CORPORATE ESPIONAGE

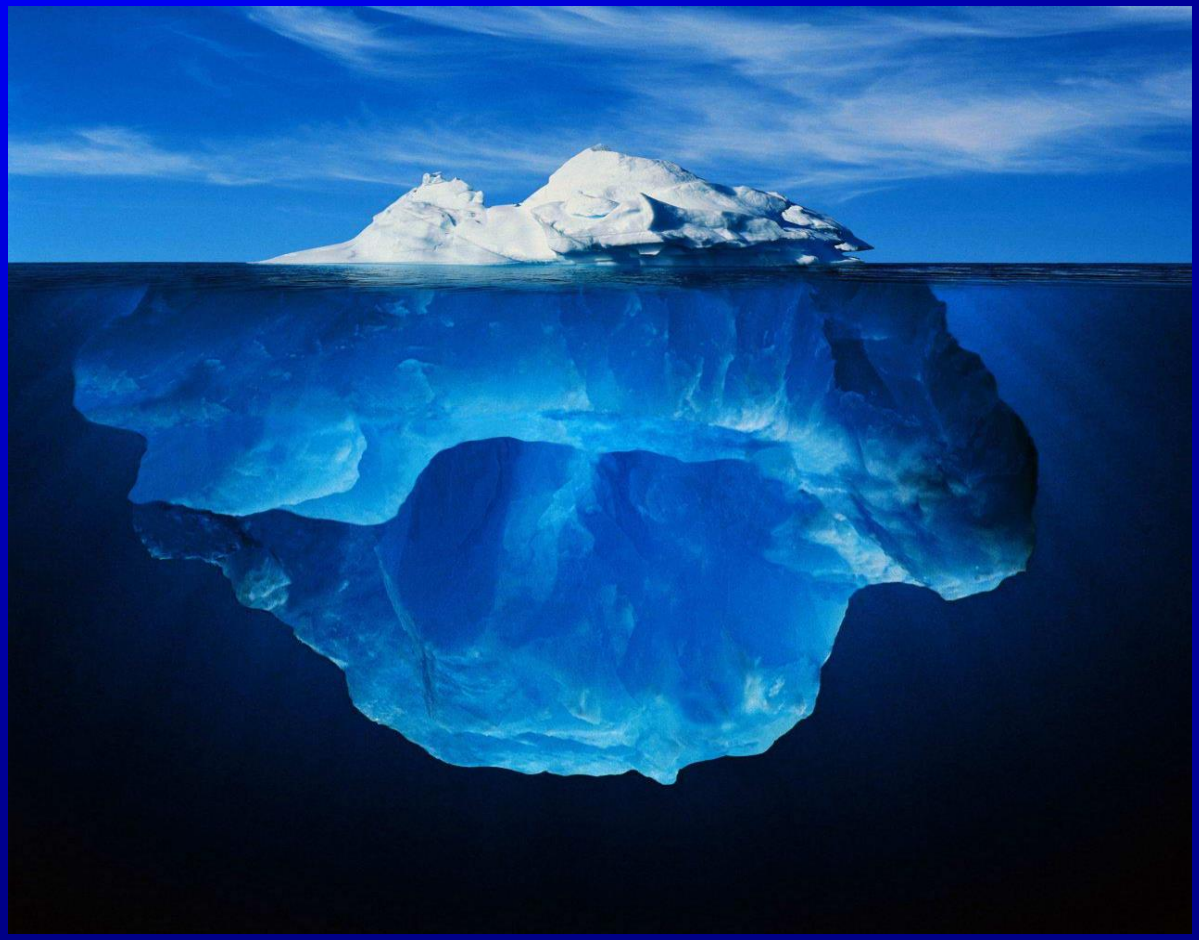
Arthur J. Harvey, PPS

Rampart Development International

ASCM Local Chapters PDM

November 9, 2022

CORPORATE ESPIONAGE



CORPORATE ESPIONAGE

- Why it is done
  - Who does it
  - How big is the problem

CORPORATE ESPIONAGE

- THE METHODS
  - Overt
  - Covert

CORPORATE ESPIONAGE

- PROTECTION METHODS
  - People
  - Paper
  - Information
  - Physical

CORPORATE ESPIONAGE

- Defined
  - The gradual and continual siphoning off of secrets without arousing the suspicion of the victim
- Note: This is the same goal for government operations and is key to any successful operation

CORPORATE ESPIONAGE

- Why is it done
  - To gain competitive information
    - Sales
    - Technical

CORPORATE ESPIONAGE

- To seek Revenge
- For a profit
  - A private operation

CORPORATE ESPIONAGE

- Who Does It?

CORPORATE ESPIONAGE

- Who Does It?
  - A Competitor

CORPORATE ESPIONAGE

- Who Does It?
  - A Competitor
  - A Disgruntled Employee

CORPORATE ESPIONAGE

- Who Does It?
  - A Competitor
  - A Disgruntled Employee
  - An Unsuspecting Loyal Employee

CORPORATE ESPIONAGE

- Who Does It?
  - –A Competitor
  - –A Disgruntled Employee
  - –An Unsuspecting Loyal Employee
  - –An Entrepreneur

CORPORATE ESPIONAGE

- How Big Is The Problem
  - Companies loose an estimated over $100 Billion per year
  - It strikes all kinds of companies
  - Grew in the 90’s and has continued into Y2K
  - Devices and gadgets easily acquired
  - The gradual erosion of workplace ethics

CORPORATE ESPIONAGE

The Economic Espionage Act of 1996

CORPORATE ESPIONAGE

- The Two Basic Methods
  - Overt
  - Covert

CORPORATE ESPIONAGE

- Who are the victims?

EVERYONE

CORPORATE ESPIONAGE

- Overt Methods
  - Listening
  - Databases
  - Exhibits and Trade Shows
  - Field Sales Force
  - Reverse Engineering
  - Market Studies
  - Public information
  - Employment Interviews
  - Head Hunters
  - Outside Employees

CORPORATE ESPIONAGE

- Covert Methods
  - Trespassing on Property
  - Secret Observations
  - Electronic Eavesdropping
  - Hiring a Competitor's Employee
  - Placing an Agent
  - Hire a Spy
  - Stealing Documents
  - False Market Surveys
  - Phony licensing Agreements
  - Blackmail
  - Extortion

CORPORATE ESPIONAGE

- Some Additional Thoughts
  - The Entrepreneur
  - The Unsuspecting Employee
  - The Corporate Directive

CORPORATE ESPIONAGE

- The Tools
  - Bugs, Gadgets and Other Devices
- Three Categories
  - See A Secret
  - Hear A Secret
  - Steal a Secret

CORPORATE ESPIONAGE

- See
  - Cameras
  - Optics
  - Video
  - Chemical

CORPORATE ESPIONAGE

- Hear
  - Bugs
    - RF
    - Laser
  - Amplifiers

CORPORATE ESPIONAGE

- Steal
  - Books
  - Entry Tools

CORPORATE ESPIONAGE

- Five Factors To Consider
  - Suspicious Activity
  - Reasons For Acts
  - Factors Of Susceptibility
  - Are Employees Aware of Their Risks
  - What Will Make Employees More Aware

CORPORATE ESPIONAGE

- Protection Areas
  - Paper & Document Controls
  - Computers
  - Security Surveys
  - Asset Protection

CORPORATE ESPIONAGE

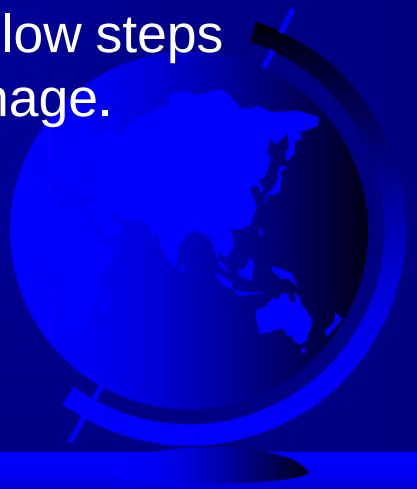
- Protection Areas
  - Paper & Document Controls
  - Computers
  - Security Surveys
  - Asset Protection

CORPORATE ESPIONAGE

- Countermeasures
  - Train the Workers
    - Observation
    - Patterns of work
  - Detection Devices
    - Phones Taps
    - Recorders
    - Bugs

CORPORATE ESPIONAGE

- Written by Garrick Otero and Vijaya Prasad
-
- James Bond’s days are numbered. The iconic spy’s agency MI-6, the CIA, NSA, and other intelligence agencies are continuously moving away from human intelligence and into the world of satellites and unmanned drones. Unfortunately, there just aren’t many jobs available for gadget-toting sneaks.
- As part of *Handshake*’s continuing effort to help its readers achieve their dreams, we’ve provided five easy-to-follow steps that will help you start that career in corporate espionage.

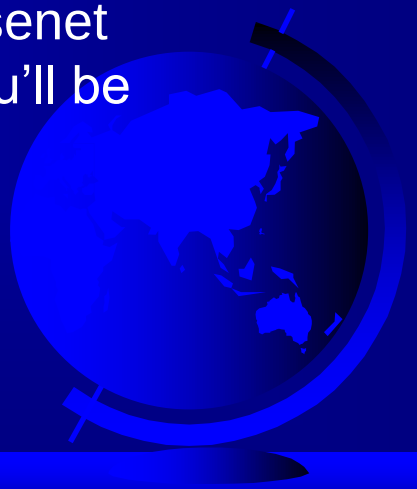


CORPORATE ESPIONAGE

- **Espionage Essential #1: Clone The Hard Drive**
- Mainstream operating systems (such as Vista and OSX) commonly provide hard drive encryptions and remote wiping, but these features don't mean a thing if you can steal the entire hard drive before anyone notices. Think a more modern version of Tom Cruise's character in *Mission Impossible* when he breaks into the CIA and copies the information onto the disk.
- Modified versions of programs like Blindwrite can lift the info as a solid block of bits without having to break up the data, avoiding any need to decrypt it immediately. Instead, it lets you take the information and retrieve it on your schedule.

CORPORATE ESPIONAGE

- **Espionage Essential #2: Crack The Passcode**
- Acquiring the information doesn't matter if you can't crack the information. Good news—there is an online community where global computer geeks convene. They make a decent living cracking encryption algorithms on everything from DVD copyright blocks to internal corporate password databases. We could tell you where to go, but we wouldn't want to make it too easy.
- So query the right message boards/IRC channels/Usenet threads with Google Translate as your guide, and you'll be cracking in no time.



CORPORATE ESPIONAGE

- **Espionage Essential #3: Tap The Phone Line**
- A butt set, despite its name, has nothing to do with human anatomy. It's a simple tool that hooks into phone lines from outside the building and lets you listen in on your targets' conversations. You can buy a set for $100-$200 or make your own with a cheap phone and a few parts from Radio Shack. Don't be too discouraged if the company you're targeting has secured phone lines; just find some upper-level executive's house and tap in there. You might have to spend a long time listening to your mark's teenage daughter's love life, but eventually you're bound to hear a business secret or two.

CORPORATE ESPIONAGE

- **Espionage Essential #4: Steal The Corporate Secrets**
- These babies are just plain cool. Logistically, bugging a board room to listen to corporate secrets can be challenging. Fortunately, CEOs and board members tend to have even bigger egos than bank accounts, so their offices and conference rooms are on top floors with massive windows. They use the windows to look down at all the little people scurrying around—you'll use them to reap the company's profits.
- Laser mics shoot a laser beam at the window, which vibrates from the sound waves in the room. These waves distort the beam before it bounces back to the mic's receiver, which sends all those data gigabytes to a filter and converts it to sound for your listening pleasure.
- These gadgets are available from Brickhouse Security for a very reasonable $51,495, or you can buy a $24.95 lock-picking kit from the same company, break into their headquarters in NYC, and steal it.

CORPORATE ESPIONAGE

- **Espionage Essential #5: Last Resort: Extortion**
- Even in the digital age, the old classics still do the trick. In fact, human intelligence is still the best kind. Coerce the right people and they'll not only tell you everything they know, but they can also plant bugs, tap phone lines, copy hard drives for you, and do anything else that requires privileged access.
- Some spies like to use bribery as well. That might work to get a janitor or a secretary to help you out, but do you really have the cash to bribe an executive? Besides, extortion is a hell of a lot more fun. In all seriousness, the average client for espionage profession is a corporate executive, a government agency, or a corporate CEO.

CORPORATE ESPIONAGE

- And if you're attached to your current life, consider this before committing to a life of espionage. According to J.D.LeaSure, the CEO of ComSEC LLD, a counter intelligence firm, "You're committing to a lifestyle not a career. It's a combination of counterintelligence and tactics that encompass so many platforms and protocol."
- Dig up a dirty secret you can use to your advantage, such as threatening to expose that {O Robotics employee who reads *Handshake*} remaining Google employee using Windows. And you're on your way to corporate espionage heaven or jail, whichever comes first.

CORPORATE ESPIONAGE

- **Industrial Espionage: Developing a Counterespionage Program By Daniel J. Benny, Ph.D.**
- Published: September 25, 2013 by CRC Press
  Content: 232 Pages | 33 Illustrations
  Hardback
  ISBN 9781466568143
  ISBN 9781466568150
- http://www.crcpress.com/product/isbn/9781466568143
- From Amazon.com:
  Features Identifies the threats against organizations proprietary information from industrial espionage.
  Provides guidance in assessing the threat from espionage but exploring motives and spy tradecraft that is utilized. Presents the optimal physical security, policy, and procedures to have in place for a corporate counterespionage program.Covers physical security measures that can be used to protect proprietary information.

CORPORATE ESPIONAGE

- **The International Journal of the Business Espionage Controls & Countermeasures Association (BECCA)**
  ISSN 2168-9741 (International Standard Serial Number)
  Box 55582 Shoreline, WA 98155-0582
  Journal@BECCA-online.org

- **Journal Update 2014**

  BECCA Members use the Journal to publish research papers and other materials as part of their academic pursuits in degree programs, to enhance their careers in the public and private sectors, and for other purposes as they see fit.
  It is a "publish or perish" world, especially in academia. Unfortunately, there are unscrupulous people who take advantage of this situation. The audacity of those who rip-off other people's work without at least giving the author credit is revealed using Internet search procedures based on the spelling, syntax, style, and other features of the original copyrighted materials.

CORPORATE ESPIONAGE

We all see these rip-offs on the Internet where the thefts are sometimes difficult to track due to the sheer volume of information. It also happens on campuses. One college student went so far as to copy major portions of a research paper written by his own professor when she was writing under her maiden name.

BECCA members have called our attention to a number of apparent copyright violations over the years, rip-offs based on materials we have published in The Business Espionage Report (TBER), the Certified Confidentiality Officer (CCO) Program, and the BECCA Journal. Many of the offenders do not even list the authors as sources.

CORPORATE ESPIONAGE

Tips for Preventing Business Espionage

Any type of business that possesses proprietary information may be under threat of corporate espionage. Data compromised could consist of employee information, client information, research documents, client agreements and prototype designs for new products and more.

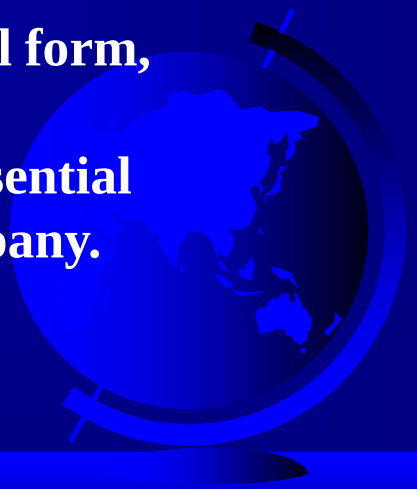
Outside interests steal information to blackmail or extort the company for money. They may also develop elaborate scams, commit credit card fraud, or other criminal behavior with the information stolen.

Most often, business espionage is committed by employees. In fact, employees account for 85 percent of corporate espionage. In total, companies lose up to $100 billion per year due to business espionage.

CORPORATE ESPIONAGE

Statistically, companies have proven that 75 percent of business espionage occurs from obtaining a physical document or disk, rather than hacking. Companies are breached by individuals dumpster diving and collecting trash. Companies should monitor their practices to ensure that these particular occurrences do not occur. Businesses may implement a number of security safeguards to prevent these actions from occurring.

- **Shred Documents**
- **Since a majority of information stolen is in the physical form, companies should shred all documents before they are discarded. A regular shredding process will prevent essential company information from being stolen from the company.**



CORPORATE ESPIONAGE

Avoid Printing Proprietary Information

- **Do not print sensitive company information unless it is absolutely necessary. Then immediately place the information in a secure envelope or place until it reaches the intended party. Information lying around on a desk may be easily copied, photographed, or stolen. Companies should change their policies in order to prevent this occurrence.**

- **Physical Security**
- **Secure all necessary printed documents in a locked file cabinet. Keep the cabinets locked when the cabinets are not in use. This prevents employees or other parties from stealing documents or copying documents.**

CORPORATE ESPIONAGE

Electronic Deterrents

- **Companies invest significant amounts of capital into protecting electronic documents from hacking or outside intrusion. The likelihood of a virus or Trojan is possible; however, businesses are more likely to be breached through a printed document rather than hacking. Businesses must provide means to protect printed documents from tampering.**

- **Copy-Proof Technology**
- **Companies should invest in technology that prevents documents with sensitive company information from being copied. Common solutions might be a program like Adobe Acrobat, or Pagemaker, allowing you to watermark or otherwise protect your documents from duplication.**

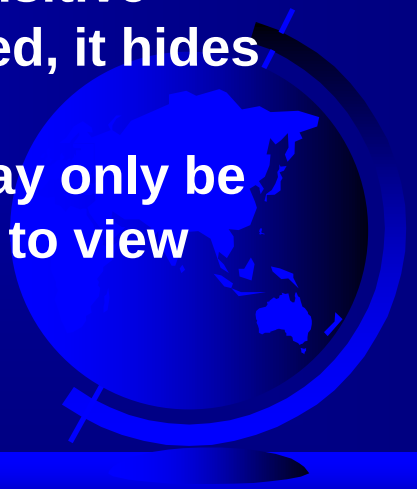
.

CORPORATE ESPIONAGE

Enterprise Rights Management

- **Companies may set access controls within software indicating authorized parties that are allowed to print specific runs of specific documents. This will prevent individuals from carelessly printing materials which may expose the company to unnecessary risks.**

- **Print Encryption**
- **Print encryption is another method to protect sensitive company information. When a document is printed, it hides sensitive information in the print fields where the encryption occurs. The information encrypted may only be viewed by individuals who possess the authority to view the information.**



CORPORATE ESPIONAGE

Preventing Computer Espionage

- **Trojan Horses and viruses are often used to lift information from corporate individuals. This type of espionage is very targeted and covert. Computer hackers have developed elaborate Trojans to prevent corporations from determining the origin of the hacker. The hackers also guard against spy program removal and from detecting that the program exists by circumventing any virus software. Corporate hackers use the information to provide directly to a competitor or to convince corporations to purchase their software to prevent future attacks. The latter occurrence is akin to blackmail.**
- **Information may also be shared to the very individuals you are entrusting to keep you protected. Individuals who purchased anti-Trojan or anti-virus software must trust the individuals in the corporations employed to protect them, because that company may also be guilty of corporate espionage. Anti-virus developers may hack a system faster than any outside entity.**
- **Disgruntled employees may be likely candidates for business espionage. Companies should be aware of Web 2.0 services, anti-virus and anti-Trojan software, and off-site storage. Businesses should protect all copyrights, trademarks, and patents that are stored electronically, as well as other intellectual e-properties.**

CORPORATE ESPIONAGE

Not only should the company be concerned about their own information, but they should also be concerned with maintaining the security of their clients' information. Sensitive information such as addresses, Social Security numbers, account numbers and credit card numbers must be protected. Breach of this type of information may cause irreparable harm to an individual and can be the responsibility of the company. When personal information is lost or breached, companies may lose millions of dollars and face charges from millions of legitimately irate customers. Non-compete and non-disclosure agreements are a start in preventing employees from exposing company data. However, employees will often share data despite the agreement. Companies need firewalls and other ways to block company sensitive data from leaking from the corporation. All anti-virus and anti-Trojan software should be updated frequently. Screen employees and hire those who you trust will not be a great risk in sharing sensitive corporate information.

CORPORATE ESPIONAGE

Servers should only be accessed by trusted IT professionals. Servers should be stored offsite or be stored in locked cabinets that cannot be accessed by normal means. The cabinets should be able to withstand heat and cutting tools. Employees should be sure their computers are free of keystroke gathering technology when working from remote locations on web based applications.

- **Traditional anti-virus software may no longer protect some corporations. Many companies need customized applications to block competitors from accessing sensitive data. Companies must remain vigilant and continuously update prtective measures, as technology changes quickly. Old software will leave the company vulnerable to potential security breaches.**

CORPORATE ESPIONAGE

Some Resources

- **https://www.congress.gov/104/plaws/publ294/PLAW-104publ294.pdf**
- **https://media-drift.com/corporate-espionage-is-entering-a-new-era/**
- **https://www.ekransystem.com/en/blog/prevent-industrial-espionage**
- **https://www.dni.gov/index.php/ncsc-features/203-about/organization/national-counterintelligence-and-security-center?start=66**
- **https://www.fbi.gov/investigate/cyber**

CORPORATE ESPIONAGE

- Demonstration

CORPORATE ESPIONAGE

Questions

Arthur J. Harvey, PPS
Rampart Development International
Derry, NH 03038

aharvey@rdi.qozzy.com

Mobile Phone 508.878.0165