



Corporate Eavesdropping

Eavesdropping on corporate secrets is big business.

Your competitors, and those seeking to hurt your organization, will go to any length to gather your privileged and confidential information concerning data about products, new releases, pricing, strategies, organizational re-structuring, financial structuring, etc. Corporate offices, private meetings, corporate computers, and even the homes of executives could be "bugged".

- It is estimated that \$376 million dollars are spent every year to purchase devices to "bug" corporate targets.
- 56% of the equipment used for eavesdropping is purchased from outside of the country.
- The average cost spent to eavesdrop on one corporate target is \$57,000.
- The US Department of State estimates that 8.2 billion dollars is lost annually due to illegal eavesdropping.

Technical Surveillance Countermeasures

Initial Assessment of Risk Level. Our team will estimate the level of countermeasures required by reviewing the type of sensitive data at risk and by looking to see which security weaknesses could be exploited.

Determining likely sources of electronic surveillance. Given the physical setup of the target, we will estimate what eavesdropping equipment might be employed and develop countermeasures to screen for them (Sweeps). Depending on the initial assessment, this can involve simple monitoring during a sensitive meeting, repeated site examinations, or continuous on-site monitoring.

Follow-up countermeasures. We will then determine what measures should be taken to keep your risk level at a minimum. This usually entails determining how frequently the area should be re-screened, as well as determining what future events are most at risk.

Sweeps

A "Sweep" is a process of countermeasures employed to detect and neutralize "bugging" devices.

We provide both basic and extensive service. The level of service is defined based upon the degree of your eavesdropping risk. Based on this information, we recommend the best course of action to reduce that risk.

Below are a few of our "Sweep" methods:

Conference monitoring: Room(s) are "swept" to be certain no surveillance equipment is present. During the meeting, surveillance is continued so that unauthorized transmitters or cameras (which generate RF waves) can be detected.

Photography: The room is photographed to check if anything has moved or is different when compared with previous photos.

Telltails: A detailed marking system is utilized to insure that nothing has been moved - a possible clue to a new installation of bugging devices.

Telephone Line Monitoring: We have developed technology that alerts us of any line tampering that may have occurred during the time between TSCM exams.

Radio-frequency Detection Equipment: We use OSCOR (Omni-Spectral Correlator) for radio frequency and telephone line monitoring.



Are you bugging yourself?

No one would voluntarily put themselves or their corporation at risk, but many people do unknowingly. Adopt the following low-key measures immediately:

1. Be wary about what you say around:

- Cordless Telephones
- Cordless Microphones - frequently used in business presentations
- Cellular Phones

The above items all function as "short or long range radio transmitters." Cordless telephones or microphones can send a signal from 1/4 to 1/2 a mile beyond your office, with cellular phones being able to transmit much further. With the proper equipment, it is not difficult to listen in through these devices. When the above items are on and transmitting, all spoken data is automatically exposed.

2. Change your voice mail code frequently.

Since the messages on voice mailboxes are "password protected", hackers can gain access without you knowing. Your code is the vulnerable part of your voice mail system, and a great deal of information can become susceptible to loss through this system.

3. Take the following precautions when using fax machines and dictation tapes.

- Remove the tape from any fax machine whenever valuable information is sent. Many fax machines make their copies using a continuous carbon copy tape.
- Many fax messages are sent after hours - which places them in the bin and makes them susceptible to theft. The timing of a fax is important when you are transmitting sensitive messages.
- Erase or lock-up dictation tapes after they are used. Second copies can always be created from these tapes, it is not enough to secure the printed copy.

While these are ways to protect yourself from minor security risks, if you believe your company has a higher than normal risk factor, or you have noticed privileged information becoming public a "Corporate Sweep" may be necessary.

Time Domain Reflectometry: TDR equipment can create an "EKG-like" picture detailing the activity within your phone line. Repeat checks could identify splices, cuts, or even wires moved apart since the last sweep. This type of sweep can be done from outside of the building.

Carrier current devices: Special receivers are used to detect bugging devices that are using power lines to transmit information. We use a similar type of technology to jam the devices that are transmitting your information.

Devices to prevent telephone line recording: We can jam phone lines using a device that emits a sophisticated counter-sound that is unnoticeable so that normal conversations are not disrupted. This counter sound also prevents recorders from operating.

Filter on Phone/Computer Lines: This filter stops transmissions and neutralizes bugging technology. Without this filter, your phone line can be converted into an antennae which can then broadcast your private conversations.

Acoustic Noise Generators: Acoustic noise generators produce white noise to defeat hidden microphones (acoustic, ultrasonic, IR, and RF "cloak" are available as needed)

[Contact us](#) if you believe that you have a problem. We will meet with you in a secure environment to review your concerns.

If you believe that you are being monitored, contact us from outside of your office building.