Interested in learning more about security?

# SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

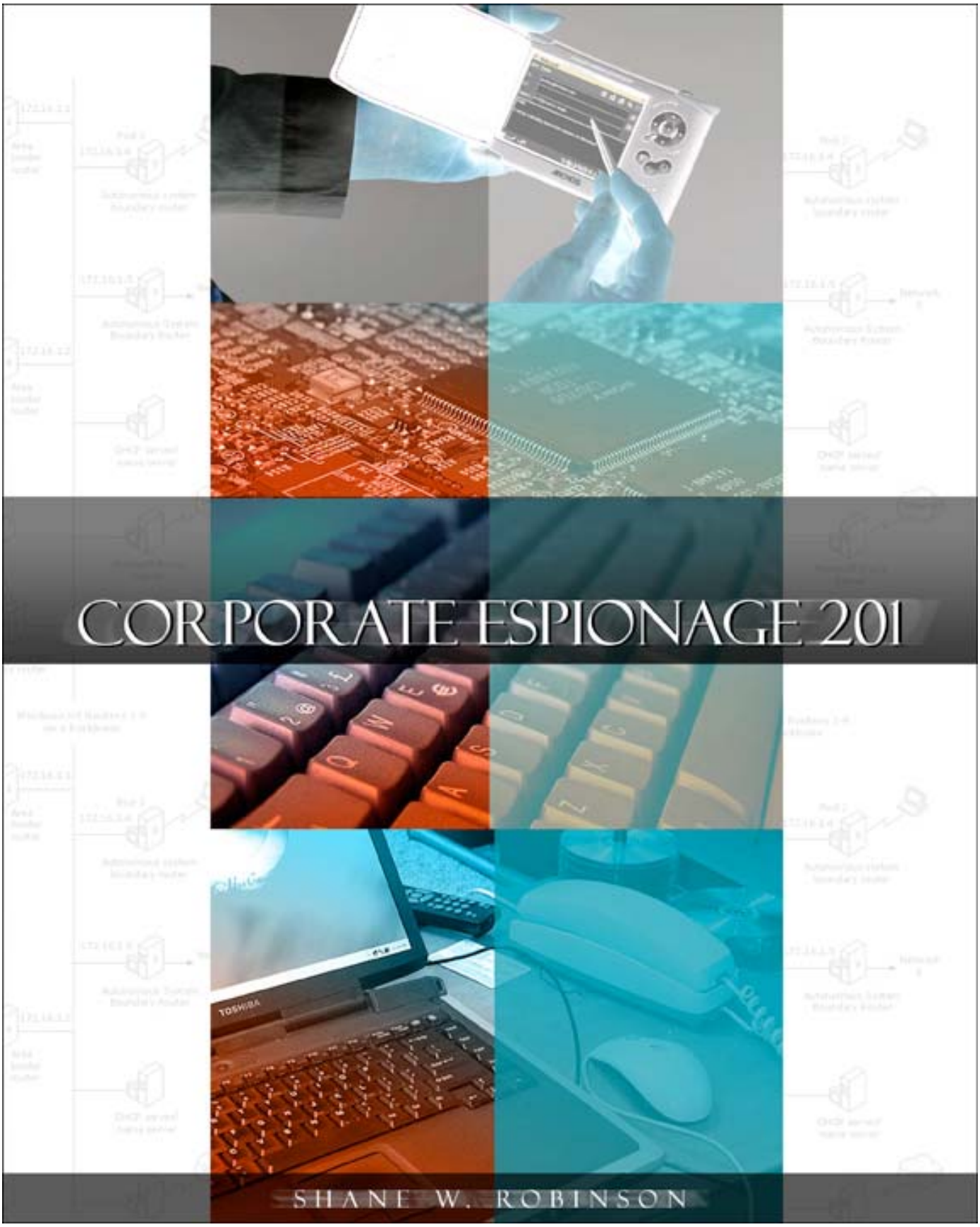
## Corporate Espionage 201

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.

Copyright SANS Institute

Author Retains Full Rights

AD




Version 1.0



© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

## INTRODUCTION

Jackpot! The payoff? Enormous caches of valuable data consisting of:

- Client lists
- Trade Secrets
- Expansion plans
- Marketing plans
- Personnel records
- Production processes
- Confidential financial data
- Customer billing information
- R&D blueprints for new technologies

The increasing high stakes game of corporate espionage is being played by individuals, corporations and countries worldwide. These players will use any ethical, and in most cases, any unethical, means to acquire data that will give them a competitive or financial advantage over their competition. The level of seriousness and dedication of these players for the game of corporate espionage is evident by the estimated $2 billion that they spent to spy on each other in 2004, according to the Society of Competitive Intelligence Professionals (SCIP).[1]

To gain an advantage over their competitors, many corporations are hiring ex-military and government agents trained in the art of spying -- I mean 'intelligence gathering techniques'. These skilled individuals are used to head new company divisions whose mission is to spy on and obtain information from competitors under the guise of competitive intelligence.

In 1999, it was estimated that companies lost more than $45 billion to theft of trade secrets and other valuable corporate data.[2] Today's total losses are anyone's guess. The lack of quantifiable losses can best be explained by the ***2005 Computer Crime and Security Survey*** conducted by the Computer Security Institute and the FBI. The survey states that the reporting of computer intrusions and data loss has continued to decline over the past few years due to companies' fears of negative publicity.[3] Additional reasons for their lack of disclosure could be to avoid public humiliation or class-action lawsuits. So companies try to keep incidents hush-hush while they try to correct security flaws.

Once proprietary information is in the hands of a competitor, it becomes very easy for them to start eating away at their rival's profit pie by manufacturing counterfeit products. In 2005, Custom and Border Patrol agents alone seized 220 shipments of counterfeit computers and related hardware (keyboards, chips, monitors, routers, memory sticks and flash drives) with a value of $4.8 million. This is considered a drop in the bucket compared to the global market for counterfeit products: pharmaceuticals, clothing, cosmetics, mechanical parts, IT hardware, etc. As a result of counterfeit products, U.S. businesses lose $200-$250 billion in revenue and 750,000 jobs annually.[4]

To save money and increase profits from losses to competitors, many corporations are opening offices and factories abroad, in addition to outsourcing certain business functions overseas. This practice is akin to putting the fox in charge of the hen house. According to J.J. Smith of the Society for Human Resources Management, there has been an increase in the theft of personnel records from companies in India alone. Foreign corporations hope to gain a competitive edge by poaching key personnel in hopes of obtaining trade secrets, business and process information.

This paper discusses the various techniques and technologies used by corporate spies, spooks and competitive intelligence professionals to obtain OPD (other people's data), suggested countermeasures, and real life cases of those individuals who have been caught stealing OPD.

## HOW IT'S DONE

The following is just a small sample of the technical and non-technical methods by which a corporate spy or disgruntled employee can get his hands on OPD.

### It's All There in Black and White

Most organizations have done a pretty good job of securing their networks and workstations. They have implemented a strong password policy, filter emails and attachments for proprietary information being sent out of the


© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

organization, and have even encrypted their most valuable data from unauthorized access. However, the Achilles heel for most organizations is the network printer. Most corporate security measures are rendered impotent once a user sends a document containing trade secrets to the network printer: someone walks by and takes it before the user can walk down the hallway and around the corner to retrieve the document.

To protect printouts from falling into the wrong hands, organizations can install a biometric device, like Silex Technology America's SecurePrint.[5] Devices such as SecurePrint hold a document in the local print queue until the sender goes to the printer and places his finger in the biometric fingerprint scanner. Once the person has been authenticated, his print job proceeds. This ensures that the sender of the document is right there to retrieve his document before anyone else does.

**Oldie But Goodie**

A favorite of many corporate spies has been the faithful keylogger. Like any other technology, the software and hardware keylogger has undergone upgrades. The Ghost Keylogger (www.keylogger.net) program for instance is able to email the keystrokes of anyone using the computer it is loaded on to a predefined email address. Imagine an online computer reseller or VAR (value added reseller) shipping its systems with a keylogger already preloaded and preconfigured. They could then receive confidential personal and corporate data from all over the world without ever having to leave their office. Two nice features of programs like Ghost Keylogger are that it password protects its settings, and encrypts the keystroke log file, to ensure the confidentiality of the data it has collected.

Hardware keyloggers used to sit between the computer and the PS2 keyboard. These were easy to spot, and easy to foil by using a USB keyboard. Thanks to Amecisco, Inc. that has changed. They have integrated the keylogger hardware directly into the keyboard itself.[6] So peeking around the back of the box or running spyware programs is of little use in spotting keylogging hardware anymore.

**More Power to Ya**

Wireless networking has become a great tool for many companies; tools, however, can be used for both constructive and deconstructive purposes. A few years ago, it was very easy to connect a rogue wireless AP to a corporate network, and copy data from a distance without being detected. Today, IT professionals have gained the necessary training, experience, software and hardware necessary to safeguard their networks from unauthorized wireless access. Thankfully a new technology, Ethernet over Power (EoP) [visit Homeplug.org for more information], has emerged that will once again allow an insider to covertly access and scan a corporate network for sensitive information.

By inserting a network cable into a device like Netgear's XE102[7] and then plugging it into an electrical outlet, an individual can turn a building's electrical wiring into a 56-bit DES encrypted network that cannot be sniffed or detected like wireless. By using a second EoP device, an intruder can be anywhere in a building and casually search for and steal data without revealing his real physical location. If an EoP device is discovered, it will most likely be overlooked as a power supply or some sort of surge protector.

Netgear XE102 [7]

**A Tale of Two APs**

While efforts are being focused on securing corporate wireless networks, very little attention or effort is being paid to secure the wireless client. By using simple Wi-Fi phising techniques, an attacker can capture limitless amounts of valuable personal and corporate data with very little effort. By downloading free access point (AP) software like HostAP[8], SoftAP[9], or wifiBSD[10], a spy can use his laptop or PDA to impersonate any legitimate wireless hotspot



© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

AP. An illegitimate AP clone, aka 'evil twin," can be quickly set up in any hotel, airport, conference center or Starbucks.
Once a user is connected to the fake AP, a spy then has a "man in the middle" platform from which to capture account information, credit card numbers, user names and passwords, confidential emails and any other information that passes through the evil twin.[11] Unfortunately, personal firewalls offer no protection from this type of wireless threat, but specialized software like AirDefense's AirDefense Personal 1.0 Lite software can protect users from wireless-specific vulnerabilities while accessing hotspots.[12]

**USB**
The capacity of USB drives today has increased while their size has decreased, thereby making USB drives one of the best ways to transfer data, both into and out of a system. Thanks to the variety of products that USB drives have been integrated into, it is very easy to sneak them into the work place.

USB Wristband[13]

Swiss Army USB Knife[14]

USB Keychain Soccer Ball[15]

These 'camouflaged' drives are difficult to spot by the average security guard. Normally the drive is emptied into a bowl along with a person's watch, change, pen and car keys. Once safely on the other side of the metal detector, the guard smiles and politely hands the individual back his 2Gig USB drive, and off he goes to copy OPD.

If an individual feels wary about trying to sneak a USB drive in through the front door, there is an alternative. Simply mail the USB storage device to yourself at work, copy the secret process for creating scented Post-It notes, and then mail the USB drive back to yourself (using a fictitious name and a secure mail drop of course). Most organizations do not scan or x-ray incoming or outgoing mail, and those that do, like government agencies, are usually only looking for explosive devices.

An effective, but not foolproof, countermeasure to data theft by USB is to disable the USB (and FireWire) ports in the system's password protected BIOS. There was a time when simply removing the battery on the motherboard for a few minutes would clear the BIOS password, but thanks to security conscious PC makers, that has changed.

The savvy spook now knows that most of the time, the manufacturer's default password has not been changed. So all he has to do is visit his friends at www.defaultpassword.com to find a vast repository of default passwords for computers, cell phones, PDAs and a lot of other devices. Thankfully, corporations can use software like DriveLock to add another layer of port security to their systems. DriveLock secures systems and networks by restricting the use of ports (USB, Firewire, serial and parallel) and external devices (floppies, CD/DVD-ROMs, etc), and makes it nearly impossible to export data.[16]

**A Host with Dual Personalities**
There are still ways for a clever spy to access ports and writeable devices that have been locked down. One way is to use Knoppix. Knoppix is CD-bootable Linux-based OS[17] that can be preloaded with the usual variety of Linux-based hacker, sniffing, and password cracking tools. Once Knoppix has been loaded from the CD and into RAM, the user has automatically bypassed domain security policies that prevent the use of ports and writeable media devices.

After OPD has been written to a CD-R, DVD-R or USB drive, the bad guy simply reboots the computer and casually walks away. Within a few moments the workstation is back up and running again as a member of the domain, and no one is the wiser as to what has transpired.

**Travelers Beware**
It is naïve for any business person who travels abroad to expect privacy and security in his hotel room today. Foreign government agencies and corporations are known to bug hotel phone lines, and even enter unoccupied rooms to copy or steal any information of value.


© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

If confidential material or valuables must be left in a hotel room, businessmen should not keep them in the room safe. The safe's key is rarely changed and once it has been copied, that safe can be opened by anyone who can access the room. A possible alternative to the room safe is to place valuables in a zip lock bag and pin it to the very top, reverse side of the drapes, making sure the bag is NOT visible from the outside of the window. Given enough time, anything hidden in a room can be found. However, if nothing of value is found quickly in the usual hiding places, inside luggage, behind the TV, under the mattress, inside of shoes, a person quickly moves on.[18]

If a laptop containing sensitive company information must be left unattended in a hotel room, steps should be taken to minimize the possibility of the hard drive's contents from being accessed or copied. By using a Logicube Sonix or Talon, a foreign government spy can copy a 30Gig hard drive in about 10 minutes, while the unsuspecting laptop owner is blissfully eating dinner in the hotel's restaurant. Using hard drives with integrated AES cryptographic hardware modules, like those found in a Classified PC, can prevent the unauthorized copying of a laptop's hard drive by requiring pre-boot authentication. If the laptop is stolen so that it can analyzed, additionally integrated security mechanisms will zero out the encryption key and make retrieval of any personal or corporate data from the hard drive next to impossible.[19]

**More Tools of the Spy Trade**

There are countless devices available to assist an individual in obtaining OPD. Most of them can be ordered directly off of the Internet. Two popular websites for ordering these 'business tools' are www.spychest.com and www.spylife.com. For a very reasonable price, a spook can purchase products to allow him to covertly record a confidential meeting, listen to a private conversation from across the park, track a courier, and even see the contents of a sealed envelop without opening it.

Below are a few of items that can be found on 'spy' websites:

- SCI-EAR 2000: a small, 9V powered device can allow a person to hear a conversation or meeting in the next room for only $179.99 at spychest.com.

- Parabolic dish microphone capable of filtering out unwanted background noise to hear a conversation up to 300 yards away from $169.99 to $499.99 at spychest.com.

- You can get an ordinary looking stainless steel watch ($189.99) or pen ($159.99) with integrated 256MB flash memory capable of 8-9 hours of covert digital voice recording. Just 'accidentally' forget and leave your (recording) pen in the conference room, and record the entire strategic marketing campaign meeting. When the meeting is over, simply enter the room, and retrieve your 'favorite pen'.

SCI-MP1700 [20]

SCI-DP4802 [21]

- A Trackstick can be attached to a car for transmitting real-time GPS movement information. The information is compatible with Good Earth and provides 3D tracking of a target's movements. [22]

- You can purchase X-ray envelope spray ($41.95) at Spylife that turns opaque paper translucent for about 30 seconds, allowing the user to view the contents of an envelope without ever opening it.[23]

- Spylife sells a 9V powered wireless camera that is only 1 x ½ inches in size and transmits up to 700ft.[24]



© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

## HOW TO BECOME A CORPORATE SPOOK

For those individuals who want to become a corporate spook, but have not been fortunate enough to have been trained in the fine art of information/intelligence gathering by a government agency, they can always take a class. The Society of Competitive Intelligence Professionals (SCIP) offers courses to individuals who want to become a "competitive intelligence (CI) professional", aka ethical corporate spy. SCIP courses teach "the legal and ethical collection and analysis of information regarding the capabilities, vulnerabilities, and intentions of business competitors"[25] as well as methods to reduce a company's risk of becoming a victim of corporate spying.

SCIP believes it is the duty of the trained CI professional to show corporate decision makers "alternative courses that will avoid potential dangers, and to take advantage of the tactics and strategies that lead to the bottom-line success."[26] A potential CI professional can select courses from five categories:

1. CI Offense - provides you with tools and techniques that help grow the business, including technology, alliances, and new markets. A few courses in this category include:

   - CI for Fun and Profit in the Federal Market
   - The CI Process and Technology
   - Best Practices in Developing CI Deliverables

2. CI Defense - protects your business by identifying emerging/latent threats, defensive strategies, economic espionage, early warning systems, and the role CI plays in threat awareness. Curses offered include:

   - Analyze This! Assessing Corporate Vulnerabilities
   - Current Trends in Economic Espionage
   - Threat Awareness: What's CI Got to Do with It?

3. Essential Skills - develops core capabilities and skills for practitioners to develop skills in research planning, data collection, analysis, delivery/dissemination, and utilization by management.

   - You've got Data. Now What?
   - Behind Closed Doors: Getting Information on Companies in Countries with Limited Disclosure Laws
   - Innovative and Effective Phone Interviewing Techniques to Maximize Competitive Knowledge

4. Professional Effectiveness - increases skills that are not found expressly in your job description: managing projects and resources, dealing with management and internal clients, and navigating though your organization's unique structure, culture, and politics. Some courses include:

   - On the Job CI: A Proactive Approach to Career Development
   - Running the CI Function: Best Practices and Case Studies
   - Finding and Managing the Right CI Provider

5. Scholarly Research & Innovation - examines cutting-edge, new research as well as techniques for educating professionals[27]

## CASES OF CORPORATE ESPIONAGE

**Case 1**

Michael and Ruth Haephrati of London created a Trojan horse program that was originally intended to spy on Michael's ex-wife's computer. However, the Haephratis saw grander uses for their virus. They tried to market it to Israel's defense agencies before Ruth decided to sell it to private investigators representing corporations. The Trojan horse was used by a major Israeli corporation to infiltrate and spy on its competitor and its subsidiaries.[28]



© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

**Case 2**
A design engineer for Volterra, a semiconductor company, announced that he was leaving his job to return to Taiwan to get married. His story was a ruse to cover up his emailing corporate information to a Taiwanese startup company that had offered him a job.[29]

**Case 3**
A Netgear engineer/product development manager used an extranet connection to download dozens of trade secret files from Marvell Semiconductor, a Netgear business customer. The engineer accepted a position with Broadcom and then 'allegedly' shared the Marvell files with other Broadcom employees.[30]

**Case 4**
A man installed keylogging software on computers located at Kinko's stores throughout Manhattan to secretly record usernames and passwords of customers. He then used the captured information to access the bank accounts belonging to those individuals, and transferred their money to fraudulently opened online bank accounts.[31]

**Case 5**
A system administrator hacked into a protected computer and stole a customer database from Acxiom, a customer of the company he worked for. Acxiom manages customer information for credit card issuers, banks, automotive manufacturers, retailers and others. The total cost of the intrusion and theft of data to Acxiom was more than $5.8 million.[32]

**Case 6**
An FBI language specialist hacked into an FBI computer on six different occasions for the purpose of private financial gain.[33]

**Case 7**
A San Dimas man pleaded guilty to illegally accessing the computer system of his former employer and reading the e-mail messages of company executives for the purpose of gaining a commercial advantage at his new job with a competitor.[34]

**Case 8**
A New York paralegal tried to sell to opposing counsel a confidential trial plan for a tobacco-related civil litigation for $2 million. The trial plan exceeded 400 pages and cost several million dollars and hundreds of man hours to prepare. It included, among other things, trial strategy, deposition excerpts and summaries, and references to anticipated trial exhibit.[35]

**Case 9**
After announcing his resignation, a Cisco employee hacked into computer systems of Cisco Systems from a workstation belonging to another Cisco software engineer. He did so in order to obtain proprietary information related to released Cisco products as well as products under development, and used the other engineer's computer because it had a writable CD drive capable of "burning" CDs.[36]

**Case 10**
An employee of an on-line bookseller, that also provided email service to book dealers, intercepted and copied thousands of email messages from Amazon.com to its bookseller clients. The employee used the information in the intercepted emails to create a database of dealers' purchase orders, and analyzed the book-selling market trends to gain a competitive commercial advantage for the company he worked for.[37]


© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

## CONCLUSION

The techniques and technologies discussed in this paper are not even close to the tip of the iceberg of what methods can be used to steal information for fun or profit. As competition in the global market place increases, so will the instances of corporate espionage. Therefore, companies both big and small need to take steps necessary to protect themselves from becoming a victim. Here are four necessary steps to help protect valuable data from falling into the hands of competitors.

1. Companies must identify what information is sensitive and classify it as such. Information such as R&D processes and innovations or new market strategies are easily identified as "sensitive." However, other information such as personnel files, pricing structure, and customer lists are often overlooked and left unprotected.

2. A company should conduct a risk assessment to identify vulnerabilities, and the probability that someone will exploit those vulnerabilities and obtain sensitive information.

3. Establish, review and update security policies and appropriate safeguards, both procedurally and technologically, to thwart attempts to exploit vulnerabilities and gain access to valuable company data.

4. Train all employees. Users, managers and IT staff all need to be trained in what business information needs to be safe guarded, techniques that can be used to gain access to sensitive data, and what procedures should be taken to report compromises or suspected attempts to solicit sensitive information.

The Interior Department's Chief Information Office, W. Tipton states:

> "People using computers and the professionals maintaining networks and systems are the source of the problem, which means that training all employees is an essential step in managing an IT security program. Users who are not trained to detect phishing and pharming attacks or spyware can open dangerous backdoors to hackers."[38]

Knowledge is power. The more knowledge corporations have about the threats that are out there, the better they will be able to defend themselves from attempts to steal their jackpot.



© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

**REFERENCES**


1. Louth, Nick, "Corporate Espionage." July 1, 2004. http://money.uk.msn.com/Investing/Insight/Special_Features/Active_Investor/article.aspx?cp-documentid=142987

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

3. http://www.usdoj.gov/criminal/cybercrime/FBI2005.pdf

4. Sarkar, Dibya, "Customs agents are seizing record amounts of pirated IT hardware." Federal Computer Week. May 8, 2006.

5. http://www.silexamerica.com/us/doc/press26_eng.pdf

6. http://amecisco.com/hkkeyboard.htm

7. http://www.netgear.com/products/details/XE102.php

8. http://hostap.epitest.fi/

9. http://www.nat32.com/nat32e/htm/softap.htm

10. http://www.wifibsd.org

11. Phifer, Lisa "Anatomy of a Wireless "Evil Twin" Attach." 2005. http://www.corecom.com/external/livesecurity/eviltwin1.htm

12. http://www.airdefense.net/newsandpress/01_24_05.shtm. January 24, 2005

13. http://www.thetechzone.com/?m=show&id=477

14. http://www.thinkgeek.com/gadgets/tools/6b3b/

15. http://fredliu12.trustpass.alibaba.com/product/11452591/USB_Flash_Disk_With_Football_Shape.html

16. http://www.devicelock.com/

17. http://www.knoppix.org/

18. H. Keith Melton and Craig Pilligan. "The Spy's Guide: Office Espionage". 2003.

19. http://classifiedpc.com/topsecretPC.html

20. http://www.spytechs.com/listen_voice_equip/watch-recorder.htm

21. http://www.spytechs.com/listen_voice_equip/pen-recorder.htm

22. http://www.trackstick.com/




© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

23. http://www.spylife.com/envelopespray.html

24. http://www.spylife.com/vidcam-cmos1.html

25. http://www.scip.org/2_overview.php

26. Ibid.

27. http://www.scip.org/06annual/

28. Reuters, "Israel holds couple in corporate espionage case." January 31, 2006. http://news.zdnet.com/2100-1009_22-6033129.html

29. Forsberg, Birgitta, "The spies in the next cube Silicon Valley a magnet for trade secret theft -- and it's often an inside job." San Francisco Chronicle. April 25, 2005. http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2005/04/25/BUGGLCDPUJ1.DTL

30. www.cybercrime.gov

31. Ibid.

32. Ibid.

33. Ibid.

34. Ibid.

35. Ibid.

36. Ibid.

37. Ibid.

38. Tipton, W. Hord, "IT security starts with the user," Federal Computer Week, p. 29. May 8, 2006.

© SANS Institute 2007, Author retains full rights.



© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Last Updated: May 23rd, 2013

# Upcoming SANS Training

**Click Here for a full list of all Upcoming SANS Events by Location**

| | | | |
|---|---|---|---|
| SANS Malaysia @ MCMC 2013 | Cyberjaya, MY | Jun 03, 2013 - Jun 08, 2013 | Live Event |
| SANS Pen Test Berlin 2013 | Berlin, DE | Jun 03, 2013 - Jun 08, 2013 | Live Event |
| Industial Control Systems Security Training - Houston | Houston, TXUS | Jun 10, 2013 - Jun 15, 2013 | Live Event |
| Security Impact of IPv6 Summit 2013 | Washington, DCUS | Jun 14, 2013 - Jun 16, 2013 | Live Event |
| SANSFIRE 2013 | Washington, DCUS | Jun 14, 2013 - Jun 22, 2013 | Live Event |
| SANS Canberra 2013 | Canberra, AU | Jul 01, 2013 - Jul 13, 2013 | Live Event |
| Digital Forensics & Incident Response Summit 2013 | Austin, TXUS | Jul 09, 2013 - Jul 16, 2013 | Live Event |
| SANS London Summer 2013 | London, GB | Jul 09, 2013 - Jul 16, 2013 | Live Event |
| SANS Rocky Mountain 2013 | Denver, COUS | Jul 14, 2013 - Jul 20, 2013 | Live Event |
| SANS Mumbai 2013 | Mumbai, IN | Jul 22, 2013 - Jul 27, 2013 | Live Event |
| SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification | Washington, DCUS | Jul 22, 2013 - Jul 26, 2013 | Live Event |
| SANS San Francisco 2013 | San Francisco, CAUS | Jul 29, 2013 - Aug 03, 2013 | Live Event |
| SANS SEC 560: Network Penetration Testing @ Bangalore 2013 | Bangalore, IN | Aug 05, 2013 - Aug 10, 2013 | Live Event |
| SANS Boston 2013 | Boston, MAUS | Aug 05, 2013 - Aug 10, 2013 | Live Event |
| Critical Security Controls Summit | Washington, DCUS | Aug 12, 2013 - Aug 18, 2013 | Live Event |
| Industrial Control Systems Security Training - DC | Washington, DCUS | Aug 12, 2013 - Aug 16, 2013 | Live Event |
| SANS Thailand 2013 | Bangkok, TH | Aug 19, 2013 - Aug 31, 2013 | Live Event |
| SANS Virginia Beach 2013 | Virginia Beach, VAUS | Aug 19, 2013 - Aug 30, 2013 | Live Event |
| Mobile Device Security Summit 2013 | OnlineCAUS | May 30, 2013 - Jun 06, 2013 | Live Event |
| SANS OnDemand | Books & MP3s OnlyUS | Anytime | Self Paced |