www.SecurityWorldMag.com

SecurityWorld
INTERNATIONAL

PLUS
- Promises for the Security Industry
- Be Ready
- Open Your Door and Lock Your Window
- Keeping an Eye on Hospital

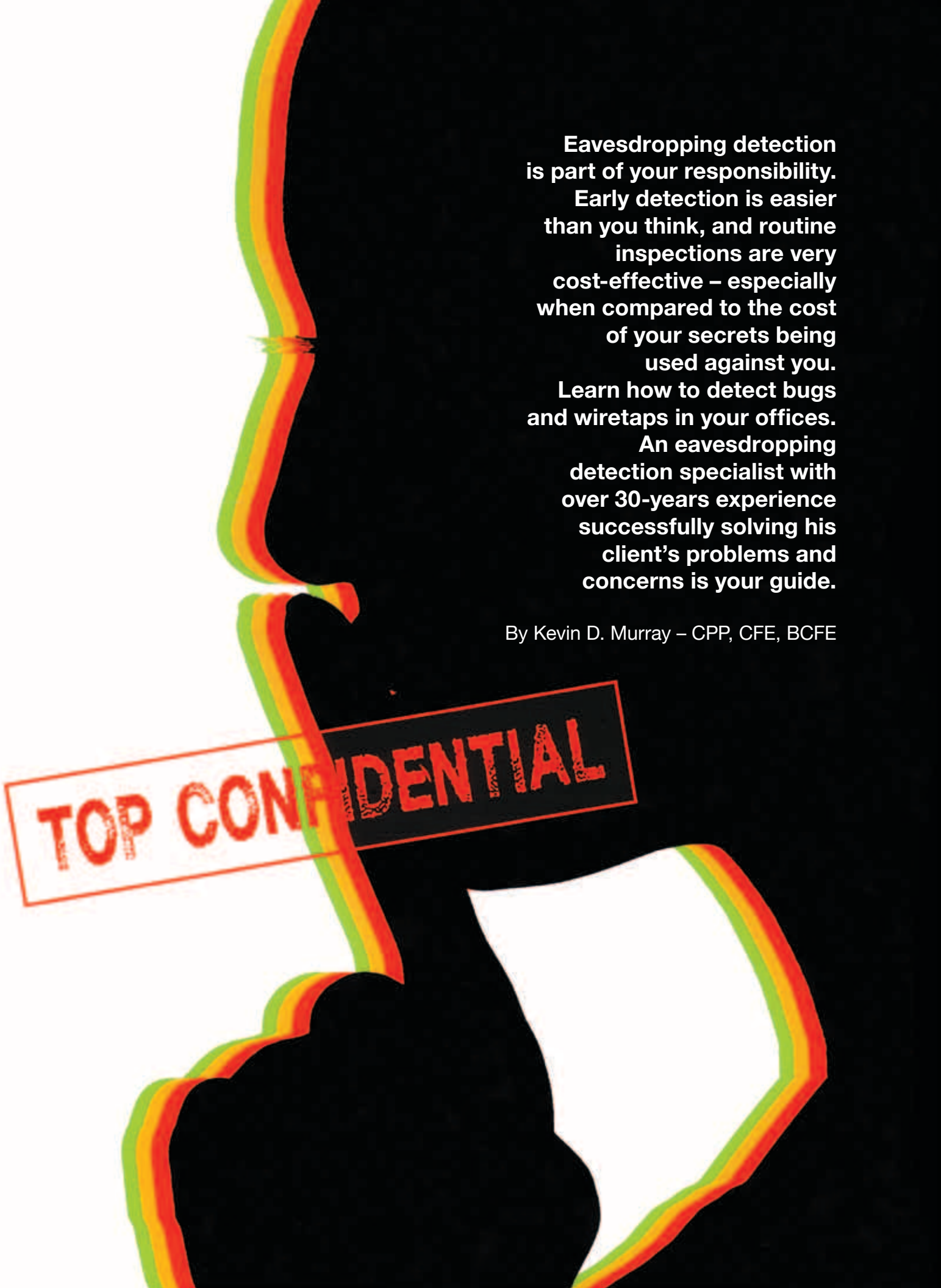
EAVESDROPPING DETECTION

WHO IS LISTENING?

Everything You Need to Know about Electronic Eavesdropping Detection for Business

Eavesdropping detection is part of your responsibility. Early detection is easier than you think, and routine inspections are very cost-effective – especially when compared to the cost of your secrets being used against you. Learn how to detect bugs and wiretaps in your offices. An eavesdropping detection specialist with over 30-years experience successfully solving his client's problems and concerns is your guide.

By Kevin D. Murray – CPP, CFE, BCFE



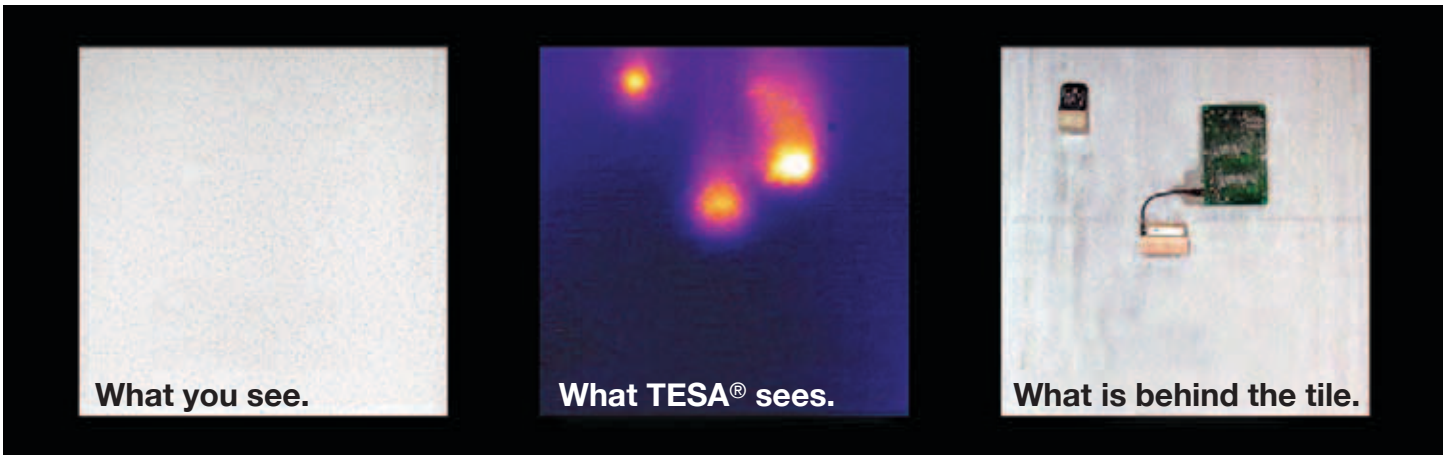


Figure 1. Thermal Emissions Spectrum Analysis ® (TESA) reveals two spycams and a battery hidden behind a ceiling tile. (Source: Murray Associates)

BUSINESSES ARE NO LONGER WAITING FOR EAVESDROPPING PROBLEMS TO SURFACE. ESTABLISH YOUR INSPECTION PROGRAM BEFORE A PROBLEM SURFACES.

"Should we be checking for bugs and wiretaps, or am I just being paranoid?"

This thought would not have occurred to you if everything were fine. Trust your instincts. Something is wrong. Eavesdropping is a common practice; so are regular inspections to detect it. Conduct an inspection, quickly.

WHAT YOU NEED TO KNOW

Trust Your Instincts

With eavesdropping and espionage, the thought would not have crossed your mind if a real problem did not exist.

Realize That Only Failed Espionage Gets Discovered

You never hear about successful eavesdropping or espionage attacks. You're not supposed to. It's a covert act. Eavesdropping and espionage is invisible. Discovery relies heavily on the victim's intuition and preparedness to handle the problem. Prevention—via regular inspections—is the logical and cost-effective solution.

Spying Is a Common Activity

Due to the covert nature of spying, the exact extent is not known. Fortunately, we can use failed espionage attempts as a gauge. They reveal over and over again that the problem does exist. Also, the plethora of electronic surveillance equipment being openly sold from Internet "Spy shops" gives us a good indication of the magnitude of electronic eavesdropping.

Eavesdropping and Espionage Can Cripple or Kill a Company

Documented cases of eavesdropping and espionage have shown repeatedly that, left unchecked, espionage will eventually desiccate a bottom line, wipe out a competitive advantage, and leave a company a shell of its former self.

Espionage Is Preventable

Information is like any other corporate asset. Management has a responsibility to protect it. Stockholders can claim negligence and hold company executives responsible if this asset is lost due to improper protection efforts. Simple LAG (Locks, Alarms & Guards) are not adequate protection.

The Law Only Protects Those Who Protect Themselves

You can't just wander into the courtroom crying, "They stole my business secrets" and expect help. You have to

Eavesdropping Detection Philosophy

Intelligence collection is a leisurely process. Enemies quietly collect long before they use. Until they use what they have gathered no harm is done. Knowing this gives you the edge.

Eavesdropping is:

- Not the goal. It is a means to an end.
- A key component of intelligence gathering.
- The one spy trick that is easily detectable.

Eavesdropping detection audits exploit weaknesses inherent in eavesdropping surveillance. Knowing "they" are listening to you gives you time to counter—before harm is done.

Inspect for eavesdropping devices regularly.

show the extraordinary steps you took—and maintained—to elevate your business information to secret status.

Counterespionage Is Not a Do-It-Yourself Project

- Don't buy eavesdropping detection gadgets.
- Don't play detective.
- Don't hire a private detective and let them play debugging expert.

This is serious business. Counterespionage work is a full-time specialty within the security field. Professional help is available.

HOW TO GET HELP

Contact an independent security consultant who specializes in electronic eavesdropping detection and espionage prevention. Recognizing this person may not always be easy.

- Contact several corporate security directors. See whom they use. Get first-hand recommendations.
- Contact industry associations for referrals—e.g., International Association of Professional Security Consultants (**www.iapsc.org**); Espionage Research Institute (**www.espionbusiness.com**).
- Conduct an Internet search using key words like "eavesdropping detection" or "counterespionage" Or, visit me at **www.counterespionage.org**.

HOW IT'S DONE

Background Interview

Upon arrival the consultant should conduct a background interview with you to obtain an overview of your security concerns—this discussion will not be held within the areas to be inspected.

Survey of Current Security Measures

This includes an inspection of perimeter and interior physical security hardware.

Visual Examination

The areas in question should be visually inspected for all types of current electronic eavesdropping devices and evidence of past attempts.

Acoustic Ducting Evaluation

Unexpected sound leakage into adjacent areas has been found to be the cause of many information leaks, especially the in-house type.

Inspection of Telephone Instruments

An extensive physical examination of the telephone instruments must be undertaken. There are more than 16 types of attacks involving bugs, taps, and compromises that can be made on a basic telephone instrument—according to the National Wiretap Commission Report. Business and VoIP telephone sytems have other vulnerabilities, some of which are simple system features that can be abused.

Note

As you can see, electronic eavesdropping detection and counterespionage consulting begins even before the electronic instruments are unpacked.

Inspection of Telephone Wiring

Wiring associated with the telephones under test is inspected for attachments and damage. Damaged wiring is often the only evidence of a prior wiretap.

Electronic Testing for Analog and Digital Wiretapping

Special instrumentation is required for these tests—e.g., TALAN™ Telephone and Line Analyzer.

Inspection of Telecommunications Junction Blocks

Junction blocks are where telephone wires connect to each other in the building. These connected wires form a path between the telephone instrument and the on-premises, telephone switching equipment. In some cases—e.g., simple residential phone service and facsimile machines—internal wiring connects directly to outside cables which lead to the phone company central office. Junction blocks are an easy, and a relatively safe place to attach a wiretap device.

Communications Room Inspection

The building communications room houses the junction blocks for the internal phone system, switching equipment for the internal telephone system, telephone company junction blocks for the incoming lines and computer local area network wiring. This is a major area-of-vulnerability

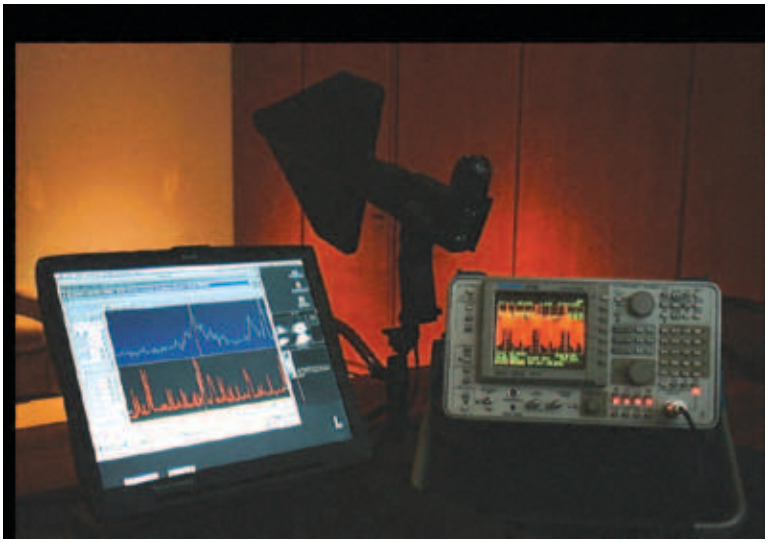


Figure 2. Radio Reconnaissance Spectrum Analysis® (RRSA) locates audio, video and data bugs. (Source: Murray Associates)

requiring inspection from both a wiretapping and physical security point of view.

Non-Linear Junction Detection Inspection (NLJD)
This detection technique is used in sensitive rooms to locate bugs, voice recorders, spycams and amplified microphones that may not be operating at the time of the inspection.

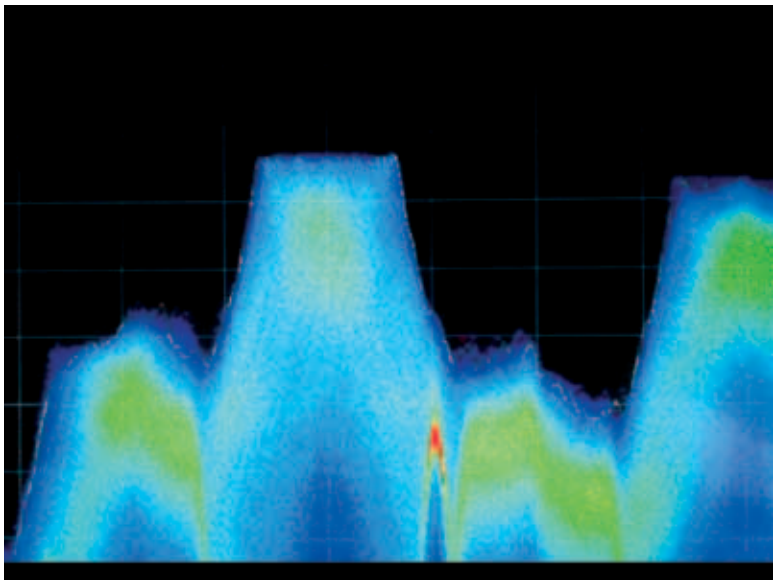


Figure 3. Second Generation RRSA® sees bugs hiding behind stronger signals —a Murray Associates exclusive capability. (Source: Murray Associates)

Radio Reconnaissance Spectrum Analysis®
Eavesdropping devices may transmit a radio signal—over-the-air, or on building wiring. They are detected with an instrument called a spectrum analyzer (US$10,000 to US$110,000). In simple terms it can be thought of as a radio which has a very long, and continuous, tuning dial. The received signals are shown on a display screen for visual analysis, and are also converted to sound and picture. Each signal is individually evaluated to determine if it is carrying voice, data or video information from the area.

Thermal Emissions Spectrum Analysis®
Electronic eavesdropping devices and covert spy cameras are discovered with speed and certainty thanks to a relatively new detection method—Thermal Emissions Spectrum Analysis® (TESA). TESA allows hidden bugs and spy cameras to be 'seen' on a portable video display by virtue of the minute amounts of heat radiated as electricity flows in their circuitry.

Surveillance devices hidden in ceiling tiles, in walls and in other common objects create warm spots. TESA sees these areas even if they are only 18-thousandths of a degree Celsius different in temperature from the surrounding area. This is less than the amount of heat your fingertip leaves on an object after you touch it for a split second.

Additional Tests
As in the medical profession—eavesdropping detection specialists also have many tests that are applied depending upon a client's specific needs or concerns. Each situation is a bit different. There is, of course, the core group of the aforementioned inspection procedures. Additionally, there are tests that are used as the situation demands. This forces the consultant to add "thought" to your inspection process. The overall goal should always be "solve your concerns" not simply dash blindly through a checklist.

Final Report
When the inspection is over, you should receive a full verbal debriefing. In this meeting your consultant will highlight all serious problems found, and will recommend solutions which need to be implemented immediately. You should also receive a written report within a week.
This should include:

- A description of areas and equipment inspected;
- An explanation of all tests conducted;
- The findings;
- Recommendations for security improvements;
- A review of other espionage loopholes found;
- Security improvements made since the last inspection; and,
- Counterespionage tips for deterring future attacks.

BE PREPARED

Electronic spying is a serious economic and privacy concern in corporations and government agencies. Current security best-practices suggest offices, conference rooms, and other sensitive areas undergo eavesdropping detection inspections two to six times per year. Executives' home offices, vehicles and off-site meeting locations are vulnerable as well and should be checked, too.

Businesses are no longer waiting for eavesdropping problems to surface. Establish your… *(Continued on rear center panel.)*

What To Do

If you suspect you have a problem:

- Do not discuss your electronic eavesdropping or espionage concerns—in person or via telephone—while in a sensitive area, or on a questionable phone.
- Engage the services of a specialist promptly.
- Do not leave their sales literature in suspected areas.
- Conduct business in a normal manner while you develop your defense. The element of surprise is an important part of the eavesdropping detection audit.

inspection program before a problem surfaces. Inspections need to be conducted regularly to:

- Detect spying before their efforts become problems;
- Protect individual privacy and personal safety;
- Limit windows-of-vulnerability;
- Satisfy on-going legal requirements for due diligence;
- Establish the legal eligibility requirement for business secret status in court; and,
- Identify new privacy invasion and info-theft methods.

Unfortunately, not re-inspecting periodically may be interpreted as an admission that previously protected information is no longer important.

NO LONGER HELPLESS

Congratulations!
Your security knowledge is more complete than ever. No longer will you be powerless to protect your company's ideas, plans, strategies, hard work, and privacy. No longer will you stand helpless as the opposition picks your pockets. No longer will you live in fear that stockholders will revolt, and judges won't take you seriously. No longer will you have to stand by and wonder if your eavesdropping sweeps are being conducted properly. You now know the qualities to seek when enlisting the aid of professional counterespionage counsel.

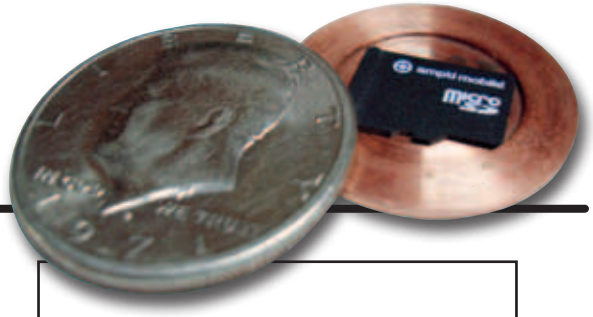
EXTRA THE SPY COIN STORY

I give spy coins to my clients.
It is a reminder that information loss is mostly a people problem, not an electronic problem. Filing cabinets of information can walk out the door in pocket change!

Careless people often blab information, forget to secure it, toss it in the garbage can, or otherwise lose it—hundreds of laptops are lost every day. People also steal it when they become greedy, spiteful, conned, blackmailed, or caught up in a "cause."

Investigating an information loss, however, begins with an electronic surveillance detection audit. Here's why...
- Serious espionage will include electronic surveillance.
- The possibility must be resolved before accusing people.
- Bugging is the easiest spy technique to discover.
- Electronic surveillance evidence helps prove your case.

Best advice... Conduct audits on a regular basis. Uncover signs of espionage during the intelligence collection stage, *before* your information can be abused.



About the author...
Kevin D. Murray began his career as a Pinkerton Investigator, then advancing to Director of Investigations (NJ) and Director of Electronic Countermeasures, company wide. He went on to found Murray Associates in 1978.

Mr. Murray is a Certified Protection Professional, a Board Certified Forensic Examiner and holds additional certifications. He is on the advisory board of the Espionage Research Institute (ERI); and is a member of the International Association of Professional Security Consultants (IAPSC) where he served several times on the Board of Directors and as the Ethics Committee Chairperson. He earned a BS degree in Criminal Justice (magna cum laude) and has taught at John Jay College of Criminal Justice in New York City. His chapters on eavesdropping and espionage appear in six college-level textbooks.

Murray Associates is an independent eavesdropping detection and counterespionage consultancy for business and government. Their *executive suite* audits for illegal electronic surveillance are an integral part of security plans at many organizations worldwide.

To date, no Murray Associates client has suffered an electronic surveillance information loss from any area under their regular care.

Murray Associates
PO Box 668
Oldwick, NJ 08858 (USA)
+1-908-832-7900
Privacy@spybusters.com

Eavesdropping Detection and Counterespionage Consulting for Business & Government

www.spybusters.com

***Free** spy news and security tips at: spybusters.blogspot.com*

MURRAY ASSOCIATES