Executive Briefing

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 CounterSurveillance Solution Provider
President/CEO of **TapSweep CounterSurveillance Services**

Table Of Contents

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, 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", the Internet, a typical electronics or hardware store -- is all that's required to purchase and deploy a powerful surveillance device capable of transmitting audio and video information.

"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 poling confirmed they had NOT reported incidents of corporate espionage to authorities." *National Counter Intelligence Centre*

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

Technical advancements: the 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. The increasing demands of an aging population are providing developers incentive to develop better micro-transmitters and receivers for the soon to boom hearing aids industry. 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.

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.

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?

Solution Provider Overview

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.
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:
We specialize in the most common threats in audio and video bugging and telephone wire-tapping—which most likely cover most SME threats.
We provide you with the information needed to decide on the best plan—level, price etc.—AND overall preventative and maintenance strategy.

We provide:
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) Technicians with cutting-edge best practices, and, depth of knowledge.
4) Awareness of business issues such as costs, and developing a realistic business case.
5) Customized 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) Up-to-date industry information.
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.

Detailed Services Breakdown

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 wires and telecommunications. This covers the above two levels.
We also perform vehicle sweeps at a flat rate fee.

How TapSweep Works: Six 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:

1) Discuss your unique situation, history of possible threats and warning signs
2) Offer an Executive Briefing to assist in interpreting your situation, probable scenarios and consequences—and preventative actions.
3) Assess your situation—it just makes sense that our experts first take a thorough look at your situation for things you may have missed before doing a sweep.
4) Develop an over all plan/strategy 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) Assist your execution of a security-maintenance plan.
6) Continue being available 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
- 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.

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 the easy-to-purchase and use bugging equipment, re-purposed items such as baby-room monitors, cordless & cell phones, recording devices for note-taking is proof that the threat exists widely, and much damage is already being done without the victim's knowledge or awareness.

The sliding ethical scale away from privacy of others and the quest for individual gain greatly increases the odds of being compromised.

The cost of personal and industrial espionage goes far beyond loss of a bid, concept, idea, litigation matters, theft or safety: it can topple large businesses, create financial catastrophes, and ruin lives.