GIAC
CERTIFICATIONS

# Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

## Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

# CORPORATE ESPIONAGE 101




**Shane W. Robinson**
**Version 1.3**

## INTRODUCTION

Psssst! Hey, buddy….wanna buy a trade secret?

Information can make the difference between success and failure or profit and loss in the business world. If a trade secret is stolen, then the competitive playing field is leveled or worse,

© SANS Institute 2000 - 2005 Author retains full rights.

tipped in favor of the competitor. To complicate the problem even more, trade secrets are not only being sought after by a company's competitors, but from foreign nations as well. They are hoping to use stolen corporate information to increase that nation's competitive edge in the global marketplace.

Although a lot of information gathering is accomplished by combing through public records, i.e. public databases, and patent filings; however, the best way to get the really good information is by taking it. This paper discusses the various aspects involved in the 'taking' of corporate information. It covers some background information on corporate espionage, who is doing the spying, how it is being done, a few real life examples, and some guidelines to follow in order to protect a business from becoming a victim.

## JUST HOW BAD IS IT?

Corporate espionage is a threat to any business whose livelihood depends on information. The information sought after could be client lists, supplier agreements, personnel records, research documents, prototype plans for a new product or service.[1] Any of this information could be of great financial benefit to a scrupulous individual or competitor, while having a devastating financial effect on a company. Just about any information gathered from a company could be used to commit scams, credit card fraud, blackmail, extortion or just plain malice[2] against the company or the people who work there. A customer lists, for example, could be sold to a competitor or used by a sales person to start his own company; thereby effecting the profitability of the victim company.

Corporations are implementing technology faster than they can defend against ways it can be used against them. As corporate infrastructures become more open and complex to handle more sophisticated applications, remote customers and users, remote offices and telecommuters, corporations will become more susceptible to intrusions and information theft. Despite the potential risks, security is usually an afterthought to most companies. Few companies spend the money needed to train personnel or to purchase hardware and software needed to monitor and protect their computers and networks. The reasoning behind businesses not spending money on security is because they do not like to spend money on a problem that they do not think they have.

In 1999, Fortune 1,000 companies lost more than $45 billion from the theft of trade secretes, according to a survey by the American Society for Industrial Security and Price Waterhouse Coopers.[3] Today, theft of trade secrets is estimated to be around $100 billion. Finding accurate statistics on corporate espionage is impossible, because no company wants to admit that it was a victim of trade secret theft. Companies do not usually notify the authorities, because they are frightened that admitting to a security breach will cause its stock prices to plummet or a major deal or negotiation to fall through. Banks are notorious for not reporting computer or network security breaches, because they do not want the federal government noseying around their systems or questioning their policies and practices. Small businesses do not report incidents of corporate espionage for fear that their trade partners will not do business with them if they find out that their partner's systems are not secure.

© SANS Institute 2000 - 2005 Author retains full rights.

## THE SPY WHO HACKED ME:

Corporate spies, infiltrators or hackers can be classified into two basic categories, insiders and outsides. Insiders are usually employees: executives, IT personnel, contractors (programmers, network penetrator or computer auditors), engineers, or janitors who have legitimate reasons to access facilities, data, computers or networks. A frequently quoted statistic states that employees commit 85% of corporate espionage crimes. Think of the possibilities. Insiders have immediate access to enormous amounts of valuable company information and can misuse their privileges or impersonate someone else with higher privileges to plant a Trojan, copy information, or to taint research data. The basic reasons for insiders to "sell out" to a competition are: lack of loyalty, disgruntled, boredom, mischievousness, blackmail, and most importantly, money.

Outsiders are spies, attackers, or hackers who enter from outside a company. Since the end of the Cold War, a number of countries have been using their intelligence-gathering capabilities to obtain proprietary information from many of America's major corporations too. Outsiders can enter from the Internet, dial-up lines, physical break-ins, or from partner (vendor, customer, or reseller) networks that are linked to another company's network.[4]

A kite is a special type of outsider, an expendable contractor. A kite provides his clients with actionable intelligence that they either do not know how to get or do not want to get caught collecting it themselves. A kite also provides plausible deniability to his or her clients. If a covert operation is discovered and there is litigation or a criminal charge, the hiring company can deny all responsibility by denying all knowledge of the kite's actions, like cutting the string to a kite and letting it fly away by itself. A company can claim ignorance by demonstrating in court that the "consultant" signed a contract saying that he would abide by all ethical rules, and that the company had no idea what the "consultant was doing.[4]

> An increase in unemployed intelligence officers since the Cold War ended and the proliferation of advanced technology has made corporate spying much easier. Dr. Robert Ing, author of Improvised Technology in Counter-Intelligence Applications, says that "instead of missile launch codes, the new targets of choice are technological and scientific data concerning flat-panel TV, electric cars, new computers, competitive strategies and innovative manufacturing/distributing processes."[1]

Because people are naturally lazy and take what they read for granted, it is easy to fake credentials and gain employment in a targeted company. With a fake resume, a 'paper' certification, and an instant degree from a fictitious college purchased off of the Internet, any one can create the identity of their choice.

At (Removed to protect the guilty since they have since adjusted their degree programs) University[5] anyone can buy an instant verifiable degree of their choice from the fictitious school

© SANS Institute 2000 - 2005 Author retains full rights.

of their choice. For example, you can purchase the following degrees:

- Associate for only $450
- Bachelor for only $550
- Master for only $655
- Doctorate for only $995
- Combination Bachelor/Master for only $1100
- Combination Master/Ph D for only $1,600
- Combination Bachelor/Master/Ph D for only $1,895

With each degree purchase, a person can also:

- Make up the name of the university or college
- Backdate the graduation date on the diploma
- A printed transcript is provided with each degree purchased. It shows representative courses that correspond to experience as compared to a traditional classroom setting. A person can define the course dates, grades and grade point average.
- The diplomas are professionally printed on parchment paper, with a raised gold seal, and placed in a diploma holder. "They are beautiful and ready for display."
- Transcript verification service

**SPOOK TOOLS AND METHODS:**

Computers, LANs and the Internet have made the theft of trade secrets very easy. In today's information age, a thief does not always have to break into an office and steal a briefcase full of documents. With the abundant use of technology, a thief can copy digital information onto a floppy or email it across the Internet to an anonymous Hotmail account for retrieval at a later time. As the old saying goes, information is power and power is money, and in the corporate world there is an enormous amount of information. Obviously proprietary information like secret formulas, manufacturing schematics, merger or acquisition plans, and marketing strategies[1] all have tremendous value and are targets to cyber thieves.

Companies can expect an intruder to enter through the path of least resistance. A majority of the times this path is right through the front door. As more and more companies are promoting a casual atmosphere for their employees, they are overlooking establishing and implementing proper security procedures. Security guards are rarely posted in many companies' lobbies, office doors are left unlocked, and computers are usually left unsecured or lack intrusion safeguards. [6] A lack of security and training allows an attacker to use a variety of techniques to gain access to a company's vital information.

© SANS Institute 2000 - 2005, Author retains full rights.

Some techniques for accessing valuable corporate information include: physically removing the hard drive and copying the information to another machine, hacking, dumpster diving, social engineering, bribery, hiring away key employees, and the list goes on.

## Hacking

Hacking is considered one of the top three methods for obtaining trade secrets, and it is only increasing in popularity. There are two main reasons why hacking is on the rise: (1) the enormous availability of hacking tools. Currently, there are over 100,000 websites that offer free downloadable, and customizable hacking tools. (2) Hacking is relatively easy to do. There are tools available that require no in depth knowledge of protocols or IP addressing, they are almost as easy to use as point and click.

Hacking can be broken up into three categories: system, remote, and physical.

System hacking assumes the attacker already has access to a low level, privilege user account on the system. If the system does not have the latest security patches and correct security settings, there is a good chance the attacker will be able to use a known exploit to gain administrative privileges.

Remote hacking involves an attacker attempting to penetrate a system remotely across the network or Internet. The attacker usually begins with no special privileges, and tries to obtain higher level or administrative access. There are several forms of this type of hacking: unexpected input, Buffer overflows, default configurations, and poor system administrator practices.

Physical hacking requires the attacker to personally enter a facility. Once inside, the intruder can:

- Roam the building searching for a vacant office or unsecured workstation with an employee's login name and password lying around;
- Search for memos or unused letterhead, and then insert the fake documents into the corporate mail system;
- Attempt to gain physical access to a server or telephone room in order to gain more information on the systems in use;
- Look for remote access equipment and note any telephone numbers written on the wall jacks;
- Place a protocol analyzer in a wiring closet to capture data, user names, and passwords;
- Steal targeted information or hardware containing targeted information.
- Attach a hardware keystroke logger between the keyboard cable and the keyboard port on a user's workstation. Hardware keystroke loggers do not require drivers, uses no system resources, works on all PC operating systems, installs in seconds, and they do not send alerts to administrators. However, they do record a user's keystrokes character by character until the logger is disabled. When a password is

© SANS Institute 2000 - 2005, Author retains full rights.

entered, the logger allows access to the recorded keystrokes.[7] Keystroke loggers have recording capabilities ranging in sizes from 8k (8,000 keystrokes) to 64k (more than 65,000 keystrokes). A keystroke logger can be used to record:

1. E-mail compositions
2. Instant Messaging
3. Chat room activity
4. Web URL's
5. User names and passwords
6. Anything else a user types

## Social Engineering

Social engineering is another popular method of obtaining valuable corporate information. The basic goals of social engineering are the same as hacking in general: to gain unauthorized access to systems or information in order to commit fraud, network intrusion, industrial espionage, identity theft, or simply to disrupt the system or network. Social Engineering is the tricking of a person into revealing their password or other valuable coporate information. Even not-so-casual conversations with unsuspecting relatives of company executives have become conventional tools in corporate espionage.

A classic social engineering trick is for an attacker/hacker to send email claiming to be a system administrator. The hacker will claim to need user's password for some important system administration work, and ask the user to email it to him/her. A hacker will usually send this email message to all the users on a system, hoping that one or two users will fall for the trick.

Another common social engineering trick is "shoulder surfing", someone looking over an employee's shoulder while he or she types in a password. Password guessing is an additional easy social engineering technique. If a person can find out personal things about other people, he can usually use that information to guess a password. For example, the names of children, their birthdays and anniverseries or social security number are all likely candidates for guessing as passwords. [8]

## Dumpster Diving

Dumpster diving is a messy, but a very successful technique for acquiring trade secretes and other valuable information. No matter how disgusting dumpster diving sounds, it is legal. Once trash is discarded onto a public street or alley, it is considered fair game. "The courts have held that if it is left to be accessed by commercial carters, then it is no longer private property. It is only private property if there is a 'no trespassing' sign and you had to trespass to get into the dumpster."[4]

The LAN Times listed the following items as potential security leaks in corporate trash: company

© SANS Institute 2000 - 2005, Author retains full rights.

phone books, organizational charts, memos, company policy manuals, calendars of meetings, events and vacations, system manuals, printouts of sensitive data or login names and passwords, printouts of source code, disks and tapes, company letterhead and memo forms, and outdated hardware.

Trash can provide a rich source of information for any corporate espionage agent. Phone books can give a hacker names and numbers of people to target and impersonate. Organizational charts contain information about people who are in positions of authority within the organization. Memos provide small amounts of useful information for creating authentic looking fake memos. Policy manuals show hackers how secure and insecure a company really is. Calendars can tell an attacker which employees are out of town at a particular time. System manuals, sensitive data, and other sources of technical information may give an attacker the exact information he needs to access the network. Discarded hardware, particularly computers with hard drives, can be restored to provide all sorts of useful information.[9]

## Whacking

Basically, whacking is wireless hacking. To eavesdrop on a wireless networks, all an intruder needs is the right kind of radio, and to be within range of a wireless transmission. With the wide usage of 802.11b devices, it is possible to pick up signals from outside an office building. Once tapped into a wireless network, an intruder can easily access anything on both the wired and wireless networks, because the data sent over networks is usually unencrypted. [10]

If a company is not using wireless networking, an attacker can pose as a janitor and insert a rogue wireless access node into a supposedly secure hard-wired network. Once the WAP, wireless access point, is installed, an intruder can safely sit outside an office building with a laptop and a wireless NIC, and leisurely sniff and explore a company's network looking for weaknesses and information to exploit. If the WAP is discovered, it will most likely be mistaken for a hub or Jet direct box.

## Phone Ease Dropping

Ease dropping on phone transmissions is yet another tool in the game of corporate espionage. A person with a digital recording device can monitor a FAX line and record a FAX transmission and reception. By playing the recording back into a modified Group III or Group IV FAX machine, an intruder can reproduce an exact copy of a message without anyone's knowledge. Even without monitoring a FAX line, a FAX sent to a "communal" FAX machine can easily be read or copied before it picked up from the incoming FAX basket for delivery to the intended recipient. [11]

By picking up an extension or by tapping a telephone, it is possible to record the tones that represent someone's account number and password using a tape recorder. The tape recording could be replayed over the telephone to gain access to someone else's account.

© SANS Institute 2000 - 2005 Author retains full rights.

## THE MISSION: Information Retrieval

Now that we have the players and the tools, what types of information do corporate spies seek? Basically any digital or hardcopy date can be valuable to competitors. The more information a competitor can gather, the clearer picture is painted of a firm's actions, plans, operations and strategies. Ultimately, the goal is to outmaneuver a company and gain a competitive advantage.

A few of the information targets competitors seek out include the following:

- Marketing and new product plans
- Source code
- Corporate strategies
- Manufacturing, technological operations
- Target markets and prospect information
- Plant closures and development
- Usual business methods
- Product designs, research and costs
- Alliance and contract arrangements: delivery, pricing, terms
- Company Websites
- Customer and supplier information
- Merger and acquisition plans
- Financials, revenues, P&L, R&D budgets
- Marketing, advertising and packaging expenditures
- Pricing issues, strategies, lists
- Staffing, operations, org charts, wage/salary

Besides proprietary company information, personnel records are also hot targets for pilfering. Any of the following information could be of value to the right person or company:

- Home addresses
- Home phone number
- Names of spouse and children
- Employee's salary
- Social security number
- Medical records
- Credit records or credit union account information
- Performance reviews

© SANS Institute 2000 - 2005, Author retains full rights.

**EXAMPLES OF CORORATE ESPIONAGE:**

### Case #1

Two large companies were bidding on a $900 million contract. One company hacked into the other's network and downloaded e-mail related to the bidding. The hacking company then underbid its competitor, and won the contract. The hacked company discovered the penetration weeks later, and only because an audit was under way at the time of the attack and discovered the hacker's actions. [11]

### Case #2

An employee, a hacker, of a medical company, used a DOS attack to overwhelm a competitor's server. Once the server was downed, the hacker uploaded a Trojan. The Trojan then silently sniffed the network for passwords and stored them in a secret file. The hacker used the information accumulated in the secret file to gain access to its competitor's e-mail system, obtain a database password, and then download pricing information. The rival company then used the pricing information to undercut its competitor. [12]

### Case #3

A French defense contractor knew its designs were being leaked outside the company despite the company's safeguards on how digital information could leave the premises. A hacker, working as part of a team, had obtained a job inside the defense company. He then began using steganography to embed trade secrets inside of images, which were then posted on the company's public website. The second team member then stole the trade secrets right off the company's home page. [13]

### Case #4

A group of strangers walked into a large shipping firm and walked out with access to the firm's entire corporate network. They accomplished this by obtaining small amounts of access from a number of different employees in that firm. First, they did research about the company for two days before even attempting to set foot on the premises. For example, they learned key employees' names by calling HR. Next, they pretended to lose their key to the front door, and a man let them in. Then they "lost" their identity badges when entering the third floor secured area, smiled, and a friendly employee opened the door for them.

The strangers knew the CFO was out of town, so they were able to enter his office and obtain financial data off his unlocked computer. They dug through the corporate trash, finding all kinds of useful documents. They asked a janitor for a garbage pail in which to place their contents and carried all of this data out of the building in their hands. The strangers had studied the CFO's voice, so they were able to phone, pretending to be the CFO, in a rush, desperately in need of his network password. From there, they used regular technical hacking tools to gain super-user access into the system.

Fortunately in this case, the strangers were network consultants performing a security audit for

© SANS Institute 2000 - 2005 Author retains full rights.

the CFO without any other employees' knowledge. They were never given any privileged information from the CFO but were able to obtain all the access they wanted through social engineering. [14]

### Case #5

A high-ranking executive was on the road with a laptop computer. The laptop was loaded with the company's latest and most vital activities. The laptop was left in the hotel room while he was at dinner. A competitor's 'consultant' walked into the room as though he was the occupant while the maid was turning down the bed. Once inside, the kite booted the laptop, copied all the data contained on the hard drive and left the room without leaving a clue he was ever there. His partner was keeping an eye on the executive while he dined. If the target left unexpectedly, he simply used his cellular phone to call his partner to abort the mission. [15]

## DEFENSIVE STEPS

So how can a company protect itself from corporate espionage? The basic first line of defense against any form of corporate espionage is a two-pronged approach, controlled access and knowing your employees and customers.

### Controlled Access

Protect the most critical data by encrypting it. If it is encrypted and it is stolen it will be useless to anyone. If your network is on the Internet, use a firewall and audit the servers for security holes on a regular basis. Also make sure that the operating system has all of the latest security patches and fixes installed. [1]

Sensitive information about your business should never be stored on a networked computer. Instead, it should be kept on a stand-alone computer with no connection to any other computer or telephone line. This computer must be kept in a separate locked office or room at all times. Secure the room by using quality deadbolt locks and steel clad doors, adequate lighting, and install a monitored alarm system in the room. Allow only those who need to know or use the sensitive information to have access to the room.

Make sure to install anti-virus and password security software on the secured system. This computer should be checked for viruses on a weekly basis and the password used to access sensitive files should be changed just as often. The computer hardware should be locked or bolted down to a very, large piece of furniture or to the floor or wall. It is also advisable to place a disk drive lock over the disk drive bays of the computer to stop anyone from making a copy of files onto a floppy[1], or worse, inserting a disk and placing a virus in the computer.

It is recommended that companies review security measures in sensitive areas of their operations such as research and development. Educate traveling executives who carry company laptops about using precautions to prevent theft and examine communications with overseas facilities

© SANS Institute 2000 - 2005 Author retains full rights.

with an eye toward installing commercially available encryption that is extremely hard to crack.

### Knowing Personnel

Knowing employees means verifying the backgrounds of new employee applicants or employees assigned to work on sensitive projects. When hiring new employees in sensitive areas or who will have access to sensitive data, do a thorough background check. Call all of the references the prospective employee provides and then call the human resource departments of his or her last few jobs and ask for additional references. Confirm that they are who they say they are and not an undercover operative looking to photocopy company secrets for profitable sale to your competitor. [1]

> Most of the Big Five accounting firms have set up in-house forensic investigative practices within the past five years. "It's only in the last couple of years that these types of due diligence investigations have really become accepted," says Lisa Dane, manager in the forensic and corporate investigations practice at Deloitte & Touche in New York says that she catches a job candidate lying about his or her credentials at least once a month. "People have claimed to receive degrees from Harvard and Stanford Business Schools - some have attended and some have never attended at all," she says. [16]

In addition to controlling access to sensitive areas and data, and verifying people are whom they say are, following this basic security to do list will help to defend against corporate espionage:

1. Lock all doors. Computer passwords alone won't keep determined infiltrators from stealing.
2. Encrypt sensitive computer files.
3. Cross-shred all paper documents before trashing them.
4. Secure all dumpsters and post 'NO TRESPASSING' signs.
5. Conduct routine security awareness training for all employees
6. Do not discuss company secrets in unsecured environments.
7. Do not assume consultants or outsourcers are working on your behalf.
8. Require that all visitors be escorted at all times.
9. Instruct employees to report any repair people that show up without being called, and to not grant access to equipment until the workers' identities are established.
10. Keep wire closets, server rooms, phone closets, and other locations containing sensitive equipment locked at all times.
11. Keep an inventory of the equipment that is supposed to be in each server room, wire closet, and so on. Periodically check for extra or missing equipment.
12. Make sure all discarded magnetic media is erased; data can be retrieved from formatted disks and hard drives.
13. If possible, place locks on computer cases to prevent hardware tampering

© SANS Institute 2000 - 2005 Author retains full rights.

14. Configure the BIOS to boot from hard drive only, and if the BIOS will support it, enable the setup password to prevent someone from altering the boot sequence.
15. Never leave a voice mail message or e-mail broadcast message that gives an exact business itinerary or names and telephone numbers of clients where you can be reached.
16. Use code numbers or names when using two-way radios or pagers.
17. Institute a security policy for your company network and use it. Train all of the employees on safe computing practices. Teach them how to keep their data and computers safe from unauthorized access.

## REFERENCES


1. Ing, Dr. Robert. "IMPROVISED TECHNOLOGY IN COUNTER-INTELLIGENCE APPLICATIONS." http://www.pimall.com/nais/n.cntint.html (29 Jan 02)

2. Williams, Jim. "Infowar: Corporate Hacking." 25 Jan 99. http://netsecurity.about.com/library/weekly/aa012599.htm (26 Jan 02)

3. Edwards, Cliff. 18 Dec 00. http://abcnews.go.com/sections/tech/DailyNews/transmetaspy000701.html (28 Jan 02)

4. Mokhiber, Russell and Weissman , Robert. "Corporate Spooks." 6 Mar 01. http://www.commondreams.org/views01/0306-03.htm (24 Jan 02)

5. (This site has since revised their web page.)

6. Edwards, Cliff. "High-Tech Spy vs. Spy."

7. Sweet, Michael. "Whose Shoulder Are You Looking Over?" Jan 02. http://www.smartcomputing.com/editorial/article.asp?article=articles/2002/s1301/15s01/15s01.asp (04 Feb 02)

8. Armstrong , "Social Engineering." Del. 25 Oct 96. http://www.seas.rochester.edu:8080/CNG/docs/Security/node9.html (28 Jan 02)

9. Berg, Al. "Cracking a Social Engineer." 6 Nov 95. http://packetstorm.decepticons.org/docs/social-engineering/soc_eng2.html

10. Nelson, Matthew G. "Wireless Goal: Don't Get Whacked." 9 Jul 01. http://www.informationweek.com/story/IWK20010705S0013 (28 Jan 20)

11. http://www.knowledgekeepers.com/main.asp (1 Feb 02)

12. McKay, Martha. "Corporate spies find they can hack it." 20 Feb 00. http://www.tbicentral.com/articles/article00110.asp (6 Feb 02)

13. "The untold tally of 'Netspionage." 11 Sep 01. http://zdnet.com.com/2100-11-523788.html (25 Jan 02)

14. http://www.securityfocus.com/infocus/1527

15. Consol, Mike. "Industrial Espionage." 7 May 99. http://www.forensics-intl.com/art9.html (6 Feb 02)

16. Dodes, Rachel L. "The Public Face of Private Investigation." Nov 00.


© SANS Institute 2000 - 2005, Author retains full rights.

http://www.bizforward.com/wdc/archives/2000-11/management (1 Feb 02)

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.