing information release:

1. **Defensive.** A heavily defensive posture is characterized by an emphasis on *information protection*, including significant access control and limited external system interconnections. This posture might be appropriate for a dominant market leader or an organization that benefits from the status quo. This strategy will have advantages in an environment containing emerging adversaries that are pursuing strategies to attack the leader or to change the current situation.

2. **Offensive.** The offensive posture is characterized by an emphasis on *information denial*, including attacks on the market leader. This posture might be taken by organizations that are dissatisfied with their current standing and that may be desperate to take down their stronger adversaries.

3. **Quantity.** The quantity posture is characterized by an emphasis on supreme *information transport* capability. An organization adopting this posture places its confidence in its ability to move and use massive amounts of information over a large well-established infrastructure. It depends on the sheer volume and timeliness of its data to make attacks impractical. This posture will work best when the value of the organization's information is widely distributed and is of low sensitivity.
4. **Quality**. The quality posture is characterized by an emphasis on *information management*. A practitioner of this posture gains its advantage by its ability to manage its information needs better than its competitors. Compared with these competitors, its investments may be more modest, but they are wisely made. It makes better use of less information and optimizes its use of modest protection. This posture may have advantages in a highly competitive, cost-sensitive market.

5. **Sponge**. The sponge posture is characterized by an emphasis on *information collection* and an insatiable thirst for large amounts of information. Practitioners of this posture may have adopted a follower strategy in which they quickly bring products to market based on the innovations of others. They gain their competitive advantage by saving in research and product development. To avoid being left behind, they must monitor the activities of other, more innovative adversaries and survey market responses so that once they decide to follow a given initiative, they can quickly catch up in the marketplace using their previous market presence.

The Internet has made competitive intelligence in many cases nearly effortless. Using the Concorde development effort as an example, the Russians needed physical access, money to bribe, meeting locations, etc. With so many companies putting their corporate crown jewels on unprotected and misconfigured networks, many spies now do not even have to leave their home base.

While many networks do release an overabundance of data, an organization can counterattack against competitive intelligence. When designing an Internet presence, system architects must make certain that security is an integral part of the design. As an example, certain marketing information, such as prices and sales policies, which is customarily disclosed to outsiders, should never be placed on unsecured systems where it might be disclosed to competitors. Similarly, marketing strategies, marketing plans, market share status, and other marketing information should never be shared with competitors. Designing systems with such a paradigm is often a confusing point for people working in sales and marketing. On one hand, certain information, such as prices and sales policies, is discussed with just about any prospect or customer. On the other hand, this information is of great value to the competition.

Granted, third parties working for the competition could gather this information on behalf of the competition, but such a design forces the competition to engage in borderline unethical activity (changing or concealing their identity to get information to which they would not otherwise be entitled). Just because it is questionable, does not mean that the competition is not going to use third parties to gather competitive intelligence (industrial espionage) information; this policy just makes it more
difficult for them. Separately, such a design assumes that people working in sales and marketing know who the competition is. In some industries (e.g., restaurants in a large city), there are so many competitors that it is not feasible to have an up-to-date list of all of them (even in the Yellow Pages phone directory). On another note, each organization will need to clarify the precise types of information that it wishes to withhold from the competition (or implement a data classification system).

CONCLUSION

Corporate espionage is a real problem that affects many organizations. Companies spend billions of dollars in research and development. But if they are not spending an adequate amount to protect those developments, then their competition will likely find a way to take advantage of their valuable and vulnerable assets.

Notes

1. The media often intertwine the following terms: competitive intelligence, business intelligence, industrial espionage, information warfare.

Ben Rothke, CISSP, is a senior security consultant with Baltimore Technologies. He can be reached at ben.rothke@baltimore.com. The views expressed are those of the author.