White Paper

"Protecting Corporate and Personal Information Assets Against Industrial Espionage"

A 10-point counter-measures program for detecting, and eliminating info-theft via electronic bugs -- with information that you can start using immediately.

Recommended Best Practices
Your 10 Step Counter-Measures Program

1. **Determine Your Vulnerability.**

Do you have information you wish to keep private? Could others profit from it? Do you shut doors to conduct meeting and phones conversation in private? Could the loss of proprietary trade or other secrets damage your business or reputation? Could others sue you because of negligence? If so, then you may be vulnerable, and it's best to take steps to ensure that you are taking this grave threat seriously.

2. **Verify your Threat Level.**

While at the site, please review the contents, especially the sidebar and services page on the various Threat levels. Your threat level will indicate how urgent (potentially) your situation is. Combining this information with step one should make it clear exactly where you stand.
Action Steps: Make a rough assessment, and consider the results carefully.

3. **Get Informed**

Most people are either misinformed, or uninformed about electronic surveillance, so it's best to get informed. Please review the site, do some Google searches, and read up on the subject, following your interests, hunches, instincts and suspicions. Then, re-assess your earlier ideas, just to be sure that you are neither overcompensating, nor worrying needlessly, nor in denial—which can be dangerous.
Action Steps: Make a decision as to whether you need to take further action—only you can tell. At this point, it's best not to discuss the matter with anyone else. If you feel that you are vulnerable, and that the threat risk is high, OR IF YOU ARE UNCERTAIN, it's best to consult an expert. Look for a company that specializes in electronic counter-surveillance sweeps only; and one that provides a range and depth of sweeps suitable for your needs. If regular sweeps are not being preformed, chances are you do not need a sweeps costing tens of thousands dollars to sniff out the most sophisticated of bugs. Eavesdroppers can achieve excellent results with low cost bugs and simple rudimentary installations, for obvious reasons.

4. **Consult an Expert**

If you feel that you are vulnerable, and that the threat risk is high, OR IF YOU ARE UNCERTAIN, it's best to consult an expert. Look for a company that specializes in electronic counter-surveillance sweeps only; and one that provides a range and depth of sweeps suitable for your needs. If regular sweeps are not being preformed, chances are you do not need a sweeps costing tens of thousands dollars to sniff out the most sophisticated of bugs. If the planter of such devices can achieve excellent results with low cost bugs and simple rudimentary installations, they will do so for obvious reasons.
Action Steps: Review the information in the site to determine what to look for in a security company. Then look in the yellow pages, the Web, and elsewhere for a provider that best suits your needs—we may or may not be your best choice, and we're fine with that. We're more interested in ensuring that YOU get the protection

you need. This paper is part of our mission and mandate to inform the public. Even if you contact us, we may refer you elsewhere if we are not the right service provider for you. Please exercise your best judgment, and shop around if needed.

5. **If Vulnerability Index, High, Get A Full Professional Assessment.**

If your expert confirms your assessment, then it's best to get a full professional assessment of your situation. Knowing *exactly* where you are vulnerable and to whom is an essential step in all sectors of security. While these services will have a nominal cost, it will greatly reduce the overall cost of conducting sweeps, as you do not waste time and money on unnecessary areas, and only focus on the most likely sources—something only a trained expert can advise you on.

Action Steps: Review your assessment to decide what depth of 'sweep' you need. *PLEASE LIMIT YOUR DISCUSSIONS TO THE SMALLEST NUMBER OF INDIVDUALS, IDEALLY TRUSTED PEOPLE WHOSE APPROVAL OR INVOLVEMENT YOU ABSOLUTELY REQUIRE TO TAKE SUBSEQUENT STEPS, AND PLEASE CONDUCT DISCUSSIONS IN A SECURE LOCATION OR MANNER RECCOMMENDED BY YOUR EXPERT.*

6. **Keep Your Budding Counter-Surveillance Program Secret!**

Once you decide to perform a sweep, and start shutting off various easy avenues to eavesdroppers, and clearing any areas or objects recommended by your expert, do not discuss these plans with anyone. Otherwise you may alert eavesdroppers to remove or turn off equip. Also, even hint of bugging, or IE, may make shareholders nervous.

Action Steps: Perform all steps involving others on a "need to know" basis.

7. **Start Planning Ahead For Meetings etc.**

Boardrooms are accessed and attended by many people and sensitive information is shared in them. If you do not want the information leaving the room, precautions must be taken. Often the room should be swept, if only to look for devices that may have been covertly 'left behind,' such as:

A) Cell phone (which can be put in silent mode and then called to activate once the meeting has begun—a very simple and common bugging method; zB) Digital cameras (for a few dollars more, many manufactures offer remote-control devices to take auto-snap photos or turn on video mode. Many can operate over 100 feet away, much like remote door locks on most cars that can easily be activated from elsewhere in the building or on the street);

C) Wireless mikes should not be used. Their transmission signal is easy to pick up with a simple Radio Shack scanner;

D) Unplug all speakerphones (mikes can be turned on remotely without any indications that phone is in use, and your meeting can be listened into from anywhere in the world, in much the same way that a person can call in to listen to messages on an answering machine.

Action Steps: Train yourself and key personnel in informal sweeping and safety protocols such as these, as well as those recommended by your expert. These should

become as habitual as turning on security alarms, locking doors, and keeping computer anti-virus programs updated.

8. **Perform Professional Initial Sweep.**

Have at least one sweep performed professionally that focuses on the most common bugs and the frequency ranges to ensure you are truly starting with a 'clean slate."
Action Steps: Supervise sweep and personally review results to ensure that you know what's involved and how to interpret the sweep result accurately.

9. **Document Your Due Diligence**

Document your action steps via any means available, (for example, sending date and time stamped notes, or e-mails to a remote account) and request an official written report from your solution provider to verify that you have taken measures to prevent proprietary trade secrets in case of litigation for negligence by partners and shareholders
Action Steps: Start a habit of documenting your due diligence—it just may save you serious consequence down the line.

10. **Develop and Put Security Infrastructure and Maintenance Plan in Place.**

Plan for full and/or partial sweeps in the future, or more in-depth sweeps if this is deemed necessary. Discuss whether other areas may be of concern such as car, home office, lab, research and marketing department etc. with your expert, and decide whether additional steps need to be taken, and maintenance or ongoing sweeps performed.
Action Steps: Base your maintenance and regular check-ups on your needs and the recommendations of your expert. Personally ensure that ongoing safety protocols, internal sweeps, and regular professional sweeps are conducted as required for your vulnerability and threat level.

If you take the above steps in a diligent manner, and use a trained expert, you will have dramatically reduced the likelihood of wire-tapping and covert audio/video surveillance in your place of business. But remember: no one can guarantee a perfect sweep—there is no such thing. However, if you have taken the steps and documented your work, you have done your best, and what is humanly possible by acting responsibly to safeguard your companies' intellectual and information assets.

10 Potential Signs of Wire-tapping and E-Surveillances PLUS General Tips

The Signs:

1. Sudden loss of expected business, contracts etc., due to unexpected competition. Possible causes: bid information leaked, or accessed.
2. Employees seem to possess information that is supposed to be restricted
3. Competitors seem to possess information that is supposed to be restricted.
4. Any situation where there is dramatic loss of strategic advantage, from labour negotiations, to marketing campaigns, etc.
5. Any situation in which competitors seem to possess proprietary products, technologies.
6. Unusual noises on telephone lines, voice mail, answering machines.
7. Items moved in supposed secure locations, like offices, boardrooms.
8. Free, unexpected gifts from known or unknown sources in a boardroom, or private office.
9. Ventilation or air vents, or heating vents problems.
10. Unexpected tradesmen in private areas.
11. Home office intrusion—break-in, or suspicious activity.

Tips:

1. Trust your instincts—we often sense the problem before finding the evidence.
2. Question internal changes such as new furniture or items in key offices that have been moved— even slightly—or out-of-place.
3. Look for ceiling tile dust on floor or desk—in case someone's been up there.
4. Carefully examine business gifts, especially electronic items such as phones, clocks and lamps. Also: gifted pens, and various office toys—many bugs come disguised as innocent, common business items.
5. Make a list of who has access to your office. This includes all staff members, plus cleaners, maintenance people, building managers/landlords.
6. Make a similar list for those who have access to your telephone room/communications room. Also a list for the telephone rooms that are shared in the building. In most office buildings, one is on each floor that is common to the whole floor, and one is in the basement that is common to the whole building. The most vulnerable businesses are on the top floor because all the communications pass through all floors to reach them.
7. Be aware of air vents and ceiling vents. Acoustic leakage is one of the oldest types of eavesdropping, common for thousands of years, and in part responsible for the term 'eavesdropping' (throughout the years, stories have been told of savants/staff being able to hear what goes on in other parts of the house by merely putting an ear to a vent or pipe).
8. Question trades people on premise. Did your office call them, or are they showing up just claiming to be working elsewhere in the building, but your area/office was required to do their work? Most of the time, these are legitimate reasons, and your space is restricted, and it is wise to be aware never-the–less.

9. Be aware of changes to your phone system performance. It could be a simple problem with the system, or it could be caused by a wiretap or illegal electronic parasite.
10. Be aware of changes to reception to radio stations, TV or cell phones. These are often indicators of RF (radio frequency) bugs interference.