CASE STUDY OF INDUSTRIAL ESPIONAGE THROUGH SOCIAL ENGINEERING

Ira S. Winkler
National Computer Security Association
10 South Courthouse Avenue
Carlisle, Pennsylvania 17013
winkler@ncsa.com
(717) 258-1816 x257

Abstract

The Federal Bureau of Investigation estimates that U.S. Corporations lose $100 Billion annually due to industrial espionage. While many people believe that the espionage is committed by well financed organizations that can only be stopped by national agencies, that is very incorrect. Industrial espionage usually exploits simple and very preventable vulnerabilities to produce tremendous results. By focusing on comprehensive security, and not just technical security, information security professionals can significantly hamper adversary attempts to steal their organization's information assets. The presentation that describes this paper presents a case study of an actual industrial espionage attack against a large U.S. corporation.

Introduction

The theft of sensitive information from U.S. corporations is the goal for many foreign nations and companies. Adversaries do not care about what form the information takes. Whether information is in electronic format or is thrown away in the trash, it is irrelevant as long as the information is compromised. Unfortunately for most corporate security programs, there is a preoccupation with technical security that leaves information very vulnerable to basic espionage methods.

Information security professionals focus their efforts on what they know best. When they allocate their limited budgets, the division of funds reflects their perceived needs, which are basically technical security mechanisms. Firewalls and other Internet security mechanisms are the hottest selling products. While firewalls go a long way in preventing the traditional computer hackers from intruding into a corporate computer network, they do nothing to stop the most significant source of computer crime: Insiders. Two recent studies show that insiders were responsible for more than 70% of information related thefts [1, 3]. The threat prevented by firewalls is minimal, because a focused attack will bypass the strongest protection mechanisms.

Information comes in many forms, and must be protected in all of its' forms. Information security is not computer security. While computer security is an integral part of a good security program, it is only a part. Comprehensive security includes physical, personnel, operational and technical security. Industrial spies know how to bypass any strong part of a security program to attack an organization at its' weakest point.

Industrial Espionage Methods

There are wide spread reports of former Soviet Bloc intelligence operatives acting as freelancers to the highest bidders, as well as foreign intelligence agencies refocusing their efforts on U.S. companies as opposed to the U.S. Government [4, 5, 7]. These intelligence organizations bring their tried and true methods with them. Unfortunately, most corporate security managers are not aware of the threats and the methods they employ. Intelligence gathering methods are more effective on companies than they are on governments, because companies do not have the appropriate countermeasures in place.

Legal Methods

There are several forms of industrial espionage that are legal. These methods include the purchase of companies or products, and has the net result of transferring technology to the previous competitor. There are many examples of foreign firms buying U.S. companies to acquire critical technologies. The threat to U.S. national competitiveness is very serious, however there is little that can be done by a corporate security manager to prevent this type of information acquisition [7].

Another legal method of acquiring U.S. technology involves pressuring companies into giving up their technology. Basically, this involves the blackmail of U.S. companies by foreign countries. In order for a company to do business in the foreign country, the company must train native workers in a critical technology. It is then up to the company to decide if the cost of doing business with the country is worth it. At this time, a corporate security manager may or may not be involved in the decision. Obviously from an information protection perspective, the answer is obvious. From a business perspective, it is much less clear [7].

The practice of joint ventures with competitors also provides a huge opportunity for U.S. companies to give up sensitive information. During the process of expanding the state-of-the-art, a company must divulge its' knowledge of the state-of-the-art [2, 7]. In some cases, a joint venture may be the only method for a company to enter a foreign market. Again, there is a Cost/Benefit Analysis to be performed prior to entering into such a venture.

Open source information (OSI) also provides a wealth of knowledge for industrial competitors. OSI takes a variety of forms including newspaper articles, corporate Annual Reports, patent filings, court papers, and marketing information. For example, most requests to review patent filings are by foreign nationals and third party research firms. By reviewing OSI, competitors can determine a tremendous amount of information about a company and their products. The losses are tremendous and unfortunate, especially when a company does not realize that they are giving away all of their information [7].

The hiring away of employees also results in the transfer of knowledge to a competitor. While many former employees do not intend to divulge sensitive information, the transfer of the knowledge is inevitable. In the performance of day to day activities, it is impossible not to take into account the knowledge that a person has developed. For example, if a person is trying to

price a job for their present company, it is impossible for them not to consider the pricing structure of their former employer, who is now competing for the same job.

Many companies use trade shows and conferences to elicit information from competitors. Typically, corporations send their researchers and marketing staff to these events to either stay abreast of the latest research or sell services or products. These people usually give out information better than they collect it. Companies involved with industrial espionage also send information collection specialists to these events. They usually act like potential customers or fellow researchers to elicit information from people that are all to willing to give it up. Through advanced training these collection specialists have perfected the art of drawing out as much information as possible [7].

Foreign countries make it a habit to contact natives of their country that have had contact with a targeted company. These natives are requested to divulge information that they have obtained from the company. It is typical for individuals to have more loyalty to their native land as opposed to a foreign company that they have worked for. These people are readily recruited by foreign intelligence services, and the knowledge that they divulge is quickly passed to foreign companies and countries. In some cases a foreign intelligence service may recruit a national to work for a U.S. firm. They will assist in obtaining a job for that person, and help in any way possible. The individual may not realize that they will be contacted at a later time to compromise information [7].

Illegal Methods

Many of the previous methods appear to border on criminal activity. It is a fine line between a foreigner divulging information to their native country and a U.S. citizen selling the information to that country.

Many industrial espionage cases involve the use of insiders to steal information. The cooperation of insiders can occur in many ways, depending on the circumstances. As with traditional espionage cases, the recruitment of moles is frequently used. Moles are employees of a targeted company, or someone with access to the company, that agree to cooperate with the criminals, usually in exchange for money. These people abuse the access that they have to steal information, or possibly just hand over information that they already have access to. They are well established within the target, and can typically move through the organization unchecked. Moles may be recruited by the industrial espionage organization, or may volunteer their services. It is not unheard of for people to approach their company's competitors to sell corporate secrets [1, 4].

The recruitment of a mole can be risky for an attacker, because there is the possibility that the potential mole might report an initial approach to corporate security personnel. For this reason, it is very likely that an industrial spy will attain their own position within the target. Large companies have an on-going recruitment process, and it is easy for spies to obtain a job. Once inside the company, they can abuse their access and usually go undetected in their thefts of information. Again, most companies are in the process of increasing their perimeter security mechanisms, but leave their internal system without protection [4].

There are less sophisticated, but still effective methods for stealing information. Espionage could involve breaking into buildings and offices to steal the desired information. Industrial spies will go through locked and unlocked office spaces, search file cabinets, examine unprotected computer systems, etc. If a person knows where the targeted information is located, it could be extremely profitable for them to commit a simple break in. Spies will also go through trash dumpsters and other garbage containers to gather information. While many people think that this is ridiculous, it is extremely effective [4, 8].

If a company has people that travel frequently, it is very possible that their travelers could be the subject of sophisticated surveillance efforts. U.S. executives have reported that their hotel rooms appear to have been searched, that their telephone calls have been monitored, etc [7]. The value of the information that they know, ultimately drives their risk of being watched by adversary organizations.

I have left the discussion of technical collection methods for last, not because it is unimportant, but because the focus on technical countermeasures causes major security vulnerabilities with regards to the other information security disciplines. Industrial spies can collect information by computer hacking, tapping telephones, sophisticated cryptanalysis efforts, etc. There should be dozens of other papers at this conference describing technical intrusion methods in detail. Industrial spies use all known methods of technical information collection. Due to the effectiveness of currently known methods, it is unlikely that they have to develop any new methods.

Clearly, computer intrusions can yield a tremendous amount of sensitive information, however it is the goal of this paper to stress that it does not matter how much information an industrial spy ring obtains, but what information they obtain. A single document can be worth billions of dollars, and it does not matter if the information is found in a computer or in the garbage [4, 8]. In many cases acquiring terabytes of data can hinder the collection of a single document, because of the difficulty of data reduction.

Preventing Industrial Espionage

Since the methods used by industrial spies are the same as those used by traditional spies, the countermeasures used to prevent traditional espionage can prevent industrial espionage [7]. There is a great deal that commercial organizations can learn from Department of Defense security practices. While I am not advocating total adherence to DoD standards, companies must employ a level of countermeasures that are justified by the potential losses that the company can suffer. For many firms, the potential losses can easily be valued in the billions of dollars. Information security efforts must therefore address comprehensive countermeasures, that are as comprehensive as the methods employed against them. There are four parts of a comprehensive security effort that enhance and support each other: Technical, Operational, Physical, and Personnel Security. This paper introduces the concept of comprehensive security. It is strongly recommended that other papers follow up on the following concepts.

Technical Security

Technical security countermeasures reduce the vulnerabilities present in electronic systems. As many other papers at this conference address, countermeasures ensure the confidentiality, integrity, and availability of computer systems and networks. A good technical security effort also protects other electronic systems such as voice mail. The technical issues are well known and are satisfactorily addressed elsewhere.

Operational Security

Operational security addresses the business processes in use by a company that could compromise information through non-technical means. For example, the DoD policy concerning information access only on a "Need to Know" basis helps prevent the unnecessary proliferation of information. Likewise, policies on restricting the use of open communication lines, such as the Internet and telephone systems, reduces the potential for the compromise of information. Other operational security issues include enforcing your own security policies on your vendors and suppliers. It would make no sense to perform background checks on your own employees, while contractor employees, who have free access to your facilities, go unchecked.

Operational security is a complicated issue, and requires a thorough study of the way a company does business. This includes the marketing progress, which presents a major vulnerability due to the exuberance a sales people trying to close a deal by offering sensitive information. Companies must examine the entire research, development, manufacturing, and sales process for potential ways that information could be compromised. There must be a clear understanding of who to disclose information to, and under what conditions and controls.

A strong security awareness program is the foundation for a strong operational security program. People must know what information they should protect, and specifically how to protect it. Everyone should be encouraged to report any questionable circumstances, and know who to report it to. Security managers cannot assume that security issues are common sense when there is no baseline for common knowledge. Operational security issues must be further elaborated and studied in other forums.

Physical Security

As previously discussed, a large number of information compromises occur due to simple breaking and entering, and theft. Physical access to facilities should be carefully regulated and controlled. This includes limiting the access of visitors and contractors, as well as your own employees. Nobody should have a free roam of all corporate facilities.

All employees must wear access badges that indicate their status, such as employee, temporary, visitor, or contractor. This feature helps to reduce the threat of people overstating their authority. Obviously, there should be an operational security policy that encourages all people to look at badges. Another physical security issue to be addressed is the control of garbage. There have been numerous incidents of serious information compromises that have occurred solely from the

content of an organization's garbage. The U.S. military has several units devoted to trash intelligence, and invests millions of dollars in the proper disposal of classified waste. Companies that have very high value information must also consider the control of their garbage.

Security programs must also stress the use of available protection mechanisms. Locks on office doors and file cabinets frequently go unused in many organizations. Clean desk policies, that require all sensitive information to be locked up, must also be enforced. There are also computer locking products available that prevent computer access if it is turned off or idle for a certain period of time. These products prevent the exploitation of computers that are not properly turned off when not in use.

Personnel Security

There must be a thorough investigation of all people with potential access to sensitive information. Since most information might be sensitive to different departments within an organization, it should probably be a blanket policy to have a background check performed on all employees. The term employees is used broadly to include anyone with physical access to facilities or information. Facilities include any computer terminal that has access to corporate information.

Many organizations do not consider the access and opportunities that seemingly minor employees, such as janitors, clerical workers, and security guards, have to steal information. A recent edition of *2600: The Hacker's Quarterly* had an article on how to obtain a job as a janitor [6]. Criminal elements understand the potential of low level positions, and it is time for security managers to address that potential.

Systems administration staff should also establish a strategic relationship with the Human Resources department. It is critical to be aware of any pending employee departures that could be under less than amicable circumstances. Also, systems administrators must lock the accounts of departed employees on the day that they leave the company.

Case Study

The case study for the presentation addresses a penetration test performed against a large high technology firm at their request. The goal of the test was to simulate an industrial espionage attack, within the funding parameters. A comprehensive attack strategy was used to simulate an attack as accurately as possible. The attack included the use of Open Source Research, obtaining a position as a temporary employee within the target, misrepresentation of responsibilities by the temporary, abuse of physical access, internal hacking, internal coordination and facilitation of external hackers, and straight external hacking.

The results were staggering. Within one day of the on-site activities, over $1,000,000,000 of information was "stolen." While the firewall was impenetrable and Smart Cards prevented access from outsiders, information was compromised almost at will by an insider. This was accomplished in a company that has a tremendous technical security program. The security

manager understands their vulnerabilities, and wanted an independent assessment of the vulnerabilities to demonstrate the seriousness of the problem. A detailed description of the case study will be presented.

Conclusions

There is a tremendous focus by information security professionals on technical security. This is probably due to the traditional background of information security professionals being from a technical background. When they receive funding for their efforts, their initial reactions are to spend the money on what they are most familiar with, which usually does not include awareness programs or the acquisition of shredders. Firewalls and other security tools are important, but unfortunately they only address a small part of the problem. All recent studies show that insiders pose the most serious threat to information, and firewalls do little to prevent the abuse.

It is time for commercial information security professionals to realize that information security is more than computer security. A comprehensive security program that includes all security disciplines is the only effective countermeasure to a coordinated industrial espionage attack. A determined attacker will exploit the most vulnerable access points, and will not stop trying until they get what they want or are caught. A detailed and continual awareness program is the best method to deter many attacks. If all employees know what to look for, then the chances for the attack to be successful are minimized.

Bibliography

1. American Society for Industrial Security (1996), *Study on the Theft of Proprietary Information*, Arlington, VA: ASIS.

2. Cox, J. (1996), Siphoning U.S. Companies' Knowledge, *USA Today*, February 16, p. B1.

3. Katz, A. (1995), *Computers: The Changing Face of Criminality*, Unpublished dissertation: Michigan State University.

4. Pasternak, G. (1996), The Lure of the Steal, *U.S. News & World Report*, March 4, p. 45.

5. Schweizer, P. (1993), *Friendly Spies*, New York: Atlantic Monthly Press.

6. Voyager (1994), Janitor Privileges, *2600: The Hackers' Quarterly*, 11(4).

7. White House (1995), *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage*, Washington, DC: Government Printing Office.

8. Winkler, I. (1996), Assignment Espionage, *InfoSecurity News*, 7(3), p26.