

Government, Corporate, Foreign Economic Collection And Industrial Espionage

1.0 Introduction – Current Situation:

Theft of confidential information is a multi-billion dollar underground industry in the United States. Often the loss of your secrets will show up in very subtle ways, so you should always trust your instincts in this matter. When your competitors or adversaries know things that are obviously private, or the media finds out about things they should not know, then it is reasonable to suspect technical eavesdropping or bugging has occurred. Anyone who works in a sensitive or high value organization, company or agency, can, will, or has been already targeted.

FACTS

The U.S. Department of State estimated an average of \$500 million annually is expended on purchases of eavesdropping equipment used against private persons. The U.S. Department of State also estimated an average of \$300 million annually is expended on Corporate Eavesdropping devices. The average cost spent per month on eavesdropping for one corporate entity is \$30,000 - \$50,000.

FACTS

58% of Eavesdropping technology is purchased from outside the United States. It has been estimated by the U.S. Department of State that illegal eavesdropping results in a loss of \$8.2 billion a year for U.S. corporations.

FACTS

The U.S. Department of State also estimated that a \$2.2 billion dollar annual underground industry and economy of monitoring illegal eavesdropping surveillance devices exists. Statistics shows that 70% of companies that are bugged by a competitor without being detected goes bankrupt in 24 months or less.

FACTS

Federal agents sought 1,727 warrants from the Foreign Intelligence Surveillance Agency Court (FISA) for electronic eavesdropping and physical searches last year. Radio Frequency jammers are the best defense against electronic bugs. Lasers are now used in electronic eavesdropping. The biggest drawback is alignment of the laser beam. There are estimates now that state over \$950 million in illegal eavesdropping equipment is sold each year in the U.S. alone.

FACTS

The U.S. Department of State estimated an average of \$500 million annually is expended on purchases of eavesdropping equipment used against private persons. The U.S. Department of State also estimated an average of \$300 million annually is expended on Corporate Eavesdropping devices. The average cost spent per month on eavesdropping for one corporate entity is \$30,000 - \$50,000.

2.0 Who is at Risk – We Identify Your Threat:

Could someone be listening-in or watching you? Absolutely! If you believe that an eavesdropper requires a large, complicated transmitting device, or that listening devices are only used by secret government agencies, or that the devices cost thousands of dollars, you are wrong! Many "police-grade" bugs and taps are presently being offered to the general public by a number of firms for incredibly low prices, and many are smaller than an inch in diameter.

The manufacture, sale, installation, and monitoring of illegal surveillance devices is a multi-billion dollar underground industry within the United States. The significant decrease in cost and the increased availability of this equipment has made electronic bugging all too common. In a study completed by the U.S. State Department in 2000, it was estimated that at least \$800 million dollars of illegal bugging and eavesdropping equipment is imported and installed in the United States each year. The majority of this equipment is illegally imported from France, Germany, Lebanon, Italy, Canada, Israel, England, Japan, Taiwan, South Africa, and a host of other countries. In the United States, over six million dollars worth of surveillance devices are sold to the public each day. Most of these products are sold by storefront operations, spy shops, attorneys, and private investigators located in major metro areas such as New York, Miami, Los Angeles, San Francisco, Dallas, Chicago, and Minneapolis. This does not include the tens of billions of dollars spent each year for legitimate eavesdropping products purchased by law enforcement, military, and intelligence agencies.

3.0 Background - Exactly What Is Out There:

This equipment is commonly sold over the counter, via mail order, and through the Internet. Most of these bugging devices cost only a few dollars, but highly sophisticated, quality products may be purchased for less than one thousand dollars each. In New York City alone there are a significant number of companies which will not only sell you the eavesdropping device, but will break into the target's office to install the device, and for an additional fee, will provide a monitoring and transcription service. Additionally, anyone with a soldering iron and a basic understanding of electronics can build and install an eavesdropping device. Numerous books are available through book retailers such as Amazon.com. In addition, plans and schematics for these types of devices are available on the internet. These plans range from a very simple wireless microphone to

elaborate infrared audio transmitters. The raw materials needed to build these devices are easily obtained at Radio Shack, or salvaged from consumer electronic devices such as cordless telephones, intercom systems, and televisions. Bugs, wiretaps and covert video surveillance are all techniques used to gather intelligence, trade secrets and other valuable information and intellectual property. These techniques are typically called espionage, which is the act of gathering information illegally. It is important to note that computer hacking has become the method of choice for espionage.

3.1 Electronic Bugging Brief:

Surveillance equipment once originally intended for use by law enforcement, military, and intelligence agencies, are now being sold in record numbers over the counter, via mail order, and through the Internet. Most of these bugging devices cost only a few dollars, but highly sophisticated, quality products may be purchased for less than one thousand dollars each. In New York City alone there are a significant number of companies which will not only sell you the eavesdropping device, but will break into the target's office to install the device, and for an additional fee, will provide a monitoring and transcription service. Additionally, anyone with a soldering iron and a basic understanding of electronics can build and install an eavesdropping device.

Electronic Bugs

Bugs can be hidden in any type of device, container, or vessel that could typically be found in the targeted area. The RF bug is extremely easy to detect, is inexpensive, disposable, and difficult to trace back to the person who planted it.

Radio Frequency - A Radio Frequency or RF bug is the most well known type of bugging device. A radio transmitter is placed in a specified area or site for best vantage of the intended target. This bug can be activated by voice or internal device, remotely, or on a schedule timer.

Optical - An Optical Bug is a bugging device that converts sound (or data) into an optical pulse or beam of light. It is rarely used, expensive, and easy to detect. The beam from some of these devices resembles that of a common laser, and is easily seen by the naked eye. A good example of this would be an active or passive laser listening device.

Hybrid – Hybrid devices are the newest category of electronic bugs. A good example of this is a key capture device, connected between a keyboard and a computer. As the computer user types away, the key capture device stores each keystroke and sends it via the internet to a listening point. It is important to note the wireless keyboards are extremely susceptible to covert eavesdropping. An "Electronic Bug" is a device that is placed in an area for the purpose of intercepting communications and transfers that communication to a remote listening point. The eavesdropper can be just a few feet to a

few hundred feet or even miles away from the target, depending on what device is used. The following paragraphs describe five primary categories of "Bugs".

Acoustic – An acoustic bug involves directly intercepting a communication with the naked ear (without the use of electronics). It might involve using a water glass, stethoscope, or rubber tube to intercept the sound, or relies on sections of a physical area where sound is leaking through soft spots around windows, structural defects, ventilation structures, poorly installed power outlets, and so on.

Ultrasonic - An ultrasonic bug is a device used to convert sound into an electrical signal above the range of human hearing. The ultrasonic signal is then intercepted at a nearby location, and converted back to audio sound.

Warning Signs of Covert Eavesdropping or Bugging

Corporate spies find new soft targets. How would you like the new emerging technology you have been working on for a defense contract or plans for future corporate takeovers you are planning to become public knowledge? Would copies of your product designs be of any use to your competitors? Would it be beneficial for your competitors to know how much you are quoting for the same project? You are a potential target. Could eavesdropping on anything you say, write, or do increase someone else's wealth or influence? If the answer is yes, you are a potential target. The higher the value of your information, the more likely it is that you are a target.

4.0 Here Are Some Questions To Ask Yourself:

Do others seem to know your confidential business or professional trade secrets? Theft of confidential information is a multi-billion dollar underground industry in the United States. Often the loss of your secrets will show up in very subtle ways, so you should always trust your instincts in this matter. When your competitors know things that are obviously private, or the media finds out about things they should not know, then it is reasonable to suspect technical eavesdropping or bugging.

Does information about closed meetings and bids seem to be widely known? Confidential meetings and bids are very popular targets for corporate spies. How would you like the plans for the corporate takeovers you are planning to become public knowledge? Would copies of your product designs be of any use to your competitors? Would it be beneficial for your competitors to know how much you are quoting for the same product or performance?

Have you noticed strange sounds or volume changes on your phone line? This is commonly caused by an amateur eavesdropper when they attach a wiretap, or activate a similar listening device. Surveillance devices often cause slight anomalies on the telephone line such a volume shift or drop-out. Professional eavesdroppers and their

equipment usually do not make such noises. If this is going on it could indicate that an amateur eavesdropper is listening in. On the other hand, you could simply be experiencing a flaw in the line, but you should check it out.

Have you noticed static, popping, or scratching on your phone lines?

This is caused by the capacitive discharge which occurs when two conductors are connected together (such as a bug or wiretap on a phone line). This is also a sign that an amateur eavesdropper or poorly trained spy is playing with your phone lines.

Are sounds coming from your phones handset when it's hung up?

This is often caused by a hook switch bypass, which turns the telephone receiver into an eavesdropping microphone (and also a speaker). If you hear sounds in your handset, there is probably somebody listening to everything you say or do within twenty feet of the telephone.

Does your phone often ring and nobody is there, or a very faint tone or high pitched squeal/beep is heard for a fraction of a second?

This is an indicator of a slave device, or line extender being used on your phone line. This is also a key indicator of a harmonica bug, or infinity transmitter being used. These devices cause your phone to ring randomly. When you answer, the device emits a faint tone and/or squeal/beep as it re-verifies your user information.

Does your other electronic equipment suddenly develop strange interference?

Many amateur and spy shop eavesdropping devices use frequencies within or just outside the FM radio band. These signals tend to drift and will "quiet" an FM radio in the vicinity of the bug. Look for the transmissions at far ends of the FM radio band, and at any quiet area within the FM band. If you find a quiet band and the radio begins to squeal, and then slowly move it around the room until the sound becomes very high pitched. This is referred to as feedback detection or loop detection and will often locate the bug. The "stereo" function should be turned off so the radio is operating in "mono" mode, as this will provide a serious increase in sensitivity. If you find a "squealer" in this manner then immediately contact a security professional and get them to your location FAST.

Does your television suddenly develop strange interference?

Television broadcast frequencies are often used to cloak an eavesdropping signal, but such devices also tend to interfere with television reception (usually a UHF channel). Televisions also "draw in" a lot of RF energy and, because of this, are very sensitive to any nearby transmitters (this is technically called "Bandwidth" and TV signals use a lot of it). A small handheld television with a collapsible antenna may be used to sweep a room. Carefully watch for interference around channel numbers 2, 7, 13, 14, 50-60, and 66-68 as these frequencies are very popular with eavesdroppers.

Have you recently been the victim of a burglary, but nothing was taken?

Professional eavesdroppers often break into a targets home or office, and very rarely leave direct evidence of the break-in; however, occupants of the premises will often "pickup on something not being right" such as the furniture being moved slightly.

Do electrical wall plates appear to have been moved slightly or jarred?

One of the most popular locations to hide eavesdropping devices is inside, or behind electrical outlets, switches, smoke alarms, and lighting fixtures. This requires that the wall plates be removed. Look for small amounts of debris located on the floor directly below the electrical outlet. Also, watch for slight variations in the color or appearance of the power outlets and/or light switches as these are often swapped out by an eavesdropper. Also note if any of the screws which hold the wall plate against the wall have been moved from their previous position.

Has a dime-sized discoloration suddenly appeared on the wall or ceiling?

This is a tell tale sign that a pinhole microphone or small covert video camera has been recently installed.

Has anyone recently given you any type of electronic device, such as a desk radio, alarm clock, lamp, small TV, boom box, or CD player?

Many of these "gifts" are actually Trojan horses which contain eavesdropping devices. Be very suspicious of any kind of pen, marker, briefcase, calculator, "post-it" dispenser, power "post-it" dispenser, power adapter, pager, cell phone, cordless phone, clock, radio, lamp, and so on that is given as a gift. That little gift the salesman left for you may be a serious hazard.

Has a small bump or deformation appeared on the vinyl baseboard near the floor?

This is a strong indicator that someone may have concealed covert wiring or a microphone imbedded into the adhesive which holds the molding to the wall. Such deformation will often appear as a color shift, or lightening of the color.

Does the smoke detector, clock, lamp, or exit sign in your office or home look slightly crooked, or have a small hole in the surface, or has a quasi reflective surface?

These items are very popular concealment's for covert eavesdropping devices. Often when these devices are installed at a target location they are rarely installed straight. Check these items for slight changes in their appearance, and watch out for items like this that "just appear".

Have you noticed white dry-wall dust or debris on the floor next to the wall?

This is a sign that a pinhole microphone or video camera may have been installed nearby. It will appear as if someone has dropped a small amount of powdered sugar either on the floor, or on the wall.

Have you noticed small pieces of ceiling tiles, or "grit" on the floor or on the surface area of your desk?

This is a prime indicator that a ceiling tile has been moved around, and that someone may have installed a hidden video camera or other eavesdropping device in your office or near your desk. Also, watch for cracks or chips in the ceiling tiles. Amateur and poorly trained spies tend to crack or damage acoustical tiles. The ceiling tiles in any executive area should never contain any cracks, nicks, gouges, or stains. Any ceiling tile that becomes damaged (for what ever reason) should immediately be replaced and the cause of the damage documented.

Have telephone, cable, plumbing, or air conditioning repair people shown up to do work when no one called them?

This is a very common ruse which eavesdroppers use to get into a facility. They fake a utility outage, and then show up to fix the problem. While they are fixing "the problem", they are also installing eavesdropping devices. Some of the more popular outages involve power, air conditioning, telephone, and even the occasional false fire alarm.

Have you noticed that your door locks suddenly do not "feel right", suddenly start to get "sticky", or have completely failed?

This is prime evidence that the lock has been picked, manipulated, or bypassed. Try to always use biaxial locks with sidebars (such as ASSA or Medeco). Also, only use double sided deadbolts in all doors, good quality window bars on all windows, and a good quality door bar on all doors that are not used as primary entry doors.

Has your furniture recently been moved slightly, and no one knows why?

A very popular location for the installation of an eavesdropping device is either behind, or inside furniture (couch, chair, lamp, etc.) People who live or work in a targeted area (such as large cities and/or corporate and government buildings) tend to notice when furnishings have been moved even a fraction of an inch. Pay close attention to the imprint which furniture makes on rugs and the position of lamps shades. Also, watch the distance between furniture and the wall, as eavesdroppers are usually in a hurry and rarely put the furniture back in the right place.

Have things recently seemed to have been "rummaged" through?

A "less than professional spy" will often rummage through a targets home for hours, but very rarely will they do it in a neat and orderly fashion. The most common "rummaging" targets are the backs of desk drawers, the bottom of file cabinets, closets, and dresser drawers.

Have you received a copy of your private conversations?

As simple as it seems, this is the strongest indicator, and solid proof of eavesdropping. An eavesdropper will sometimes send a victim a copy of a private conversation that they intercepted in an attempt at blackmail, or in an attempt to terrorize or to stalk the victim. This is commonly seen in civil lawsuits, criminal court cases, marital problems, shareholder disputes, custody battles, and other situations where one side has a position of weakness and is trying to physiologically undermine their opponent. While there are

many different things to look for, the key to success is to look for things that should be there and aren't, and to look for things that should not be there and are! If any of the multiple warning indicators above apply and you are concerned about eavesdropping or wiretapping, then it would be wise to take immediate action.

4.1 What To Do If You Think You Are Bugged:

Special precautions and behaviors must be practiced if you suspect bugging or wiretapping. The following should be used as a general guide if you believe you have been bugged.

Immediately contact an electronic bug detection specialist. Handle the logistics of the inspection away from your office.

Use a phone away from your office or home. Never call from any type of cordless phone, cellular telephone, Personal Communications Service (PCS) phone, or any other type of wireless device.

Consider having a complete sweep of the suspicious location. Have someone who specializes in technical counterintelligence do a bug sweep and make sure that this person is an expert with computers, telecommunications, and electronics.

Be Very Discreet... Watch what you say at home or at the office, and never discuss your concerns inside, outside, or near any suspect facility, any overt attempt on your part may be interpreted as hostile by the eavesdropper, and either ward them off for the time being or send them underground or worse yet deeper into your organization masking the problem

4.2 What NOT To Do If You Think You Are Bugged:

DO NOT use your office telephone to talk about your suspicions.

DO NOT use your cellular or cordless phone to talk about your suspicions.

DO NOT discuss your suspicions at the office, in your car, or at home.

DO NOT purchase a spy shop bug detector.

DO NOT send e-mails about your suspicions.

DO NOT try to find the bug or wiretap yourself.

DO NOT contact the telephone company.

DO NOT contact the FBI/Secret Service.

DO NOT try to get the local police to help.

5.0 How Will Key Stakeholders React?

This is extremely important to corporations as well as civilian and government agencies, as the hint of covert activities or risks might affect the valuation or credibility of the company, or organization of its services that it provides. Knowing that its inner most secrets have been compromised not only effect short term goals but could also effect local and national security. In addition, legal requirements like Sarbanes-Oxley, SAS #99 and the Industrial Espionage Act of 1996 have increased the visibility surrounding electronic eavesdropping.

5.1 Stakeholders To Consider Are:

Investors—Stockholders of publicly traded companies will consider the impact on the stock price (market cap).

Customers—Both Government or Civilian Customers will be concerned about loss of personal information and identity theft (a very hot topic today) as well as compromised security technology that could be exploited against our country.

Suppliers—Suppliers will be concerned that their confidential information or pricing may have been exposed.

Employees—Employees will be concerned about loss of personal information and identity theft (a very hot topic today)

5.2 What Is The Impact Of The Information That May Have Been Compromised?

Each bugging incident is different. The effect of the incident is dependant upon the value of the information that is available and garnered. Additionally, the use of the information that has been accessed must be evaluated. The following questions must be asked:

- ◆ What is the national or commercial value of the information?
- ◆ Could the information be used by criminals or with criminal intent?
- ◆ Who stands to gain from having access to this information?
- ◆ Who has a motive to have done this?
- ◆ Who has access to the area where the device was found?
- ◆ Has anyone's personal security been put at risk by any of this information?

All these questions must be answered to construct a plan to deal with an electronic bugging incident. Failure to follow the guidelines included here has the potential to compromise an investigation and further exposes the organization to other breaches in security.

5.3 Frequently Asked Questions:

Q - What percent of electronic sweeps find bugs?

A – The number of successful sweeps is estimated at 9%. This is due to poor training, outdated equipment and advances in the bugging devices themselves.

Q – What is the most widely know bugging incident.

A – Watergate - in the early morning of June 17, 1972, five men are arrested for breaking into the Democratic National Committee headquarters at the Watergate.

Note: There are no accurate statistics collected by any public or private organization.

These answers represent the combined experience of three firms and decades of work.

Bugging methods vary widely as does the type of bugging device.

Anyone with information or data that someone else feels is of value is a potential target.

Everyone has enemies (foreign governments, terrorist groups, competitors, activists, disgruntled employees and customers, disloyal partners, unions v. management, management v. unions, etc., etc.) and Eavesdropping congers up images of shadowy figures in trench coats lurking about conducting suspicious activities. But in the high tech world of today, that could not be further from the truth. In order to help you understand electronic bugging, here are some frequently asked questions:

Q - How hard is it to buy an electronic bug?

A – Not hard at all. You can even make them from components from Radio Shack.

Q - What are the most common types?

A – The tape recorder with a wireless microphone that is good for about 300 feet.

Q - How many electronic "bugs" are planted per year?

A – No one really knows, but it is believed to be in the hundreds of thousands worldwide.

Q - What percentage is used in business?

A – It has been estimated that 63% of electronic bugging devices are used for Corporate Espionage.

Q - What percentage is planted by foreign sources?

A – 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.

6.0 Summary:

If you wait until the attack takes place to protect yourself, the survival price tag will be extremely high, and you may not even be successful. You need to detect pre-attack signs of intelligence gathering (eavesdropping) BEFORE the attack. At this stage, security is both cheap and effective, knowing that an eavesdropper could have their home, office, car or other facilities bugged at any time. Remember this, all properly conducted sweeps are productive, it is less expensive to protect against them by deflection than to incur the expense of lost information and the bad publicity caused by a compromise.

The effectiveness of your overall privacy and security require the immediate implementation of Eavesdropping Countermeasures to ensure that these devices are not active in your homes, cars and workplace. We have industry experts across the intelligence and operational communities already standing by to support Department of Homeland Security, Department of Defense and Department of State as well as the Private Sector that are committed to providing this level of counter surveillance security to your organization.

For more information please visit: www.ComSecLLc.com The ComSec LLc point of contact for any questions related to this matter is Mr. J.D. LeaSure- at Ph: 757-615-7053 or via email at CEO@ComSecLLc.com

