Spy-OpsTraining Brief

Volume 0, Brief 0

March 2005

Corporate Espionage

CONTENTS:

Objectives:

- Understand the current state of corporate espionage
- Understand the implications of corporate espionage
- Understand both the insider and external threats associated with corporate espionage

Abstract

Corporate espionage is the dirty little secret of global business. Espionage activities are often masked under the title of competitive intelligence. But in the end, thieves or spies still acquire sensitive, restricted information assets of another entity, which may include product designs, business models, marketing plans, research and development files, customer lists, employee lists, pricing strategies and other intellectual property.

This module will provide a basic understanding of the current state of corporate espionage, as well as illustrate many techniques used in committing this new type of crime.

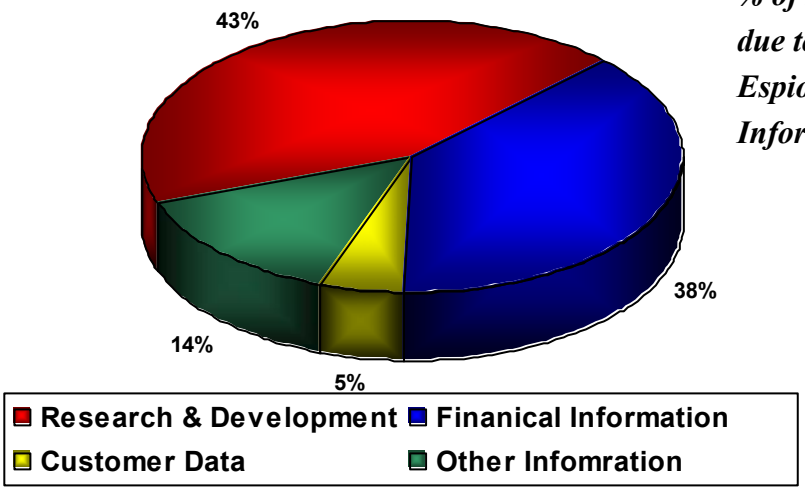
Brief

Corporations are comprised of assets which have value, information being one of those assets. Information, often known as intellectual property (IP), is critical to a corporation as it can make the difference between success and failure, or between profit and loss. In fact, it is estimated that 70 percent of the average enterprise's value is held in its information. (Source: Trends in Proprietary Information Loss, American Society for Industrial Security and PricewaterhouseCoopers.)

Corporate espionage, although it can take on many forms, from theft of physical assets to sabotage, is most often associated with the theft of information or intellectual property (IP). Call it espionage or competitive intelligence, the fact is that individuals still illegally acquire sensitive, restricted information assets of another entity which may include all types of intellectual property including product designs, business models, marketing plans, research and development files, customer lists, employee lists, and pricing information.

As the following chart depicts, it is estimated that the type of information that is typically acquired during corporate espionage is primarily related to research and development or financial information. However other information, including customer data, is also at risk.

Corporate spying does not just occur between businesses. Corporations spy on individuals, political groups, special interest groups and even citizen groups. So even if you don't think you personally have anything worth stealing, someone else might.



% of Losses due to Corporate Espionage by Information Type

Global Considerations of Espionage

The United States is the world's largest economic power. Globalization and competition have led to increased corporate espionage targeting U.S. companies. How big is the problem? No one really knows. According to Robert Bryant, former head of the FBI's National Security Division, lack of industrial espionage laws has hamstrung hundreds of FBI investigations involving the intelligence services of at least 23 countries, half of them unfriendly states and the rest friends and close allies.

The development of a global economy, with a rapid expansion in foreign trade, travel, and personal relationships of all kinds, now makes it easier than ever before for foreign intelligence officers or agents of foreign corporations to establish personal contact with, and have access to valuable classified, controlled, or proprietary information. As international contacts have become more common, it has become easier for intelligence officers and agents to contact, assess and develop targets without arousing suspicion.

KEY WORDS

Computer Crime

Trade Secrets

Competitive Intelligence

Intellectual Property

Economic Espionage

Sources of the threat to classified and other protected information include:

- Foreign or multinational corporations
- Foreign government-sponsored educational and scientific institutions
- Free-lance agents (some of whom are unemployed former intelligence officers)
- Computer hackers
- Terrorist organizations
- Revolutionary groups
- Extremist ethnic or religious organizations
- Drug syndicates
- Organized crime

The above mentioned groups and the intelligence services of friendly and allied countries are now more active in intelligence operations against the United States than during the Cold War. Espionage by friends, in addition to adversaries, has long been more widespread than generally realized.

To protect their reputations, corporations mostly don't admit to spying or being spied on. Currently there are no regulatory requirements to report corporate espionage incidents and many of them go undetected. However, under the Economic Espionage Act of 1996 (EEA), businesses can request investigation by the Federal Bureau of Investigation and criminal prosecution by the U.S. Attorney's Office for theft of trade secrets.

What Exactly is Espionage?

Espionage is the use of illegal means or deceptive practices to gather information. It is also commonly referred to as industrial or economic espionage. One report on corporate espionage produced by the National Counterintelligence Agency suggests that U.S. businesses lost $44 billion in a two year period in the late 1990s due to economic espionage. In 1999, Fortune 1000 companies reported a total of $45 billion in losses due to corporate espionage. Currently, it is believed that theft of trade secrets exceeds $100 billion annually. It is an epidemic – an epidemic that is not being openly discussed nor fully addressed. Many of today's most successful enterprises have been hit hard by electronic espionage incidents and the number is climbing.

Industrial Espionage (or Economic Espionage) is the clandestine collection of sensitive, restricted or classified information. This information by its very nature is not openly accessible and can only be obtained through covert collection means. Industrial Espionage might include the theft of sensitive or restricted competitor information (such as financial data, restricted manufacturing processes,

GLOSSARY OF TERMS

Espionage is the use of illegal means or deceptive practices used to gather information.

Dumpster Diving is the process of sorting through a company's trash for information that could be of use to a competitor or a hacker - network passwords, credit card numbers, or research results, for example. It's a common tactic in corporate espionage.

Whacking is the use of a wireless network without authorization to obtain information.

Spyware refers to software that performs certain tasks on your computer, typically without your consent. This may include giving you advertising or collecting personal information about you. It can even capture every keystroke and send it to others without your knowledge.

customer accounts, etc.), covert recruitment of sources within a competitor's firm, and other such methods.

Each and every day covert activities are being conducted for the purpose of obtaining information that can create value for another organization, be it a business or another government.

Two cases in point are:

Case #1

Two ex-Transmeta employees were caught with internal documents from Transmeta, Sun, NEC Electronics and Trident Microsystems in their possession. They were busted at the San Francisco International Airport, boarding a plane for China with some of the stolen Sun and Transmeta trade secrets. Other trade secrets were seized from their homes and office.

Case #2

The United States lost competitive advantage in a strategically important emerging industry when a Chinese citizen employee of Ellery Systems, Inc. resigned and took with him computer software source codes. The codes had cost $950,000 to produce and had a potential market value of billions of dollars. As a direct result of this loss, Ellery Systems, Inc. went out of business and 25 employees lost their jobs. Man-years of incredibly complex and hard work and millions of dollars of investment were lost to a foreign country.

Other Cases of Interest

The following Corporations and Firms have also been sited for Corporate Espionage. Some of these cases are currently under litigation.

- Avery Dennison/Four Pillars
- Lucent Technologies
- The Cleveland Clinic Foundation
- Kodak
- MasterCard
- Bristol-Meyers Squibb/Taxol
- Gillette
- PPG Industries/Owens-Corning
- Idexx Laboratories
- Solar Turbine
- Deloitte &Touche
- The Atlanta Journal-Constitution
- Intel

Government Involvement

Earlier this year in a report to the European Parliament, a British investigator asserted that both U.S. and European companies routinely engage in corporate espionage. Additionally, many foreign corporations regularly receive help from intelligence-gathering networks in their own governments which use the latest in information monitoring technology to keep abreast of supposedly private Web communiqués. There are a number of objections to government involvement in economic espionage. Some examples are given here:

GLOSSARY OF TERMS (Cont.)

Intelligence - Secret information, especially about an actual or potential enemy.
OR
An agency, staff, or office employed in gathering such information.
OR
Espionage agents, organizations, and activities considered as a group:
"Intelligence is nothing if not an institutionalized black market in perishable commodities" (John le Carré).

Counterintelligence— intelligence activities concerned with identifying and counteracting the threat to security posed by hostile intelligence organizations or by individuals engaged in espionage or sabotage or subversion or terrorism.

Counterespionage - Espionage undertaken to detect and counteract enemy espionage.

- What kind of information does a business need and who defines the requirements?
- How specifically can government spying help private industry?
- To whom should the information be given?
- How can covert information be handed out without disclosing sensitive intelligence sources and methods?
- By providing intelligence to the private sector, a government could find itself in a position of dictating industrial policy.
- Government sponsored commercial espionage activities could alienate allies and trading partners and intimidate customers and suppliers overseas.

Corporate Espionage Techniques

Corporate espionage is typically thought of as a high tech crime. While this is often true, corporate spies are perfectly happy to get information from the easiest and most available sources—including the trash. Information is taken by both insiders within the corporation as well as individuals and organizations external to a corporation.

Insider Threats

The Insider Threat can be anyone—from hackers to rogue employees. There are four major types of insider threats, which are used to facilitate corporate espionage.

1. Bribery. Employees may be approached directly by outside corporate intelligence agents offering cash to provide them with proprietary or confidential data.

2. Social Engineering. The manipulation of a network administrator or other IT personnel (by insiders or outsiders) to divulge information, such as logon or other authentication information, which can be used to obtain access to sensitive information.

3. Group Collusion. When several employees band together to use their collective knowledge and privileges to gain access to information.

4. Employee Access Privileges. Using the employee's own access privileges to enable them to access proprietary or confidential information.

Also important, but often overlooked, is the disgruntled employee. A disgruntled employee is more likely to sell proprietary information for profit than a satisfied employee. Intelligence agents follow a structured process to find out who of those potential employees might be a good candidate for recruitment. The following five steps are often used to turn insiders into spies.

DID YOU KNOW?

1. *Over 95% of corporate espionage attacks go unreported.*
2. *On average it takes 2 to 3 years for a corporate espionage investigation to be brought to court.*
3. *Thousands of jobs are lost due to theft of trade secrets annually in the United States.*
4. *The average organization loses more that $10 per day per employee due to fraud and abuse.*
5. *In 1999 the FBI and the US Chamber of Commerce announced that US companies lose about $2 billion a month to corporate espionage and the problems has continued to grow.*
6. *More than 56 percent of the Fortune 1000 admit to having experienced acts corporate espionage .*

Spotting - finding out who has access to sensitive information.
Assessment - finding out who has a motive to sell the information (personnel problems, high debt). Face it, extortion works!
Development – preparing the targeted employee for recruitment.
Recruiting – actually getting the targeted employee to say "yes" to agreeing to spy.
Training – teaching them how to obtain and deliver quality corporate information.

External Threats

External espionage conducted by outsiders is more publicized than espionage performed by insiders, especially because of the media attention giving to hacking and whacking. Vulnerabilities, often in systems, enable outsiders to eventually access the proprietary information that they seek. There are five major types of external threats which are used to facilitate corporate espionage.

1. Password Cracking. Several freely available password cracking programs, including BO2K and SATAN, help hackers gain access to networks. Most password analyzers are limited to simple combinations of dictionary words and numerical combinations. For the determined spy, rather than the thrill hacker, this would be a preferred method.

2. Backdoors and Trojan Horses. Programs can be executed on a user's computer to enable an outsider to gain control of that computer and gain further network access. NetBus, Back Orifice and, now, BO2K can all be used to capture data from the victim's computer and send it to a remote location. BO2K has been enhanced so that it can disguise itself once it has been installed on the user's computer. Generally, backdoors are e-mailed to the user, downloaded from a Web site, and disguised as a benign e-mail attachment or program. Once the attached file is opened, it installs itself on the user's computer without their knowledge or consent. Some backdoors (or spyware) enable snoopers to record all keystrokes input on a user's computer, enabling the spy to capture proprietary data or authentication information, which will enable access to proprietary data.

3. Packet "Sniffing" Utilities. A program or device that monitors data traveling over a network, enabling spies to steal information. Intrusion detection solutions may assist IT managers to identify and stop sniffing on their network. However, with the widening use of wireless networks, this problem is growing even with encrypted networks.

4. Social Engineering. A non-technical approach to obtaining information stored on your network.

ALERTS

ALERT 1: *Two-thirds of computers have spyware on them, leading to significant growth in espionage activity.*

ALERT 2: *Two-thirds of security experts believe that the U.S. will suffer a 'devastating' cyber-attack within 10 years. One half believes it will occur within two years. The attack may hit critical infrastructure or large industries, like banking.*

SOURCE: Pew Internet & American Life Project and Elon University

It may include contacting employees in an attempt to receive sensitive documents over e-mail. As an example, help desk employees are often targeted by social engineers in an attempt to learn about the network structure and to gain access. While social engineering cannot be managed by IT, at the very least employees can understand varying techniques that are used to gain network access or to obtain sensitive information. Protecting documents with file passwords and/or encryption can also minimize the threat of social engineers.

5. Dumpster Diving. This is the most basic form of corporate espionage and simply means looking through a corporation's trash for valuable information. Organizations who do not shred and destroy CDs, DVDs, Papers, Disks, and Tapes contribute to the problem and often make corporate espionage very easy.

Other techniques require more elaborate preparation and technical knowledge. One example is gaining access to cache chips on certain fax and photocopying machines which have the capacity to digitally store hundreds of pages of documents. Another example is the frequent targeting of laptop computers for theft or intrusion because of the vast amount of information they hold. These and other techniques can provide spies and terrorist organizations with information about an organization which may be used to its detriment.

High Risk Industries

One area that is a primary and valuable target for espionage activities is the high technology sector. Typical areas within this sector that are of high value and make attractive targets for corporate espionage include:

- Advanced materials and coatings
- Advanced transportation and engine technology
- Aeronautics systems
- Aerospace
- Armaments and energetic materials
- Biotechnology
- Chemical and biological systems
- Computer software and hardware
- Defense and armaments technology
- Directed and kinetic energy systems
- Electronics
- Energy research
- Guidance, navigation, and vehicle control.
- Information systems
- Information warfare
- Manufacturing and fabrication

Additional Training Brief Topics

Corporate Espionage
Unmanned Aerial Vehicles
Body Armor
Armored Vehicles
Creating a Microdot
Intelligence Gathering Techniques
Tracking
Digital Spying
How Spies Get Caught
Interrogation
Terrorism
Long Range Microphones
Dirty Bombs
Biological Weapons
Electronic Bugging Systems
Chemical Weapons
Personal Security
Security Systems
Biometric Facial Recognition
Biometric Fingerprint Analysis
Biometric Retina Scan
Biometric Voiceprint Analysis
Computer Bugs & Software
Computer Hacking
Electronic Footprints – Your data
Hacking - Social Engineering
Introduction to Intelligence Technology
Introduction to Secret Intelligence
Language of Intelligence
Offshore Banking
Information Protection
Invisible Inks
Locks
Night Vision

...and many future topics of interest all available on

www.Spy-Ops.com

- Manufacturing processes
- Marine systems
- Materials
- Nuclear systems
- Semiconductors
- Sensors and lasers
- Signature control
- Space systems
- Telecommunications
- Weapons effects and countermeasures

Conclusion

In conclusion, there are three primary motivations behind corporate espionage. First, an individual corporation may use corporate espionage to advance their goals towards maximizing shareholder value. Secondly, state-sponsored corporate espionage is an essential ingredient of modern day economic warfare or military application of the intellectual property. Third and finally, special interest groups may conduct corporate espionage to gather data to further their cause (i.e. environment interests).

Summary

Corporate Espionage has risen to epidemic levels. Espionage strategies range from illegal to merely seedy. In most cases, the best defense is employee awareness. The current organizational focus on risk management, governance, and compliance has, for some, blurred the responsibility for ensuring the security of an organization's assets. In a competitive marketplace where information is a priceless commodity, espionage is not likely to go away. Corporations have to reconsider the effectiveness of their overall security programs, given the current threat of corporate espionage. Comprehensive security programs should address this threat. Though espionage cannot be eliminated, implementing multi-layer safeguards will at least minimize losses.

REFERENCES

Notable Industrial Espionage Cases

http://www.dss.mil/search-dir/training/csg/security/Spystory/Industry.htm

A Case of Corporate Espionage

http://icmr.icfai.org/casestudies/catalogue/Business%20Ethics/BECG036.htm

Economic Espionage Act of 1996

http://rf-web.tamu.edu/security/secguide/T1threat/Legal.htm#Economic%20Espionage

Who is Doing What to Whom

http://www.dss.mil/training/csg/security/T1threat/Intro.htm#Who's Doing What

Spy-Ops Training Brief Answer Sheet

Volume 0, Brief 0

Corporate Espionage

In Order to earn 3 Continuing Education Units (CEUs) from Spy-Ops, in conjunction with the Technolytics Institute, you must complete both the exam and on-line exercise. Mail the completed answer sheets with your name, address, signature and date along with a check for $10.00 made payable to "Technolytics," to the Spy-Ops address below. Additional sheets for the on-line exercise may be attached if needed. An official completion certificate will be mailed to you within 2 weeks from receipt of this information by Spy-Ops. For additional training briefs visit www.spy-ops.com today!

Spy-Ops
4017 Washington Road
Mailstop 348
McMurray, PA 15317
Phone: 888-650-0800
Fax: 412-291-1193
E-mail: info@spy-ops.com

Applicant Information:

Name: _____

Address: _____

_____

City: _____ State _____ Zip _____

E-Mail: _____

Phone: _____

Exam

____ **1. What is the annual estimated loss due to theft of trade secrets?**

a. $40 million
b. $15 million
c. $100 billion
d. $40 billion

____ **2. Why would government or other state sponsored agencies conduct corporate espionage?**

a. To obtain advanced technology without the development expense.
b. To gain financial advantage for their businesses and economy.
c. To obtain information so that countermea sures to weapons can be developed.
d. All of the above

____ **3. What is the number one area for losses due to corporate espionage?**

a. Sales and Marketing
b. Research and Development
c. Customer Data
d. Financial Information

____ **4. What percentage of security experts think there will be a devastating cyber attack within the next two years?**

a. one quarter
b. two thirds
c. one tenth
d. one half

____ **5. What espionage technique can be used internally and externally?**

a. Social Engineering
b. Bribery
c. Spoofing
d. Group Collusion

Spy-Ops Training Brief Answer Sheet

Volume 0, Brief 0

Corporate Espionage

On-Line Exercise

Research and identify the top 10 countries spying on U. S. businesses. Also determine why the biggest threat comes from within an organization itself. Write a 1 page report on the above topic areas **(500 words).**

Please write your answers to the on-line exercise in the space below.
Alternatively you may attach additional sheets with your answers.

I certify that I have personally completed this test and the answers are my own.

Completed By: _____

Signature: _____Date: _____

Spy-Ops
4017 Washington Road, Mail Stop 348, McMurray, PA 15317
Phone: 888-650-0800 Fax: 412-291-1193 E-mail: info@spy-ops.com