TSCM Bug Sweeps... When and When Not To - Part II

by Kevin D. Murray, CPP, CISM, CFE

The following advice is specifically meant for:

- Private Investigators,
- Security Directors,
- Security Consultants,
- and new TSCM practitioners.

Technical Surveillance Countermeasures (TSCM), or a bug sweep, is an analysis of an area to detect illegal covert electronic surveillance. In addition to listening devices, sweeps also take into account optical, data, and GPS tracking devices.

Part II - Post-sweep tips to keep your current business clients espionage-free.

In Part I we discussed how to handled requests from new clients for TSCM bug sweeps. In Part II we look at helping your current business clients.

After they learn you can help them – with your business espionage solutions – you will be viewed as a more valuable resource. Your revenue will also increase.

A typical case involving current business clients...

Most companies do very little to protect themselves against business espionage. Worse, they do not even know what protection measures are available, or where to go to find them. The natural result is "The Ostrich Effect." Ignore the risk and maybe it will go away.

As their security advisor you should be helping them avoid this major disaster.

Step 1. Partner with a competent counterespionage consultant.

As mentioned in Part I of this series, partner with a competent specialist. You may already have someone you know and trust. If so, great. If not, conduct a search using a term like *counterespionage consultant*. Once you have found specialists to vet, ask plenty of questions. If you are not sure of what to ask, search *TSCM compare* (skip the paid ads) for a list of questions.

Qualify your specialist with questions, but be sure to note their professionalism, too. Their presentation and demeanor will reflect on you, and the judge if you need them to testify in court.

Knowing a competent counterespionage consultant will make the rest of the steps very easy for you.

Step 2. Contact your clients.

Make an appointment with the company president, chief legal counsel, or security director. Present your concerns about their security blind spot. Be serious. Be sincere. Bring in documentation which supports your concerns; news articles, government reports, etc. Let them know you foresee business espionage as a major security vulnerability for them—a vulnerability which is not being addressed.

TSCM Bug Sweeps... When and When Not To - Part II

by Kevin D. Murray, CPP, CISM, CFE

You can be sure they have already thought about this. However, they probably didn't know what to do, so nothing was done. They should be very pleased by your initiative and should welcome having the problem properly handled.

Offer to create a pro-active strategy for them.

Begin by setting up an on-going schedule of TSCM eavesdropping detection inspections which include information security surveys.

Here's why...

Intelligence collection is a leisurely process. No harm is done until the collected information is used. This is the time to search for evidence of it happening.

Business espionage happens in multiple ways and often includes electronic eavesdropping. Fortunately, electronic surveillance is the easiest evidence of an attack to discover.

Periodic TSCM inspections can reveal an attack while there is still time to thwart it. This is why smart information security programs start with regularly scheduled sweeps.

TSCM is even better than Intellectual Property insurance. Insurance can't prevent monetary, business opportunity, competitive advantage, or reputation losses. TSCM can!

TSCM is actually inexpensive super-insurance.

TSCM inspections can do more than just reveal electronic surveillance. Some practitioners are also qualified to conduct information security surveys, which identify: decaying security hardware (locks and alarm points); poor employee security practices; and reveal new non-electronic information vulnerabilities as they develop. Look for consultants who have earned certifications, like: CPP[1] and CISM.[2]

The benefits to your client include:

- Protection of profits.
- Business strategies remaining viable.
- Intellectual assets remaining theirs.
- Personal privacy and safety protected.
- Fiduciary responsibility to stockholders is documented.
- Financial disasters are avoided.
- They will be perceived as a hardened target instead of an easy mark.

Prevention is always cheaper and smarter than sustaining losses.

The benefits you will see include: more frequent contact with your client; a more regular revenue stream, and opportunities for new work—based on implementing the security recommendations made by you, or your TSCM inspection consultant.

---

[1] Certified Protection Professional

[2] Certified Information Security Manager

TSCM Bug Sweeps... When and When Not To - Part II

by Kevin D. Murray, CPP, CISM, CFE

Step 2. Map out a strategy.

Determine which on-site areas to inspect. Be cost-effective. Create a priority list of sensitive areas. Begin the inspection process at the top of the list. At some point you will be able to say, "If these areas are clean, non-sensitive area problems are unlikely."

Determine what events will require attention (board and off-site meetings, for example).

Determine how often inspections should be scheduled. Two to four times per year is average for most businesses.

Be flexible and even a little unpredictable. Areas being inspected may be mixed and matched. Quarterly TSCM inspections limit the window-of-vulnerability and may include:

- Highly sensitive areas such as boardrooms, executive suites and dining rooms, legal and personnel departments—four times per year.
- Medium sensitivity areas like division heads and managers' offices—twice per year.*
- Lower sensitivity areas—once per year.*

* Randomly insert these areas into the quarterly TSCM inspection schedule.

Take into account the location of these areas when you are mapping out your strategy. If the once and twice per year areas are near each other, don't schedule them during the same quarter. Why? Because the radio-frequency portion of the TSCM inspection process covers a large area. Unscheduled, nearby areas can benefit every quarter with proper planning, at no extra charge.

Step 3. Implement the TSCM inspection plan.

Step 4. Document your efforts.

Make sure you, or your partnering specialist, can produce intelligent reports with concise, practical recommendations. No technical jargon. Reports should document:

- The purpose of the TSCM inspection.
- The areas covered.
- A brief description of the inspection process and analysis.
- Floor maps and photos.
- A historical log.
- Clear, actionable recommendations.

It is important to note that you, or your specialist, be independent. This means the person conducting the TSCM inspection does not receive any profit or benefit from their recommendations, i.e. don't partner with an alarm company or the local spy shop.

Take time after each audit to review the report with your client. Offer to oversee the implementation of recommendations whenever possible. The more work you remove from your client's shoulders, the more they will rely on you.

"Why bother. We wouldn't be an espionage target."

Being *in business* automatically means a business has some sort of competitive

advantage over their competitors. The more successful a business is, the more they need to fear the theft of their advantages.

This means that ***all*** of your business clients are candidates for pro-active business espionage prevention. All of them.

It's no secret that business espionage is a growing problem.

The world has changed. *Corporate Espionage* is the new *Honest Competition*. Your business clients need *Operational Privacy* to compete.

You are capable of helping them. All it takes is initiative.

TSCM inspections with information security surveys are bedrock of long-term, active relationships.

If you don't help your clients, another person reading this paper will.

###

About the Author

Kevin D. Murray CPP, CISM, CFE is a technical information security consultant and TSCM specialist with over four decades of experience.

Murray Associates is an independent security consulting firm which provides eavesdropping detection and counterespionage services to business, government and at-risk individuals.

Headquartered in the New York metropolitan area, a Murray Associates team can assist you quickly, anywhere in the United States, and internationally.