

How Often Do You Find a Bug?

by Kevin D. Murray, CPP, CISM, CFE



Q. How often do you find a bug?

A. It depends on the type of sweep.

We conduct Technical Surveillance Countermeasures (TSCM) sweeps for bugs and surveillance devices in businesses and government (and occasionally residential or matrimonial type sweeps).

Business and Government TSCM Sweeps

Regularly scheduled, due-diligence, technical information security surveys rarely turn up devices. No surprise there. Typically, organizations using our services already have a high overall security profile. They are "hardened targets." For those clients, the

bug sweep bonus is... having a known window-of-opportunity when something is found.

Often, what we do find are other information vulnerabilities like: decayed security hardware; security policies no longer being followed; and other [unseen security issues](#).

Discovery statistics on our "emergency sweeps" (sweeps where [electronic surveillance](#) is suspected) varies from year to year, about 2%-5%. However, **the rate of determining what happened and resolving the client's concerns is extremely high.** (Isn't that the real point of the exercise?) More often than not, these info-loss cases



Commonly used miniature microphone.

How Often Do You Find a Bug?

by Kevin D. Murray, CPP, CISM, CFE



can be traced back to the human element, or the poor security practices, which allowed the leak to occur some other way.

With organizations, the opposition's focus is on getting the information, in *all* its forms. Corporate espionage, industrial espionage, call it what you will. There is no one spy tool of choice here. It's electronic surveillance *plus* hundreds of other tradecraft techniques which may be employed. Solving these organizational emergency cases requires more than a simple TSCM bug sweep. Required add-on skills and experience include: corporate investigations, alarm system design, computer forensics, and information management to name a few.

Residential Bug Sweeps

When it comes to residential and matrimonial bug sweeps, the find rate for locating bugs and surveillance devices is quite high. This makes sense. The opposition's focus is narrow; they want to intercept communications and/or determine the location of a specific person. Electronic surveillance *is* the tool of choice. Personal privacy is the biggest loss.

Solving these cases is relatively easy for a number reasons:

- The spy is usually a do-it-yourselfer, an amateur, or someone with limited tradecraft skills.
- The victim has a good idea who is doing the spying.
- Resources rarely permit the purchase of advanced bugging or tracking devices.
- Surveillance devices adequate to accomplish the goal are inexpensive and easy to obtain.

- Locations for placement of bugs, taps, spy cameras and trackers are limited.
- Having a personal stake in this type of surveillance, spies often tip their hand to show power.

The Security Director's Dilemma

Justifying cost to the bean counters.

Private investigators and people who handle residential and matrimonial bug sweep cases don't charge very much for their services. Mainly because private individuals have limited budgets. But, also because their overhead is low. Their detection gadgets are often basic and inexpensive, insurance costs (if any) are not up to corporate standards, for example.

Professional security consultants who specialize in business and government-level TSCM are not a dime-a-dozen. They invest heavily, and continually in: sophisticated instrumentation, professional certifications, and advanced (and continuous) training. Their overhead includes: an office staff, trained Technical Investigators, licensing, insurance, instrument calibration, and an annual Carnet so they can travel Internationally for their clients.

Security directors know, [it's not all about the money](#). It's about what you get for your money. A cheap sweep is a mental band-aid, and a CYA move.

They are charged with protecting corporate assets. This type of information security requires a security consultant with a depth of experience and knowledge of: information management, corporate

How Often Do You Find a Bug?

by Kevin D. Murray, CPP, CISM, CFE



investigations, complex security systems, and yes...
Technical Surveillance Countermeasures.

Benefits of Quality TSCM

Second to 'getting the goods', the goal of espionage and voyeurism is 'never be discovered.' Obviously, if you don't check, you won't know you're under attack. Organizations don't have a choice. They don't want their pockets picked, so TSCM is an important element of their security.

The benefits of a Technical Information Security Survey (enhanced TSCM) in an organization's security program include:

- Increased profitability.
- Intellectual property protection.
- A working environment secure from electronic surveillance invasions.
- Advance warning of intelligence collection activities (spying).
- Checks the effectiveness of current security measures and practices.
- Document compliance with many privacy law requirements.
- Discovery of new information security loopholes, *before* they can be used against them.
- Help fulfill legal the requirement for "Business Secret" status in court.
- Enhanced personal privacy and security.
- Improved employee morale.
- Reduction of consequential losses, e.g. information leak can spark a stockholder's lawsuit, activist wiretaps, and damage to "good will" and sales.

The benefit list is really longer, but you get the idea.

There are some excellent corporate-level TSCM consultants out there. Now that you know about the different levels of service, track one down to help solve your information security concerns. You will look like a hero to all your colleagues, except perhaps, the near-sighted bean counters.



—**Kevin D. Murray** CPP, CISM, CFE is a business counterespionage consultant and TSCM specialist with over three decades of experience.

Murray Associates is an independent security consulting firm, providing (surprise) **Technical Information Security Surveys** for 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.

v.170622