

How Not to Tell All

Richard B. Isaacs

Security Management, May 2004

Companies generally appreciate the importance of obvious trade secrets, but they are often unaware that much of their other information being made public can be pieced together by industrial spies and used against them to gain a competitive edge. Consider, for example, the following scenarios: a business person receives a call at home from an undergraduate doing a paper. The student asks questions about certain business operations, which the businessperson graciously answers. The “student” is actually calling on behalf of a competitor. In another scenario, a startup company eager to get publicity about staff, a larger company hires away the key players, effectively crippling the startup as a possible competitor. The larger company does not ask the new employees to reveal secrets of their previous employer, and, indeed, does not really care whether they even show up for work in the morning, as long as it is not at the former employer’s place of business.

In a third scenario, new neighbors move in next door to a young, fast-track research scientist. Within a year or two they are close friends with free access to each other’s homes. This allows the new neighbor, a long-term low-level agent with his homeland’s government, access to information brought home by the scientist, something neither the scientist nor the company will ever know. In another case, a senior executive is at a trade show where he is induced to exchange some very minor, then somewhat less minor, information about a forthcoming product in exchange for help with a personal problem. The company, unaware of the issues, will never know that a person of responsibility has been suborned.

Each of these situations could pose serious problems to a company in terms of lost revenue. The common factors here are that:

- The people involved are trusted insiders.
- Incidents take place off-site and out of the company’s sphere of control.
- Information is willingly made available.

Since these situations primarily involve trusted people outside the company’s direct control who are often dealing with information that the company has not deemed confidential, the conventional wisdom (have good access control, shred documents, sweep the executive conference room for

bugs, get encryptors for telephones), while absolutely true and very important, does not deal with either the core or the bulk of the problem.

Starting points. To deal with economic espionage and information loss, security professionals have to come to grips with four basic points: Companies tend not to pay attention to the problem. No one person takes responsibility for the problem. Spies and competitive intelligence professionals know how to be unobtrusive. Outside expertise is probably needed.

Lack of attention. According to the *2002 Annual Report to Congress on Foreign Economic Collection and Industrial Espionage*, economic espionage and loss of critical information cost American companies more than \$300 billion a year. The average cost per incident is \$50 million for manufacturing companies and \$500,000 per incident for non-manufacturing firms. Short division tells us that if only manufacturing companies were hit there would be 6,000 incidents a year, and if only non-manufacturing companies were hit, there would be 600,000 incidents a year. The number for both combined is between the two, but large enough for anyone to safely assume that their company either was, is, or will be a victim.

Based on the magnitude of the losses involved, it would be reasonable to assume that economic espionage is an active concern for companies. In fact, however, losses from economic espionage can always be explained away by factors other than information loss, and companies may be repeat victims, losing business, closing divisions, and sometimes even going out of business, without ever considering the possibility that they have been victimized.

Nobody takes responsibility. The natural corollary to this is that there is nobody in the company designated to take responsibility for preventing or dealing with economic espionage. By this I mean that, other than companies that have defense contracts involving classified information, where there are statutory requirements to be met, I have never encountered a corporation where a senior manager was responsible for preventing and dealing with espionage and information loss. With no management interest, there is no funding. With no funding comes increased opportunity for theft.

Spies are unobtrusive. It is estimated that well over 90 percent of the information that competitive intelligence professionals seek is available legitimately through public sources or is otherwise willingly given away (an al Qaeda manual estimates this to be 80 percent for their specialized needs) When well-trained spies contrive to encounter unsuspecting employees off site and get them to divulge valuable information, the other 10 to 20 percent is at risk. In either case, companies will not know when they have been targeted.

The solution requires expertise. Anti- and counterespionage are specialized fields with few players on the commercial side. A company is unlikely to have anyone on staff with the experience and skills to ferret out unseen threats and vulnerabilities. As with many other highly specialized fields, a company will probably need to get consulting help to properly protect its information assets from spies.

OPSEC. Once a company recognizes the problem and decides to do something about it, what can be done? A generally accepted approach to information protection has been to make use of a government-developed process known as Operations Security or OPSEC. The OPSEC process was developed during the Vietnam War when it was discovered that people were dying because of what was believed to be espionage. However, it was later obvious that the losses resulted from information that was not secret but pointed the way for knowledgeable analysts to understand what was actually happening.

In the government, OPSEC is used to identify and protect information that is critical but not classified (there are already procedures in place to deal with classified information). This includes unclassified indicators that may lead to compromise of classified information. For example, employee attendance at specialized conferences would be an indicator of an employer's interest in that area.

The private sector does not have an information classification system, but OPSEC can be used to identify and protect all information that would give competitors and adversaries an advantage. This includes both trade secrets and other information that is not a trade secret but is nonetheless critical.

OPSEC is a formal process for looking at the protection of critical information from the viewpoint of an adversary and then denying that adversary the information it needs. It is important to remember that OPSEC largely a way of thinking. It is not a series of steps to be taken one after the other. Rather, it is a process, with each piece of the OPSEC process being reiterated and interacting with every other piece. The components of the process are: analyze the threat, identify critical information, examine vulnerabilities, assess risk, and apply countermeasures.

Threat analysis. While every adversary would like to have a competitor's information, few would consider taking illegal actions to gain some specific information, and fewer still would have the means to take these illegal actions. But since over 90 percent of the information desired will be available through open sources, most of a company's adversaries do not

need to break the law to get what they seek. They are a threat largely because the company willingly chooses to make that information available.

Some percentage of adversaries do have both the intent and capability to be a threat, however. These few must be carefully watched to make sure that they are prevented from taking advantage of the company.

Companies need to determine which adversaries have both the intent and capability to be a threat. These few must be carefully watched to make sure that they are prevented from taking advantage of the company. For example, certain foreign governments may be targeting certain industries. Companies can assess which governments are adversaries, based information provided by federal authorities, and steps must then be taken to protect against their efforts.

It is important to remember that without trust there can be no betrayal. Thus, trusted insiders present the potential threat of being suborned or stealing information for money or for some other reason. Being prepared for this eventuality is important.

Other adversaries may target a company to further political objectives. For example, if the company does animal testing, cuts down trees to make paper, or has financial dealings with places to which others object, information loss may lead to physical danger. Other adversaries may merely have a financial interest. The planning and intelligence gathering for kidnappings can take anywhere between six months and three years.

Critical information. Every company must identify its critical information that needs protecting so that it can be denied to those who would make use of it. The critical information identified must be the information that would be critical to competitors and not necessarily to the company itself. By identifying and analyzing competitors' needs and viewing the company through a competitor's eyes, the OPSEC team can identify the data that would be most critical to the other party's needs.

A senior company employee must be looking, from the OPSEC point of view, at everything published or made public, including technical articles, popular articles, business publications, annual reports, statements, marketing materials, internal newsletters, sales materials, advertising, speeches, presentations, media interviews, and press releases. But OPSEC goes beyond printed materials. There are often physical clues that give away valuable information that should be masked. All of these need to be reviewed to ensure they do not reveal sensitive, proprietary, or trade secret information, or indicators of that information.

Vulnerability. Vulnerability exists when an adversary can exploit critical information (see **sidebar** at bottom of article). A vulnerability may arise from lack of training, release of information the company has failed to identify as critical, use of insecure communications, publishing of VIP itineraries, interviews, corporate publications, press releases, publicizing of attendance at specialized conferences, subornation, disgruntled employees, desperation, or a host of other reasons.

The company is also vulnerable when employees, suppliers, consultants, temps, OEMs (original equipment manufacturers), and others who handle corporate information (we will call them “participants”) deliberately or accidentally disclose information that they have not been told is critical. Whether a participant is at a trade show or talking on the phone, the mere fact that the person has been asked for information does not mean that he or she needs to give it out. But if the information has not been identified as critical, the participant is likely to reveal it. And any loss from its disclosure is a management issue, not an employee issue.

The company is also vulnerable if its participants have vulnerabilities of their own. A company should do checks to determine any such vulnerabilities of participants and their employees, and it should obtain nondisclosure agreements from them.

Finally, keep in mind that governmental regulations or court mandates may make critical information about a company accessible to the public. Access and use of such information can tell adversaries much of what they want to know, and this access breaches no legal or ethical boundaries. For example, one company may see from statutory reporting requirements that another competitor is making progress in a mutually competitive area, and it may decide to throw money at the problem and beat them to market. Defending against this vulnerability is difficult, since the information is required by statute.

Risk assessment. After a company has assessed the likelihood that each specifically identified adversary will use any of the identified vulnerabilities to gather and exploit the company’s critical information, the company can put a dollar figure on the impact that such a loss of information could have on the corporation.

Risk is calculated as:

risk = probability x impact

where

probability = threat × vulnerability

so that risk decomposes to

risk = threat × vulnerability × impact.

Threat. Threat comes from specific competitors or adversaries. If there is no threat, there is no risk. But the numbers tell us that there is a real threat – an that given the prevalence of industrial espionage, there is probably a specific individual or organization has the desire, the skill, and the intent to acquire your company’s critical information.

Vulnerability. Some targets are more vulnerable than others, generally through neglect because the entire issue has been overlooked. If vulnerability is lowered, risk will be lowered as well.

Impact of the theft. How damaging is the loss of specific assets? If the impact is low, the company need not care. If it is high, it is cause to worry.

To see the interaction among threat, vulnerability, impact, and risk, look at theft of pens. The threat is high, because everyone walks off with pens. The vulnerability is high because nobody monitors pens. The impact is low (pens are cheap), so there is little risk. It is more cost effective to order another box of pens than to track them or to try to prevent their theft.

Risk assessment is a decision-making step; based on impact, a decision can be made as to whether a countermeasure needs to be developed to deal with that specific vulnerability. The company has, after all, only limited resources, and it must spend them wisely.

Countermeasures. Countermeasures are designed to reduce risk, transfer it, or, at a minimum, make it tolerable. Companies should implement countermeasures on a priority basis, starting with those vulnerabilities that would have the greatest adverse impact if they were exploited.

Countermeasures don’t need to be exotic or expensive. They are often simply smarter ways to do a job, and a combination of simple changes will often do the trick. As an example, if you are concerned about the threat from camera-phones – and you should be – simply banning them from the premises (with proper notification), followed by consistently and strongly enforcing the measure whenever it is violated, will likely reduce the risk.

Another example would be buying an industrial shredder, which can shred everything you would normally discard. It costs little and eliminates Dumpster diving. To secure sensitive meetings when the mere knowledge of the attendees is revelatory, companies can hold meetings off site, in unusual places, or under different names.

Some countermeasures can be implemented by the company, while others may be done in conjunction with the company's consulting firm or other professionals. It may be necessary, for example, to have the company do an audit and evaluation of intellectual property. Or it may be necessary for the company to implement a document control system for certain categories of information, or to assign the company's IT department to subcontract monitoring and active response to network intrusions. Implementation of these systems and processes require the specialized consulting assistance of lawyers, accountants, IT experts, and other specialists.

Education. The easiest, cheapest, and most effective protection is education. Employee and participant education, combined with nondisclosure agreements signed at time of employment and vulnerability surveys of partner organizations, gives a company a strong base from which to work. All company employees from the CEO down, and all other participants in operations, must be educated on an ongoing basis in protecting company information so that they understand that company profits, and their jobs, may be lost through loss of information.

Everyone involved must understand their legal, ethical, and practical obligations and responsibilities. And they must understand what specific information is critical and shouldn't be revealed. They must also understand what to do if someone attempts to suborn or blackmail them. Special attention should be given to employees who deal with the public so that they know which of questions that may be posed to them by others are most likely to be legitimate and which are not.

Educating employees who generate or work with critical information is, of course, essential. But companies should never overlook their secretaries. Because they are the people who answer the phones, secretaries could create a major vulnerability if not educated about information protection.

Employees and participants should be told explicitly what types of information should not be revealed. They should be made aware of the ways that operatives can obtain information from public sources or forums and how these disparate, seemingly unimportant pieces of information, can collectively tell competitors a great deal.

While some information loss does come from subornation and espionage, which must be dealt with, most information loss, as noted, comes from open source material that the company makes available because it has not been identified as being critical. Employees and other participants are likely to

reveal information that has not been identified as critical; they will reveal it in conversations at trade shows, in social gatherings, or on the telephone.

In alerting employees to situations where they must be on guard, companies should remember to include less obvious collection venues, such as Internet chat rooms. The author was involved in one case in which employees innocently revealed valuable information in these online conversations because they wanted to be helpful and because the information had never been identified as critical.

Senior support. How well any program works will depend largely on the backing it has from senior management. Consider, for example, the experience of one company that was experiencing a rash of thefts. All of the thefts occurred overnight, so the president announced that no one would be allowed in the building after hours. One night, having forgotten an important document, the president went to the office. Despite his protestations, the security guard on duty would not let him in. The next day, he called the contract guard company and requested that the guard be promoted. This is the type of commitment and awareness that all of us should strive for.

Loss of information is a fact of life in today's business environment. But by taking the time to identify critical information, to educate employees and other participants to protect that information, and to bring in professionals to help prevent or deal with the problem, a company can move from a position of vulnerability into a position of strength and safety.

Richard Isaacs is Senior Vice President of The LUBRINCO Group, an international vulnerability management firm that specializes in protection of trade secrets and intellectual assets; international financial investigations and due diligence; and protection of management, family, and staff in high-threat environments. He is a member of ASIS International and also serves on the board of directors of the OPSEC Professionals Society.

Sidebar

How Information Thieves Work

There are many ways to find information from public sources or to set up situations where employees will unwittingly reveal critical company data. Here are a few examples.

Publicity. Companies often give out critical information when trying to garner publicity. For example, one company gave out so much information

about a new product through public relations and on its Web site that the competition could surmise the company's business plan.

Sales. Another area of trouble is the sales force. Marketing experts are paid to talk to people and to give out information that will lead to sales, and they often want to develop interest in products that have yet to reach the market. But those who give presentations often say more than they should. Similarly, attendees at trade show booths frequently discuss upcoming projects in more detail than necessary.

Socializing. Any social gathering, whether in a business setting, a sports bar, a health club, or an online forum, can be high risk. Operatives know that these are places where employees let down their guard. They may seek out sites where they know a company's staff congregates, for example, and over a period of time, gather considerable intelligence through casual conversations.

Schemes. To increase their chances of obtaining the information they seek, information thieves will sometimes employ tactics to fool employees into willingly giving information in a forum they do not perceive as a threat. For example, one company needed specialized information about a competitor's plans. The company created a nonprofit corporation seemingly unaffiliated with them. The nonprofit organization then sponsored a conference.

Invitations were sent to potential attendees and speaking invitations were offered to the competitor's key employees. The invitations to speak included an honorarium, as well as free transportation to, and lodging at, the conference.

The organization got the information it needed, and turned a profit at the conference to boot. This information gave the company a competitive advantage, and all the information was given freely and knowingly. Though this tactic has only been used once in the author's experience, it is an example of how far competitors are willing to go.

A more common scheme is to use job interviews to glean information. For example, the vice president of a technology company would scan job ads, then go on job interviews and pump hiring executives for useful information.

Other companies have created job ads so that they could interview people and obtain information. In those cases, the ads were sometimes so specific that only a few chosen people could possibly respond to them. The plans were successful. Specific projects were discussed including new technologies and project deadlines. After the company doing the

interviewing released a similar project ahead of the target company, the author was brought in to determine how the breach occurred. The author found out through investigation that no job existed and that the interview had been a ploy to get information.

Directory scouring. Another tactic the author has seen used by one recruiting firm is to dial every possible number in a company's exchange during the nighttime hours and listen to outgoing voice-mail messages. If people give their names, their job titles, and a little talk about where they are and what they are doing, the firm can get an internal directory of employees and a good idea of what is being done in the organization. Similar tactics might involve looking up personnel profiles on the company Web site.