

Understanding the Risks and Costs of Industrial Espionage and Corporate Information Theft



*Research Electronics International
Leading Manufacturer of
Technical Surveillance Countermeasures.*

Objective

- ❑ To provide a realistic view of the value and risks associated with corporate information protection
- ❑ To raise awareness of the real consequences of intellectual property and information vulnerabilities

Outline

- ❑ REI Background
- ❑ What is Espionage and,
Information Loss/Theft
- ❑ Classes of Corporate
Intelligence Gathering
- ❑ How Real? Who is at risk?
- ❑ What are the Costs?
- ❑ Case Examples
- ❑ Final Thoughts

REI History

- ❑ Founded in 1983 by Bruce Barsumian
 - Prior experience designing and building clandestine transmitters for Audio Intelligence Devices (AID)
- ❑ Partnership formed with Tom Jones in 1995
 - Background as instructor for US Navy Nuclear Power Training Academy
 - Managed crucial design engineering teams for Department of Defense contracts

REI Background

- ❑ Recognized industry leader for TSCM equipment
- ❑ REI equipment in over 85 countries, used by corporations, governments, law enforcement, and professional sweep teams
- ❑ Center for Technical Security dedicated classrooms & live project rooms for hands-on TSCM exercises



© Copyright **REI** January 2005

Industrial Espionage

- ❑ "The practice of spying or using spies to obtain information about the plans and activities especially of a foreign government or a competing company," *Merriam-Webster*
- ❑ "Spying on one's competitors to gain a competitive advantage. Often illegal," *investorwords.com*.
- ❑ Competitive Intelligence: gathering of information to enhance competitive position...

Bottom Line: information loss doesn't have to be "Espionage" (illegal/unethical) to be costly...

Industrial Espionage

Interview with Dave Szady
FBI Assistant Director, July 20 2004

- ❑ "Economic Espionage attempts to disadvantage unfairly without legitimate competition,"
- ❑ "It can impact our country's economic viability in such a significant way you impact its national security,"
- ❑ "It strikes at the heart of our national security... our economic strengths; our position in the world; our future as a country,"
- ❑ "FBI's #2 Priority, only terrorism ranks above it"

Corporate Intelligence Gathering

- ❑ Friendly Intelligence Gathering
 - Open Source, Readily Available Information
 - Published, Shared, or Disclosed
 - Corporate Competitive Profiling

- ❑ Unfriendly Intelligence Gathering
 - Typically illegal, unethical, malicious
 - Terrorism and other Threats
 - Industrial Espionage
 - Trade Secrets
 - Customer/Prospect Databases
 - Financial Information

Corporate Intelligence Gathering

- ❑ White Zone: Ethical and Legal
 - Open source information
 - Competitor profiling
- ❑ Gray Zone: Unethical but Legal
 - Dumpster diving
 - Misrepresenting yourself to gain information
- ❑ Black Zone: Unethical and Illegal
 - Information/Intellectual Property gained illegally

How information was obtained has legal implications.

More importantly, what is the impact of the information loss!

Corporate Intelligence Gathering

"Business Intelligence Spying: How Far is Too Far"
Fortune Magazine, December 18, 2003

- ❑ "Once refuse makes its way to a Dumpster, its fair game... not illegal"
- ❑ "There's no law against lying..."
- ❑ "Misrepresentation tactics are common... curious potential customer or journalist."
- ❑ "Tried-and-true method... fake job posting, meet with applicants who work for your competitor..."
- ❑ "Interviewing at rival company... also acceptable"

Corporate Intelligence Gathering

"French Spymaster (Alain Juillet) Expected to
Head Economic Intelligence Unit,"
Morningstar, December 22, 2003

- ❑ "His task will be to collect, synthesize & disseminate economic intelligence of value to French corporations..."
- ❑ Position created by the French Prime Minister
- ❑ Juillet studied at Stanford & French Int. of Defense
- ❑ Worked for Pernod-Ricard SA (drink co.), Union Laitiere Normande (dairy co.), Jacobs Suchard (chocolate co., affiliate of Kraft, part of Philip Morris Co.)

How Real? Who is at Risk

- ❑ 40% reported Intellectual Property losses

*Trends in Proprietary Information Loss
ASIS Survey Report September 2002*

- ❑ 44% of UK Businesses suffered at least one malicious information security breach in 2001

*Information Security Breaches 2002
PricewaterhouseCoopers, Dept. of Trade & Industry, UK*

- ❑ 37% report significant economic crimes...

*Global Economic Crime Survey 2003
PricewaterhouseCoopers, Wilmer Cutler & Pickering, NY*

Bottom Line: About 40% or 2 out of 5 companies
reported losses due to Industrial Espionage

How Real? Who is at Risk

- ❑ "There is an easy way to figure out if you might be a target: If you sell anything worth buying, you've got something worth stealing,"

Are you safe from corporate spies?

The Orlando Sentinel, Tim Barker, 6/22/03

- ❑ 70% of workers polled confessed to stealing corporate secrets when they left their last job.

IT Fuels Intellectual Property Theft

Personal Computer World, February 20, 2004

What are the Costs?

- ❑ Losses are extremely difficult to track and quantify (usually swept under the carpet):
 - Acknowledgment can cause other intangible loss
 - Embarrassment
 - Loss of Goodwill
 - Affects Stock Value

However, there are some statistics...

What are the Costs?

- ❑ 2001 Intellectual Property losses in the US estimated at as much as **US\$59 Billion**

*Trends in Proprietary Information Loss
ASIS Survey Report September 2002*

- ❑ Combined costs of foreign and domestic economic espionage, including theft of intellectual property, as high as **US\$300 Billion** per year and rising

*Annual Report to Congress on
Foreign Economic Collection & Industrial Espionage, 2002*

- ❑ Intellectual property theft costs U.S. companies about **US\$300 Billion**

*The ABCs of Intellectual Property Protection
CSO (Chief Security Officer Magazine), December 9, 2003*

What are the Costs?

- ❑ Value of proprietary data on a stolen laptop:
US\$690,759

2003 BSI Computer Theft Survey

- ❑ Average dollar loss per incident (2 incidents/yr):
MORE than US\$300,000 per incident

*Trends in Proprietary Information Loss
ASIS Survey Report September 2002*

- ❑ Average loss due to Industrial Espionage (2yr period): **US\$4,200,000**

*Global Economic Crime Survey 2003
PricewaterhouseCoopers*

Stats tell us **2 out of 5** companies can expect losses of
US\$600K to US\$2,100K annually.

What are You Protecting?

Often, Industrial Espionage is limited to:

- Trade secrets, product designs, code, or formulas
- Customer/Prospect lists and sales information
- Product strategy (sales plans, new features, etc.)

Losses typically leave a trail, typically quantifiable

More important considerations:

- Loss of intangible assets, goodwill, intellectual property
- Image, intrinsic value, competitive advantage
- Ability to conduct business

Difficult to trace and difficult to quantify

What are the Costs?

- ❑ Greatest impact of loss:
 - Increased legal fees & revenue loss
 - Loss of competitive advantage
 - Market share loss
 - Embarrassment
- ❑ 70% of typical US company's value may be derived from intellectual property... not tracked in accounting... typically not well protected.

Source: ASIS International (American Society for Industrial Security, International) "Trends in Proprietary Information Loss," Survey Report September 2002.

What are You Protecting?

More than just trade secrets or new product designs

Example: Coca-Cola

Company VALUE* or WORTH
Total Market Value defined by stock price

\$123.9 Billion

Total ASSETS*
(cash, property, building, inventory, equip., etc.)
usually protected by security

\$ 27.3 Billion

OTHER VALUE?
(intellectual & intangible property, brand
equity, etc.) not tracked in accounting
usually NOT protected by security

\$ 96.6 Billion

* 2003 Coca-Cola Annual Report

© Copyright REI January 2005

Case Example

"Former GM Exec Indicted...took sensitive documents to Volkswagen," *ABCNews.com*, May 2000

- ❑ Jose Ignacio Lopez accused of copying proprietary documents & taking them to VW
- ❑ VW settled for **US\$100 Million** in cash and a pledge to buy **US\$1 Billion** worth of GM parts
- ❑ Germany required Lopez to donate \$224,845 in exchange for dropping criminal charges,
- ❑ U.S. indicted Lopez for Industrial Espionage and has requested that Lopez be extradited from Spain to stand criminal charges.

Case Example

“Oracle’s unapologetic CEO admits his spies poked through dumpsters looking for dirt on Microsoft,”
Time Magazine, July 10, 2000

- ❑ Oracle hired Investigative Group (IGI) to buy trash for \$1,200 from cleaning crew
- ❑ IGI found evidence in garbage that Microsoft had given \$200K+ to independent research group
- ❑ Oracle CEO Larry Ellison: “I feel good about what we did...we weren’t spying...its not illegal... Our job is to hurt Microsoft,” *CNET*, June 2000

Case Example

*"Windows Code May Be Stolen,"
PC World Technology, February 12, 2004*

- ❑ "Microsoft's closely guarded intellectual property now out in the open..."
- ❑ By the end of the day after the story broke, Microsoft's stock fell \$0.50 amounting to a loss in total company value of
\$ 5.395 Billion

Case Example

"Verizon sues Nextel for reputed espionage over push-to-talk," *USA Today online*, June 29, 2003

- ❑ Lawsuit alleges Nextel improperly obtained confidential information, prototype handsets, business secrets, and trade information,
- ❑ By the end of the day after the lawsuit announcement, Verizon's stock fell \$0.47, amounting to a loss in value of **\$ 1.292 Billion**

Case Example

"Boeing Managers Charged in Plot to Steal
Trade Secrets from Lockheed Martin,"
US Dept. of Justice June 25, 2003

- ❑ 141 documents (3,800 pages) belonging to Lockheed Martin recovered from Boeing Manager's offices,
- ❑ Documents related satellite launch contracts which Boeing and Lockheed were bidding,
- ❑ Total value of contracts: **US\$2 Billion**
- ❑ Aprox. **US\$1 Billion** re-assigned to Lockheed Martin
- ❑ Lockheed Martin suing Boeing

Case Example

"Huawei admits to a little copying,"
CNET News.com March 25, 2003

- ❑ Huawei Technologies admitted to using Cisco Systems' source code in its routers
- ❑ Huawei said an employee inadvertently used about 2% of the 1.5M lines of code (30,000 lines)
- ❑ Admission is "evidence that Huawei has unlawfully acquired and used Cisco's intellectual property"
- ❑ Huawei now working with Cisco's main competitor 3Com to deliver new networking gear

Case Example

*"Man Held in England in Cisco Code Theft,"
Washington Post, Sept 20, 2004*

- ☐ 20-year old arrested for theft of proprietary software blueprints
- ☐ 800 megabytes of source code made available on Russian website
- ☐ FBI is investigating
- ☐ Cisco: "we will take every measure to protect vigorously our intellectual property"
- ☐ 2nd recent Cisco incident

Case Example

"InstallShield sues competitor Wise Solutions for electronic espionage", *ComputerWorld* July 18, 2003

- ❑ Suit alleges that Wise engaged in electronic espionage on at least **903 occasions**
- ❑ Alleges that Wise downloaded files containing confidential info including **names and addresses of 109,900 InstallShield customers**
- ❑ Alleges that Wise gained unauthorized access to confidential marketing and advertising plans
- ❑ Suit seeks unspecified damages

Case Example

"Bayer sued in spy case..."

San Francisco Chronicle, July 24, 2003

- ❑ Baxter alleges Bayer obtained computer files containing key drug manufacturing secrets
- ❑ Files contained info on five leading products and information on experimental compounds
- ❑ Baxter couldn't name dollar in damages, but one of the drugs represents **\$1B annually**
- ❑ Baxter is seeking damages for actual losses, plus punitive damages and triple damages under CA's trade secret statute

Case Example

"CNA says ex-execs stole trade secrets"
Chicago Sun-Times, October 2, 2003

- ❑ Four former executives accused of stealing trade secrets for rival insurance start-up
- ❑ Stolen items include underwriting analysis, pricing strategies, & policy renewal info
- ❑ "Such information would allow a competitor to cherry-pick and undercut CNA on its most profitable customers"
- ❑ Lawsuit seeks unspecified damages

Case Example

“Japanese Man Wanted on Industrial Spy Charge,”
Newsday.com, February 2, 2004

- ❑ Researcher at Cleveland Clinic (OH) charged with stealing property related to Alzheimer’s research
- ❑ Replaced vials of genetic material with tap water, sending actual vials to research center in Japan, destroyed other biological materials
- ❑ Researcher quoted as saying he didn’t think his actions were criminal...
- ❑ Japan has refused extradition to US, indicating that man has not broken any US laws...

Case Example

Rugby "Team's hotel had been swept for bugging devices," *CNN.com*, November 18, 2003

England's Rugby Coach Clive Woodward admits:

- ☐ "We take our normal precautions which are professional and thorough..."
- ☐ "People don't understand the huge stakes that we are playing for..."
- ☐ "Its just common sense..."

Case Example

“Proctor & Gamble, Potlatch resolve trade secrets suit,”
Bloomberg News, March 14, 2003

- ❑ P&G lawsuit alleged Potlatch (maker of store brand toilet paper) stole proprietary paper-making process
- ❑ Settlement terms were confidential, but P&G said the settlement terms “do fully protect P&G’s trade secrets & proprietary information”
- ❑ P&G sued Georgia-Pacific Corp. (Quilted Northern) in a similar suit
USA TODAY, September 19, 2002

Case Example

*"...Farmers spy on competitors,"
Denver Business Journal, July 28, 2003*

- ❑ Florida Dept. of Citrus using satellites to spy on Brazil's orange crop to confirm crop estimates
- ❑ Accurate crop estimates prevent Brazil from manipulating orange juice market prices by underestimating crop yield
- ❑ FL Dept. of Citrus pays an estimated \$1M-\$1.5M for satellite information

Case Example

RV Cleaning Company wins suit over trade secrets,
The Birmingham News, September 18, 2003

- ❑ Thetford stole confidential information from Environmental Products of America (EPA), a 5-employee RV cleaning company
- ❑ Thetford used information to develop a competing product line and stole EPA's biggest customers, as part of plan to "eliminate weaker competitors"
- ❑ Thetford ordered to pay **\$6 Million** in damages for stealing confidential information

Case Example

*"Samsung bans 'spy' phones,"
BBC News online, July 7, 2003*

- ❑ Camera phones banned from factories for fear they could be used for industrial espionage,
- ❑ Samsung's Official Statement: "Restrictions reflect our (Samsung's) concerns about technology leakage and privacy"
- ❑ Samsung is world's third largest mobile phone manufacturer...
- ❑ Praised for developing first camera phone in 2000



Case Example

"Tape Recorder bugs Weatherford Friends,"
Star-Telegram,
Texas, Sept 7, 2004

- ❑ For more than 20 years, 5 members of the "Weatherford Men's Business and Professional Club" gather for lunch at the Chuckwagon Restaurant,
- ❑ The group discovered an active listening device planted under the table,
- ❑ Ongoing investigation into the device involving Weatherford College Board of trustees

Case Example

"County eavesdropping case leads to felony charge,"
The Bay City Times,
San Francisco CA, July 29, 2004

- ❑ Bay County Road Commission Finance Director accused of spying on employees,
- ❑ Pending felony eavesdropping charge facing up to 2 years in prison,
- ❑ Finance Director allowed to retire early from 20-year post

Case Example

"Suit: School phones, radios bugged,"
The Journal News,
NY, August 19, 2004

- ❑ Lakeland school district aware of scheme to secretly record telephone and radio conversations,
- ❑ Eavesdropping system purchased through no-bid contract,
- ❑ 14 Plaintiffs allege civil rights violated by secret conversation recordings

Case Example

"Trade secrets carried out in a wicker basket...",
SundayTimes, SA, August 29, 2004

- ❑ ReMax real-estate agents unlawfully acquired confidential business information and trade secrets,
- ❑ Contact lists, sensitive information about recent and potential buyer's, marketing strategies, and strategies to move in on new properties,
- ❑ ReMax agents agreed to return information,
- ❑ ReMax agents said, "They made out like we stole the Kentucky Fried (Chicken) recipe..."

Case Example Summary

- ❑ Anything and everything is a target
- ❑ These losses are reported when the loss can be documented or traced
- ❑ Also, only reported when there is something to be gained by reporting
- ❑ Reality is probably worse than these cases, real impact is probably unknown and under reported

Final Thoughts

- ❑ Malicious theft/loss of corporate information happens everyday, mostly undetected
- ❑ Stats indicate 2 out of 5 companies can expect losses from \$600K to \$2.1 Million annually
- ❑ Total financial loss is exponentially more costly than the tangible loss
- ❑ Corporations need to understand their information vulnerabilities and risk exposure (70% company value is intangible)
- ❑ Security budgets should be allocated proportionately to the risks

For More Information Contact:

Research Electronics International

+1 (931) 537-6032

800 824-3190 (U.S.)

<http://www.reiusa.net>
sales@reiusa.net