

Tap Sweep

Protecting Your Information Edge

Executive Briefing

“Protecting Corporate and Personal Information Assets Against Industrial Espionage.”
A 10-point counter-measures program for detecting, and eliminating spying via electronic bugs.

By

Steve Parkin
Certified Counter-Surveillance Solution Provider
President/CEO of **Tap Sweep Counter-Surveillance Services**

Table Of Contents

Abstract

Industry Overview

Solution Provider Overview

Tap Sweep Solution Overview

Detailed Services Breakdown

Conclusions

Appendix A—10 Potential Signs of Wire-tapping and E-Surveillances & Tips

Appendix B--Recommended Best Practices--The 10 Step Counter-Measures Program.

Abstract

Industrial espionage, especially via covert video and audio surveillance is growing at alarming rate, due to an unregulated electronics industry, and corporations that are largely unaware of the threat. Theft of sensitive, critical information can cripple or destroy a company or individual, especially in small to medium sized enterprises, leaving CEOs responsible and liable.

How do SMEs protect themselves against this problem?

This Executive Briefing provides an expert's overview of the problem, the solutions and resources currently available to decision-makers, and basic frameworks, recommendations and best practices for developing and launching an effective counter-surveillance program.

Industry Overview—A Map of The Hazards

We live in an information-based society. Whether it is price bids in a proposal or RFP, strategic marketing information, labour/employee negotiations, or proprietary technical knowledge, whoever controls this information, controls the competitive edge. This makes certain kinds of information extremely valuable, and therefore a target for those who would steal it for profit.

Industrial espionage has a long and colorful history, and the fundamentals are the same now, as then: covert eavesdropping with the intent of using stolen information to the disadvantage of the original owner. However, some things have changed dramatically. Due to technological advances, the devices used in eavesdropping today have become:

- 1) Remarkably small, extremely powerful, and often so easy to “disguise” as to make them virtually undetectable—except by a properly trained and equipped expert
- 2) Inexpensive and easy to acquire. Often a short trip to a local “spy shop” or the Internet, or a trade magazine’s classified section, is all that’s required for even an amateur to purchase and deploy a powerful surveillance device capable of transmitting audio and video information across vast distances, or even using a company or individual’s ***own*** phone line to eavesdrop in offices and boardrooms where sensitive information is being discussed, and to transmit it to a remote location.

How rampant or serious is this problem? The US Department of State estimates that over \$512 million of **illegal** eavesdropping and bugging equipment is installed in US Corporations *each year*. They also estimate that the damage caused by this type of industrial espionage at over \$8.16 billion. Below are some additional, alarming facts:

“72% of businesses that have NOT taken measures to reduce vulnerability to industrial espionage and suffer a loss will go out of business within 2 years”

(CSIS /National Counter Intelligence Centre.)

“Even a whiff of such a security breach can cause a company’s stock prices to tumble or a deal to fall through”

Dr. Robert Ing, Leading Canadian Counter-Intelligence Specialist.

“42% of companies responding to polling confirmed they had NOT reported incidents of corporate espionage to authorities.”

National Counter Intelligence Centre.

What makes these statistics even more remarkable is that the above-quoted studies on equipment sales were conducted in 1997. Keeping in mind the rapid pace of technological advance, it does not take much to imagine what these figures would be today.

What is driving this explosive trend? Several core trends drive or contribute to this problem:

1. Technology developers—governments, or companies supplying governments—focus on *creating* products, not regulating or restricting their use, or protecting the public as much as they should. And, with the acceleration of micro-technology and wireless telecommunications, products and components quality is now exceptionally high and significantly less expensive. Also, the technological basis for these devices is easy to access by the unscrupulous. Certainly nothing like the legislative disincentives that exists for computer hacking, for example, exists for wire-tapping or other forms of covert electronic surveillance.
2. The increasing demands of an aging population are providing developers much incentive to develop better micro-transmitters and receivers for the soon to boom hearing aids industry. And, technical advancements in video recording has become so affordable it is included in most new cell phones, whether one wants it not. And this wireless revolution is not just limited to cordless/cellular phones and computer routers: one can now purchase wireless security cameras for well under a hundred dollars; intercoms and microphones are broadly used in home and work environments, simple fm transmitters for sending music from iPods to car stereos and around the house abound; we’re unlocking car doors and changing TV channels with radio frequencies that transmit through walls. Society has become so familiar and comfortable with these devices that we are even monitoring our own babies—which technology, ironically, is often used in Industrial Espionage, and sufficient to bring down an individual or company.
3. The victims—anyone who owns or controls valuable information from product inventors, to companies in competitive situations or negotiations, to lawyers with access to critical information, to politicians with strategic secrets (the list of vulnerable professions and businesses is long), are woefully unaware of the threat, or of how to counter it. Indeed, very few companies or individuals who might suffer from information theft, take it as seriously as computer-based crimes, or human “leaks,” which essentially leaves an entire electronic-spectrum unprotected.
4. Few trained solution-providers exist, and the industry as a whole is under-regulated. Currently, the only options are a hodge-podge of large security firms that “also provide counter surveillance services” among its numerous high-priced offerings, usually to large corporations, and private investigators who may or may not have adequate training, or

even the proper equipment to detect wire taps, or audio/video bugs, the most commonly used eavesdropping devices.

For small and medium sized businesses that are aware of this threat, or already victimized, this means few viable resources to help avert further damage. While the costs and consequences of **not** taking action, **not** being aware, or **not** taking appropriate steps are often swift, serious, and increasingly devastating to a company or individual: loss of market share or proprietary material, stock holders and industry reputation, brand value, to actual negligence or liability charges for decision-makers.

In such an environment, how do small and medium enterprises and individuals protect themselves? How do they know if they are vulnerable, how to select a suitable solution provider, and what protective counter-surveillance infrastructures and practices should they put in place?

The Tap Sweep Solution—Protecting Your Information Edge.

As mentioned earlier, counter-surveillance solution providers fall into three rough categories:

- 1) Large security companies that “also” provide wire-tapping and bug detection services as part of a larger, corporate security solution. These ‘component’ based solutions may or may not be effective—the size or reputation of the company is not necessarily an indicator of their qualifications, or their equipment. In any case, their target client is a large corporation and small to medium sized businesses and professionals would be unable to employ them at reasonable cost.
- 2) Private investigators who offer a medley of related services often claim experience and expertise in these areas, but are usually under trained and equipped, and perhaps more suited to domestic surveillance types of situations. Trust may also be an issue with such small operations, and it’s unlikely that they know enough, or have the ware-withal to purchase the expensive equipment required to detect a full range of wiretapping or bugging devices and frequencies, which are often difficult to detect even by a fully trained expert with state-of-the-art equipment.
- 3) The counter-surveillance specialist is the third and smallest category. This is an individual with sufficient training in ALL areas of detection, and the specialized equipment to carry it out. They are also familiar with industry trends, up on the latest techniques, technologies, and best practices, and will usually focus on the most common threats (audio/video surveillance and wiretapping), for it’s uncommon to find a “specialist” in too wide an area. Furthermore, they are more likely to provide additional consultation and training in developing a comprehensive counter-surveillance program, including developing a security infrastructure, and instituting best practices, and maintenance sweeps. However, not all specialists are equal. It is best to ensure that they are qualified and certified in the detection, removal, and support of the type of device suspected, with sufficient industry knowledge to keep you abreast of new threat trends.

The Tap Sweep Solution was developed by a certified counter-surveillance specialist, and designed specifically with SMEs in mind. It provides:

- 1) Core services in the most common areas affecting SMEs: wire-tapping and audio/video surveillance.

- 2) Fully qualified staff, trained with state-of-the-art sweeping and detection equipment.
- 3) Employees cutting-edge best practices, and, depth of knowledge.
- 4) Is sensitive to business issues such as costs, and developing a realistic business case.
- 5) Provides several levels of end-to-end services, packages, as well as additional consultation, and training as required to meet individual needs—from initial threat assessment, to planning, sweeping, and maintenance.
- 6) Provides clients with up-to-date industry information.

Detailed Solution Description

Whether you are merely concerned, or have seen worrying warning signs, or have actually been bugged, Tap Sweep may have a solution that's right for you. When choosing a solution provider, that's critical: an inadequate solution is as bad as an expensive "shotgun" approach. Counter Espionage is not a do-it-yourself security project. It is not recommended that business executives purchase eavesdropping protection equipment for use in-house. Properly detecting IE requires extensive training and an array of specialized equipment. It takes an expert to determine the best choices and strategies. There is just too much at stake to risk working with the wrong provider. Counter Surveillance is a highly specialized field. It is important to take the time to do proper due diligence, and make the right choice.

The Tap Sweep Technical Surveillance Counter-Measures (TSCM) service offering were developed with SMEs in mind:

1. We specialize in the most common threats in audio and video bugging and telephone wire-tapping—which most likely cover most SME threats.
2. We provide seriously interested parties with the information needed to decide on the best plan—level, price etc.—AND overall preventative and maintenance strategy, so decision-makers can take informed action, then return to their jobs—worry free.

In addition, we also:

1. Equip all involved with a general understanding of the real threats of electronic eavesdropping.
2. Provide the information clients or their security representatives require to set up an effective electronic counter measures program that should sharply reduce the likelihood of a successful electronic attack

3 Levels of Bug Sweeps—Multiple Applications.

Whether its RF bugs, wiretaps, carrier current transmitters, optical/visual bugs, wires and microphones, or acoustic eavesdropping compromises in strategic locations like board rooms, or executive offices, or other compromises just about any place where sensitive information may be gleaned, our three levels of sweeps provide the most solid coverage.

Level 1 Sweeps:

Detects lower quality wiretapping and bugging devices and will pick up most low-level domestic surveillance bugs and taps. Consumer-end industrial eavesdropping equipment can also be detected. [Most domestic sweeps are at this level, and lower levels threats in the SME environment.]

Level 2 Sweeps:

With this option, a deeper level of search is performed, and a broader range of radio frequencies and devices are explored and analyzed. Further examinations of telecommunications are performed. This plan detects most mid-level devices and some hi-end industrial devices.

Level 3 Sweeps:

A deeper and more comprehensive analysis into an even broader range of frequencies of the more specialized and sophisticated devices, as well a deeper analysis of **all** wires and telecommunications. This covers the above two levels, plus some professional-level medium to high-end industrial intelligence eavesdropping devices.

We also perform vehicle sweeps at a flat rate fee.

How Tap Sweep Works: 6 Logical Steps To Tightening the Net.

Bug sweeping is a very good start—but it is only one component of an overall “sweep” that includes the following, complete, 10 point site, threat, and situation assessment, and a written strategic plan. Specifically, we:

- 1) Interview you regarding your situation, history of possible threats, warning signs, and request that you take our Vulnerability Test to determine your vulnerability index, to obtain a complete picture.
- 2) We ensure that you have taken and understood our test, read the Executive Briefing, and have the information you need to interpret and act on your situation, including probable scenarios, and consequences.
- 3) We perform a thorough high-level, assessment—this is a standard, reasonably priced starting off point, without which we could not proceed—it just makes sense that our experts first take a thorough look at your situation for things you may not have thought of or missed before doing actual sweeps etc.
- 4) We develop an over all plan/strategy, and propose (in writing) a plan of action, that includes short-term tactical solutions to remove, disarm, or neutralize immediate threats, followed by training in creating a long-term preventive and maintenance protocol to ensure that you are covered on an on-going basis. **REMEMBER:** removal of a threat in one instance does not guarantee similar placement the next day, or a different threat. It only makes sense to tighten the net, and keep it tight.
- 5) We make ourselves available for future alerts, and execute our maintenance plan.
- 6) We keep you informed on latest developments in the industry, and, effectively, serve as a critical member of your counter-measures team—albeit on contract, and off site.

Please NOTE: Our Operating Policy

At Tap Sweep, our mission is to take the mystery out of hiring electronic counter-surveillance specialists to perform bug and wiretap sweeps of your offices, boardrooms, sensitive areas, vehicles, residences or other areas where there is a fear of proprietary information, research, trade secrets, litigations, negotiations; or personal and private matters that can be listened to or viewed, usually much to the advantage of the thief.

Security needs in today’s rapidly growing micro-electronic world are much different than just ten years ago. Back then, the LAG system (locks, alarms and guards) was commonly employed. Today, company executives can be held responsible if security needs such as proper computer firewalls and electronic counter-surveillance measures are not employed.

Tap Sweep is a security-consulting firm that specializes in the detection of unlawful/unauthorized electronic surveillance. We provide on-site services such as wiretap and bug sweeps, as well as expert recommendations to safeguard against information theft.

We will NOT accept assignments:

- ❑ To obtain privileged information
- ❑ That do not have a clear stated purpose
- ❑ That are against the best interest of the Canadian Government or its citizens

We will strive to provide absolute confidentiality and to provide honest estimates that you can rely upon as being exact.

Conclusion

Industrial Espionage via wiretapping, and audio/video covert surveillance is a very real, and present threat to small and medium sized businesses, professionals, as well as anyone with valuable, proprietary information. The prevalence of easy-to-purchase and use bugging equipment is proof that the threat exists widely, and much damage is already being done, without the victim's knowledge or awareness. The cost of IE goes beyond loss of a bid, or transaction, or technology, or idea. It can topple large businesses, create financial catastrophes, and ruin lives. Often, it is the CEO, or executive who is ultimately responsible and held accountable. Finding a solution in today's market is not easy—especially if you are uninformed. Getting informed, and selecting the appropriate level and type of counter surveillance solution is critical. One thing is certain: covert surveillance is as large a threat as computer-based virus and spying, and must be treated with similar diligence. Corporations that do not have or launch a counter surveillance security program bear the risk of becoming a victim of this threat.

Appendix A

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

The Signs:

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

Tips

- 1) Trust your instincts—we often sense the problem before finding the evidence.
- 2) Question 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 clocks, phones, lamps. Also, 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.
- 7) 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.
- 8) The most vulnerable businesses are on the top floor because all the communications pass through all floors to reach them.
- 9) 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).
- 10) 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.
- 11) 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.
- 12) Be aware of changes to reception to radio stations, TV or cell phones. These are often indicators of rf (radio frequency) bugs interference.

Appendix B--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.

Action Steps: Visit the Tap Sweep Web site (www.tapsweep.ca), download and take the self-scoring Vulnerability Test.

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.

Be Cautious!

Please take this last point seriously! If your offices or premises, or even phone or cell, or home or vehicle is bugged, discussing bugging may be the worst error you make. After all you do not even know if your leak is internal or external, and you could very well be tipping them off. This is one kind of information you absolutely do NOT want your eavesdroppers to have!

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 performed, 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, and then decide whether you need to conduct a full sweep. The cost and visibility of such a step will mean informing others, and making the situation somewhat “public”—**BUT PLEASE LIMIT YOUR DISCUSSIONS TO THE SMALLEST NUMBER OF INDIVIDUALS, IDEALLY TRUSTED PEOPLE WHOSE APPROVAL OR INVOLVEMENT YOU ABSOLUTELY REQUIRE TO TAKE SUBSEQUENT STEPS, AND PLEASE CONDUCT DISCUSSIONS IN A SECURE LOCATION OR MANNER RECOMMENDED 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 by many people, yet sensitive information is shared within. 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; B) 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 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 company's or professional intellectual and information assets.

About The Author

Steve Parkin, is the CEO and chief field agent of Tap Sweep, Counter-Surveillance Services. A veteran telecommunications expert with over 25 years in the industry and extensive training (and certification) in Technical Surveillance Counter Measures (TSCM), Mr. Parkin is committed to educating SMEs about Industrial Espionage via wire-tapping and covert audio/video surveillance, and developing viable state-of-the-art solutions, while keeping up with new threat trends.

About Tap Sweep

Tap Sweep Counter-surveillance Services is Eastern Ontario's only Certified wire-tapping and "electronic bug" sweeping specialist. Based in Ottawa, Canada, Tap Sweep offers a complete range of Technical Surveillance Counter-Measures (TSCM) solutions, including threat assessment, "bug sweeping," consultation, training and industry/insider information.

Our clients include SMEs, professionals, and individuals—anyone financially or personally vulnerable to information theft because they:

- Possess proprietary information of value to others
- Are in possession of specialized knowledge, or engaged in sensitive situations
- Are in the public eye, under scrutiny, or in positions of responsibility
- Are in highly competitive business sectors, and bidding situations
- May incur devastating business, professional, financial or personal loss due to information leaks

Tap Sweep is committed to helping you counter the threat of IE. Our two-tier service plan is geared specifically for SMEs:

- 1) We arm you with the information you need to take smart action--now
- 2) We deliver services and solutions that help you act now, while putting a long-term counter-measures plan in place.

We work exclusively and closely with decision-makers who understand the grave financial threat posed by Corporate Espionage, and help "close the door" by completing today's new security needs.

We hope you found the information in this briefing useful and informative, and that you will consider us when choosing your counter-surveillance provider.

Industrial Espionage Can Be Countered! Consider Tap Sweep as Your First Line of Defense

Special Introductory Offer

If you have read this briefing, and/ reviewed our Web site, or taken our Vulnerability Test, your interest is no doubt fueled by a serious concern over the issue of information theft via covert electronic surveillance. To help you launch your counter measures program as soon as possible, Tap Sweep would like to extend the following special introductory offer:

Contact Tap Sweep (using the secure contact protocol on our web site) within the next 30 days, and get 25% off your first threat assessment and bug sweep.

We look forward to serving you.