Electronic Eavesdropping & Industrial Espionage

- The missing business school courses. -

by Kevin D. Murray - CPP, CFE, BCFE

MURRAY ASSOCIATES

MANAGEMENT CONSULTANTS TO BUSINESS & GOVERNMENT ON ELECTRONIC EAVESDROPPING DETECTION & BUSINESS ESPIONAGE PREVENTION

ESPIONAGE 101
Intro. to Espionage

Tapped phones. Bugged offices. Purloined papers. Covert Recordings. Undercover employees (moles). Phony repair people. Car phone monitors. Fax intercepts. Pretext calls. Dumpster divers. Still with me? Competitive intelligence professionals. Renegade employees. Foreign governments. The list goes on. How are you supposed to cope? Information Security was not taught in school. You never saw this in your job description. And yet, keeping business information where it belongs is now your responsibility. Knowledge is no longer just power, it's money too. BIG money.

Picture this. You're the Chief of R&D at a mid-sized snack food company. You have just discussed a new project with your staff of fifteen. Top secret. Your company is preparing a new cookie. Encapsulated chocolate bits make noises when bitten. From loud pops to whistles to burps, depending on speed of the bite. Your kids loved the idea. But this is only half the secret. In addition to being Sonic, it's: Natural, Oven-baked, Oil-free, Kalorie-free, and Yogurt-enriched. The staff affectionately names your pet project 'SNOOKY the Cookie.' Top management is excited. Sales potential is incredible if you get to the marketplace first.

One evening a few weeks into the work, Sam, a young man who joined your company about a year and a half ago, goes to a party with his wife. He has a few drinks, and begins saying loudly, 'SNOOKY development' when people ask him what he does for a living. An older guest hears this laughing remark and draws Sam aside. He tells him they have something in common. He works for a food company too. "Sam, maybe we should talk. Let's get together for lunch."

They meet for lunch, and Sam is led to believe that their meeting is really a job interview. Over a good bottle of wine, your competitor elicits from Sam all he needs to know. He has gently extracted information that gives him a feel for the overall direction of the SNOOKY project, its time frame, and half the secret to 'Kalorie-free.' He also knows that the early experiments are promising.

From seemingly innocuous party conversation, the competition has learned of your project's existence. Their interest leads them to hire a "research specialist." Your dumpsters are now being checked regularly. They routinely find each day's work and results. You later learn of an 'air conditioning repairman' showing up at your company after hours, on a regular basis. No one knows why.

Ultimately, your competitor will hit the market six weeks before you do. Their development cost was 10% of yours. And Sam well, he still works for you. The competition didn't want him. There were plenty of other ways to scoop SNOOKY without leaving an obvious trail. This left everyone in your company saying "If I were a paranoid person I'd swear they were spying, but gee, what a coincidence." Everyone except Sam. He kept quiet. Very quiet.

Many executives, even corporate security directors, vacillate dangerously when dealing with information leaks. “I’m probably just being paranoid, but maybe we should check for bugs and wiretaps.” Maybe it’s the fear of looking silly while dealing with this invisible monster. It may be unfamiliarity with the mechanics of dealing with espionage. In either case, the business community is awakening to what governments have known since the dawn of time. If your information has a dollar value, or power value, it’s a target. Eventually, someone will try to take it.

Why is this such a growing problem?

The cold war was political. It’s over. World War III is an economic war. It’s here. Information is where the money is. Information theft is easy, safe, and lucrative. Eavesdropping laws are difficult to enforce. Advancements in electronics and optoelectronics have made communications interception easy and cheap. Competition is now global. There are more competitors than ever before. Business ethics are not what they used to be.

In short, the personal reputation and accountability plumb lines only stretch so far. The pressure is on as never before, and in a crowded business community the haze of anonymity cloaks many kinds of questionable practices.

Think about your location for a minute. Would anyone turn away the air conditioner person on an emergency call after normal business hours? Wouldn’t the guard shut off the alarm, and open the locked doors? Would the air conditioner be serviced? Or would bugs be planted? Would phones be tapped? Would pictures be taken? Would computer disks be duplicated, papers photocopied, or data altered?

Historically, the business response can be summed up in one word: LAG (Locks, Alarms & Guards). A good start, but rather prophetic in the description of its efficiency.

Example: If your personal computer is stolen, it will probably be fenced (re-sold) for less than 10% of its value. The thief receives one payment of approximately $150. The risk is high, but it must be worth it... computers are stolen. Yes, a missing computer is rather compelling evidence that a theft has occurred. Businesses respond with Locks, Alarms and Guards. For street level crime this makes sense. Nobody likes replacing $1500 computers. But what protects the $1.5 million dollar R&D program? Usually, not enough.

Industrial spies steal the information, not the containers. Information is worth more. Continuing our computer example, nothing will appear to be missing. The computer will still be on the desk. The information will still be on the disk drive. Chances of being caught stealing the information are slim. The information will be sold for what it is really worth. And... an industrious spy will sell the same information many times over. Every competitor is a potential customer. Obviously, LAG is an ineffective deterrent.

Paranoia is often used as the excuse to avoid confronting the espionage problem. It’s understandable. After all, this is a tough problem and, naturally enough, most executives are ill-equipped to deal with it themselves.

Spy Maxim #1 - Trust Your Instincts.

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

Spy Maxim #2 - Only Failed Espionage Gets Discovered.

You never hear about successful eavesdropping or espionage attacks. You’re not supposed to. It’s a covert act. Frequency of publicity is on a par with commercial airline flights: only partially completed (failed) flights make the news. Watergate, for example, was a classic case of es-

pionage incompetence in action. This apparent quiet gives the victim a false sense of security. Not only is information theft prevalent and invisible, it is also silent. Discovery relies heavily on the victim's intuition and preparedness to handle the problem.

How Much Spying is Going On?

Due to the covert nature of spying, we will never know for certain. Fortunately, however, we can use the 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 in "spy shop" stores, and "executive toy" catalogs gives us a good indication of the magnitude of electronic eavesdropping. Word filtering back through the press and from electronic eavesdropping detection specialists can make you a believer. It's happening on a daily basis.

• Washington Post News Service - An article indicated consumer surveillance gear alone was now a $100 million dollar industry. In the same article, Steve Brown, a buyer for The Sharper Image said, "Maybe the Nineties are going to be the spy decade," and indicated that his company was expanding into spy gadgetry "...because it's fun, different and (will) cause excitement in the stores."

• Associated Press - Schenectady, NY "General Electric Co. of Fairfield, Conn., says a rash of industrial spying cases at its Schenectady plant cost it millions of dollars in recent years and was a factor in the layoff of thousands of employees."

• Corporate Security newsletter - "The number of wiretaps approved by federal and state courts rose 14 percent... Sixty percent of the taps involved alleged drug law violators, but the main thing for the corporate security manager to remember is that 18 percent of the approved taps were aimed at businesses. (And don't forget the illegal taps either.)"

• Newsweek - "Eighty per cent of the Fortune 1000 companies now maintain in-house snoops, according to the Society of Competitive Intelligence Professional."

• Detroit Free Press - "Gerber Will End Tours of its Baby Food Plant Gerber Products Co., citing concerns about industrial espionage and public safety, announced Tuesday that it will discontinue public tours of its Freemont baby food plant after almost 80 years. Kellogg Co. of Battle Creek canceled its plant tours in 1986 after attracting 260,000 visitors the year before. Upjohn Co. of Kalamazoo canceled its tours last year. Other companies have either cut back or eliminated tours, citing security and safety reasons."

• Meeting News - "The threat of industrial espionage is another burden for show managers and exhibitors."

• Time - "According to U.S. officials (FBI), several foreign governments are employing their spy networks to purloin business secrets and give them to (their) private industry."

• USA Today - Reported the Securities and Exchange Commission filed a civil complaint against the Philip Morris Director of Headquarters Services and two stockbrokers. In 1988, the executive leaked insider information about the pending takeover of Kraft, Inc. to the two stockbrokers. Interesting note: The executive discovered the secret information when he was entrusted to sweep the board room for electronic listening devices.

ESPIONAGE 201

Intro. to Countering Industrial Espionage

Aside from the obvious fact that eaves dropping and espionage cancer will eventually desiccate a bottom line, wipe out a competitive advantage, and leave a company a shell of its former self, there are three more facts you need to know:

Spy Maxim #3 - 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 lost due to improper protection efforts. Simple LAG (locks, alarms & guards) will not appear to be proper protection.

Spy Maxim #4 - The Law Only Protects Those Who Protect Themselves.

You can't just wander into the court room crying "They stole my business secrets" and expect help. You have to show the extraordinary steps you took (and maintained) to elevate your business information to secret status. Simple LAG will not appear to be extraordinary.

Spy Maxim #5 - Counterespionage is Not a D-I-Y 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 Find Reputable Eavesdropping Detection & Espionage Prevention Consultants...

Contact an independent security consultant who specializes in electronic eavesdropping detection and espionage prevention. Recognizing this person may not always be easy. There are too few of them, and too many pretenders. Contact several corporate security directors. See who they are using. Contact the International Association of Professional Security Consultants via their web site www.iapsc.org

What to expect from your Consultant.

Once you have a few names, take your time, make the right choice. Your relationship will be a long term one, encompassing:

• Periodic inspections of sensitive areas for electronic eavesdropping.
• Information security surveys.
• Information security policy reviews.
• Employee security awareness development.
• Vulnerability testing and security audits.
• General security resource assistance. Do not hire someone who only checks rooms and phones. This is like locking only one door in the building. Information theft occurs in many ways.

When interviewing potential consultants be sure to ask for a detailed resume, and check it for accuracy. You should see a pattern develop:

• True counterespionage consultants devote their careers to practicing their craft.
• Counterespionage will not be supplementary to some other income source.
• 10+ years of solid security / electronic countermeasures experience is normal.
• A license and bond is required in most states.

• Also, expect satisfactory answers on, at least, the following points:
- Formal security / electronics related education.
- The type of instrumentation used.

- Proof of insurance.
- Professional affiliations.
- Security industry professional certifications (Certified Protection Professional - CPP, Board Certified Forensic Examiner - BCFE, etc.).
- Fees based solely on knowledge and service.
- A policy of not accepting remuneration from security product recommendations.

There are additional subjective criteria you'll want to consider also. Personal rapport. Appropriate dress and demeanor. Resist the temptation to bypass Mr. Right for Mr. Almostasgood just because there are some travel expenses involved or the fee quoted was not the lowest. This is false economy. Use the very best person you can find. You may only get one chance to "do it right." Remember, fees and expenses are minor compared to the value of what you are protecting.

ESPIONAGE 301
Detection of Electronic Eavesdropping Devices

The most visible part of the Counterespionage Consultant's job is the Electronic Countermeasures Sweep: the search for eavesdropping devices. It is also the task which is least understood by clients. A knowledgeable consultant will make removing the mystery the first priority. Expect to be educated on the countermeasures process, in terms equal to your prior knowledge level. Everything can, and should, be explained in lay-person terms. Deliberately hiding behind jargon, in any specialty, is rude and should always arouse your suspicions about the true competence of the speaker. From the consultant's viewpoint, the more you know, the more you will appreciate their efforts on your behalf.

Contrary to what may see advertised, there is no do-it-yourself magic bullet in eavesdropping detection. You can't dial a special phone number to see if your phone is tapped. There is not any one instrument which will detect all bugs for you. There is no gadget which will protect you from all wiretappers. Electronic eavesdropping detection is labor and equipment intensive hard work. When your consultant conducts inspections of your sensitive areas, don't be surprised if you meet 1 to 3 additional technicians, and see over $300,000 worth of electronic test equipment. This is how it is really done.

Sweep Inspection Procedures & Test Instrumentation

The 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.) Just like a doctor, your consultant will want to fully understand the symptoms and

circumstances that preceded your call for assistance.

A Survey of Current Security Measures. This includes an inspection of perimeter and interior physical security hardware. Doors, locks, windows, vents, alarm devices, waste paper disposal methods, etc. It should also include a review of your current security policies and procedures. Be prepared to take a full tour of your facility. Have all the necessary keys available, and if possible, a copy of the floor plans.

The Visual Examination.

The areas in question should be visually inspected for all types of current electronic eavesdropping devices and evidence of past attempts. The consultant and technical assistants rely heavily on their eyes, minds and experience. These are the finest detection instruments available. In addition to discovering actual devices during this stage of the inspection, they will also be searching for evidence of prior eavesdropping attempts (bits of wire, tape, holes, fresh paint or putty, disturbed dust, etc.) The visual inspection should be thorough and include: furniture; fixtures; wiring; ductwork; and small items within the area.

The 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. Open air ceiling plenums, air ducts, common baseboard heater ducts, walls common with storage/rest/coffee rooms, and holes in concrete floors have all aided eavesdroppers at one time or another.

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

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 (National Wiretap Commission Report). The newer, electronic telephones have other vulnerabilities, some of which are simple system features which can be abused.

After the instrument is inspected, it is put back together and its screws are sealed over with friable security tape, thus providing visual proof that the phone has not been opened since the last inspection. A good consultant will have these seals custom made so that they can not be easily duplicated. Executives and security personnel may periodically inspect these seals themselves. Broken seals indicate an intrusion, while missing seals indicate a switch of telephone sets. Treat either condition as a suspicious incident.

Inspection of Telephone Wiring.

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

Inspection of 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 relatively safe, place to attach a wiretap device. Extra wiring paths can also be constructed at junction blocks (using the spare wiring already in place) to route the call to a remote device, or

a listening post. This type of common attack is called a direct, or bridge, tap.

Telephone Room Inspection.

The building Telephone Room houses junction blocks for the internal phone system; switching equipment for the internal telephone system; and Telephone Company junction blocks for the incoming lines. This is another area of vulnerability which requires an inspection from both a wiretapping and physical security point of view. In large buildings, this room is usually found in the basement / utility area. Historically, they have received minimal security attention. Expect this to change as more people realize that this is the communications nerve center of their business.

Phone Line Electrical Measurements.

Measurements are taken and compared against telephone industry standards. Readings which deviate from the norm can help reveal certain types of wiretaps.

Time Domain Reflectometery Analysis.

In this test, a pulse is injected into the telephone line. If the two wires are parallel to each other, the pulse continues it's trip smoothly. If the pulse passes a point where it sees a change in the wiring (splices to other wires, a wiretap, a wall plug, the end of the wires, etc.) a portion of the pulse is reflected back.

An instrument called a Time Domain Reflectometer (also known as TDR or cable radar) injects these pulses, reads their reflections, and measures the time difference between the two events. This allows the TDR to calculate the distance to the irregularity. A time verses irregularity graph is displayed on the TDR's display. This signature is interpreted. Imperfections in line integrity are calculated to within a few inches of their actual location. An inspection of these points is made. This allows a thorough examination of the wiring, even when its hidden from normal view. Time Domain Reflectometery allows reliable testing of phone wiring up to 2,000 feet in length, and detection of some wiretap attacks at distances of up to 36,000 feet.

Non-Linear Junction Detection (NLJD)

This detection technique is used to locate the semiconductor components used in electronic circuits, e.g. diodes, transistors, etc.. Bugging devices which contain these components (transmitters, tape recorders, amplified microphones, miniature TV cameras, etc.) are discovered in this manner. They are detectable even when secreted inside walls and objects. Special feature: Discovery is not dependent on the eavesdropping device being active at the time of the search.

Non-Linear Junction Detectors are used only by the best equipped firms due to the cost of the instrument ($15,000 to $30,000). Ownership of the proper instrumentation is, of course, only one indication of competence. But, as the old saying goes, "Its hard to drive a nail without a hammer."

Radio Frequency Spectrum Analysis

Eavesdropping devices which transmit a radio signal (over-the-air, or on building wiring) can be detected by an instrument called a Spectrum Analyzer ($6,000 to $80,000). 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. Each signal is then individually evaluated by the technician to determine if it is carrying voice, data or video information from the area.

The next level up - for high-level corporate and governmental requirements -Radio Reconassence Spectrum Analysis ® (RRSA), consists of military level computer-assisted radio receivers, coupled with microwave spectrum analyzers.

Low-cost pocket bug detectors ($100 to $700) and other broadband receiving devices ($500 to $2,000) should not be confused with (or used instead of) spectrum analyzers. Effectiveness of these devices range from fairly useful in a rural residential setting to useless in an urban business environment. This is due to their common principle of operation... The strongest signal received will be from the bug in the room. Of course, the closer one is to a metropolitan area, where thousands of transmissions are being made all the time, the more faulty this logic becomes. Besides, the rule-book never said the transmitter has to be in the same room as the microphone.

The frequency range of the older spectrum analyzers used in countermeasures work is approximately 10 kilohertz (kHz) to 1.8 gigahertz (GHz). They are outdated by today's standards. Serious technicians, use Spectrum Analyzers capable of tuning as high as 320 GHz. (30-40 GHz is currently more than adequate.)

Eavesdropping radio transmissions can occur at almost any frequency. To give you an idea of the reception capability of a spectrum analyzer, think of your FM radio for a moment. Its tuning capacity is from 88 MHz to 108 MHz, 20 MHz in all; a choice of 4000 frequencies for an electronic eavesdropper to use. This is only 1/90th of what many spectrum analyzers receive.

Radio frequency spectrum analysis should also include the conversion of video signals received to a television type display. This technique detects: Video bugging devices and Computer emissions; signals inadvertently emitted by some computers which can be received and reconstructed a considerable distance away. Also detectable... emissions from a computer which has been deliberately bugged.

Radio transmissions from bugging devices are usually detectable even if the device is only in the vicinity of the areas being inspected. This means that although only certain rooms may be slated for inspection, entire sections of buildings benefits from this particular test.

Thermal Emissions Spectrum Analysis® (TESA)

This technique was pioneered at Murray Associates.

Heat is the graveyard of electricity. It is where expended electrons go to die. Look in the right places for these graveyards, and start digging. You just might find buried electronic surveillance devices... audio bugs, micro-sized video cameras, recorders, wiretaps, and the transmitters which move private sights and sounds to illicit eyes and ears.

The premise is simple. When electricity moves through any electronic circuit, some of the energy converts to heat. This is caused by resistance which is inherent in all circuits. Cooling a circuit to a temperature of absolute zero (0º Kelvin / -450º Fahrenheit) is the only way to eliminate resistance. Fortunately, refrigeration of electronic circuits is not practical in the real world, or the shadowy world of espionage. Electrons will meet with resistance. Heat will be generated. Heat will migrate. Heat can be detected.

Heat may be generally thought of as light waves that are too low in frequency for our eyes to see… thus the term used to describe this is infrared (below red). Neither can we hear radio waves, dog whistles and bats' echo-locating sounds, because the frequencies are either too high, or too low, for our ears to hear. To perceive these out-of-our-perception frequencies we need some type of instrument which will detect and then convert them into something we can perceive. A thermal imager is basically a converter - taking low frequency light waves and converting them to the light frequencies we can see. Loosely speaking, radios perform the same function for our ears.

Currently, price is the only thing standing in the way of complete acceptance and adoption of

TESA to TSCM toolkits. This instrumentation currently costs between $50,000. - $80,000. The good news is that rapid advancements in the field of thermal imaging sensors, combined with increased demand, should cause prices to fall into acceptable ranges within five years. (Note - Murray Associates currently offers this capability to their clients.)

There are three stunning advantages that TESA instrumentation brings to a TSCM inspection…

1. The ability to see slightly elevated temperatures. Example: Inspect 40,000 square feet of ceiling tiles in less than five minutes to find a 1 inch square video camera embedded in one tile.

2. The ability to see density differences in materials. Example: Inspect 40,000 square feet of ceiling tiles in less than five minutes and find where a video camera was - at one time - embedded in a ceiling tile.

3. The ability to see through some materials. Example: Certain materials which appear opaque in normal light become quite transparent when viewed at infrared wavelengths.

Common Misconception...
Inexpensive law enforcement or fire department imagers ($6,000. - $30,000.) can be used if the area being inspected is either quickly heated or cooled just before viewing. This is does not apply to TSCM work. The technique does not increase the temperature differential between a covert surveillance device and its surroundings. Small electronic objects do not have thermal mass. They will track with the temperature change as quickly as most other objects in the area.

The concept that a law enforcement, fire department or electrical maintenance thermal imager can be used in this manner has its roots in applications where the objects being viewed have great thermal mass compared to the features of interest. Finding buried bodies, and infrared examination of the Pyramids are two good examples of this.

"I tried a regular imager. It saw a hidden video camera. So why not just use it? It's cheaper." Yes, the less sensitive imagers will see very hot covert surveillance devices. They are not, however, capable of seeing the majority of surveillance devices, or the slight density differences in enclosure materials which give away current and former installations. To be an effective TSCM instrument, a thermal imager must have an NEdT of less than 20 milliKelvins.

Thermal Emissions Spectrum Analysis is not a replacement for any other TSCM inspection procedure. It is simply an additional technique which greatly enhances detection capabilities.

• **Ultra-Violet Light Inspection.**

In some cases ultra-violet light (long and short wave) will be used to inspect room surfaces. High frequency light can reveal fresh paint / putty, structural changes, hidden wiring, and other evidence of tampering not usually seen under normal light. Other tests which may be conducted include detection of: infrared light transmissions, laser beams, tracking beepers in vehicles, piezo-film and fiber-optic microphones.

• **Additional Tests**

In addition to the aforementioned tests you should be sure the investigative process covers infrared, fiber optic and other eavesdropping threats which will develop after this article is published.

• **The 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. It should include: A description of all the areas and communications equipment inspected. An explanation of all tests conducted. The findings. Recommendations for security improvements. A review of other espionage loopholes found. Security improvements since the last inspection and other useful espionage prevention information.

Final reports are important documents. Safeguard each one. Together they show your continuing effort to provide information security for specific areas within your company. This is your proof that you took extraordinary steps to legally classify your business information as proprietary and secret. You have gone above and beyond LAG. Courts will now listen, stockholders will be quiet, and the industrial spies will have to move on to your competitor's door for easier pickings.

ESPIONAGE 401
Advanced Spying

Your counterespionage consultant would be seriously remiss if only electronic eavesdropping issues were addressed. Our experience has shown that few information leaks can be blamed on active electronic eavesdropping devices alone.

Sure, theft of your thoughts is the most devastating form of espionage. That information is the freshest. But this is only one piece of the puzzle. To see the entire picture, a good spy will collect the other parts as well. Each part may seem innocuous in and of itself, but they are synergistically related.

Espionage from 15 other angles.

Lets look at attack choices through a spy's eyes. Keep in mind: Spies don't look like spies. They come in both sexes, all ages, and all colors. Spies rarely handle all of these jobs directly. Many chores are farmed out. Spies can be: hired professionals, actual end-users, employees, labor reps., etc. and most importantly each of the following attacks is preventable.

- **Spy in Disguise.**

A good spy will be able to enter most premises, day or night, without attracting any undue attention. It may mean taking a job as an office temporary, on the contract guard force or cleaning crew. Perhaps posing as a telephone/air conditioner/computer repair person, maybe even as a company executive returning to work a little overtime. The possibilities are endless. These loopholes exist even in "security conscious" facilities.

• **Dumpster Diving.**

Retrieving secret company paperwork from the trash is easier than people think. Most paper trash is collected in plastic garbage bags, section by section, from within office buildings. Each bag is clearly marked as to what section it came from. (The bags are stuffed with envelopes and other information which identifies whose garbage it is.) Most dumpsters are located in areas of public access. With this in mind, the spy merely pulls one or two papers from each bag until the bag with the target's garbage is found. The whole bag is then removed for inspection at a more comfortable location. This operation is conducted on a regular basis.

Surprise... On May 16, 1988, the Supreme Court decided that "The Fourth Amendment does not prohibit the warrant-less search and seizure of garbage left for collection outside the curtilage of a home." In other words, this practice is basically legal. This decision spawned new profit centers for many private detective agencies, who now openly advertise garbage retrieval services.

• **Plain View.**

Much valuable information is left in plain view during the work day and after hours. Correspondence, manuals, appointment books, Rolodex files, wall writing boards, and other written material all contain information that is free for the looking. Some of these items can be read, or photographed (long distance) through windows.

• **Data Dipping.**

Computers represent a gold mine of information to the spy. Whether the information can be accessed remotely, or disks can be copied on-site and carried off, the results are still the same. High value, low risk, and no evidence of loss.

To further complicate matters, sabotage is also a potential element. Imagine planting a virus in your competitor's computers, timed to erupt when its to your advantage. Chances are someone else has had the same thought about you too.

• **Heard it Through the Tape Vine**.

Dictation tapes are a great source of fresh, and irrefutable, information.

• **Key Topics.**

Most building locks are on a master key system (left open, or easily pickable), and who knows how many master keys exist. Most secretaries keep keys to their boss's offices and filing cabinets stored in their desks (easily pickable). They even keep each other's desk keys there too. To make matters worse, the desks are rarely locked. You can see where this is heading. In most business's the concept of locks and keys providing security is a cruel joke.

• **Advertising Secrets.**

Sometimes paperwork is clearly marked SECRET or CONFIDENTIAL. When not secured, this marking calls undue attention to the document. There are better ways to let insiders know that certain paperwork requires special handling, without alerting the outsider.

• **Ribbons of Knowledge.**

Carbon film typewriter ribbons store useful reproductions of whatever has been typed on them. Spies will take old ribbons and replace them with new ones. No one is the wiser, and the latest correspondence is theirs. Many plain paper facsimile machines have similar carbon film rolls. There, a perfect copy of the original document can be found. Used rolls are routinely placed in the trash. A bonanza for the Dumpster Diver.

• **Let Your Fingers Do the Walking.**

Company telephone directories may be handy

for employees, but they are outright invaluable to spies, executive recruiters, and competitors. Telemarketing people consider these to be the most valuable documents they can obtain. Brokering purloined corporate telephone directories is now a recognized profession according to Target Marketing magazine.

• **Safe-Keeping.**

It is not uncommon for filing cabinets to contain more than just files. Often, they are used to hold valuable documents, corporate seals, checks, keys, etc.. Unfortunately, the locking mechanisms which come with these units fall into the low security category... easily picked, shimmed or jimmied.

• **Help the Spy.**

Photocopy machines and facsimile machines are the two most helpful tools the spy could have. Be sure to leave plenty of paper and toner, and don't audit your supplies or fax phone bills. (Just kidding.)

• **Protect Your Vitals.**

The nerve center of most operations is probably not the president's office or the coffee machine. You could live without both for a few days. No, the most vital room in business today probably doesn't even have a working lock on the door, a fire alarm, an intrusion detector, or even paint on the walls. The telephone room is the most important room in most businesses. It's a taper's heaven, and sabotage hell. A wiretap here, or 'accidental' fire, could put a business - out of business. Do not skimp on protection here.

• **Phone Wizards.**

Most modern business telephone systems, Automatic Private Branch Exchanges (APBX), are computer driven. They often have a Remote Maintenance Administration and Testing System (RMATS or similar designation) feature which allows off-premises access to them. The purpose of this feature is to allow telephone maintenance technicians full access to the APBX from their location. With this, routine diagnostic tests, programming of station/system assignments and features, and repair assessment can be economically performed.

The RMATS feature is accessed by calling the telephone number associated with this feature and linking a personal computer with the internal APBX computer. In most cases access is password protected. However, original default passwords are rarely changed; some have been printed in maintenance manuals; and they can be "hacked" by dedicated spies, or computer hobbyists (curious or malicious). The APBX software can also be entered through an on-site terminal by: the System Administrator (an authorized company employee), a telephone company craftsperson, or an outsider who knows the proper procedures.

Some of the dangers of this unauthorized access include: Complete deprogramming of the APBX. Secret reprogramming to allow access to: WATS Services, Executive Override type features (forced access to busy extensions), Bridge Taps (software created extension lines), "free" phone calls, etc. Monitoring of the Station Message Detail Recording (SMDR) memory. (SMDR maintains a record of each extension's calls in detail.)

• **Now Hear This.**

Telephone privacy is usually assumed. However, due to the nature of telecommunications transmission (unsecured street termination's, radio transmission via satellites and terrestrial links, easy access to phone line junction boxes, etc.) only an average degree of security can be assured without using encryption techniques. This is especially true of international traffic, much of which is monitored by governments.

• **Now Hear This Again.**

Analog cordless and cellular telephones are not secure either. Radios capable of receiving the frequencies used by home cordless telephones, coupled with amplified antenna systems, are generally available. They allow reception as far away as 1 mile. This has recently become a serious method of industrial espionage for the determined spy and opportunistic hobbyist alike. The good news: Digital transmission and encryption is available for both types of phones.

Cellular telephone communications can be received by the general public over hundreds of square miles. Note: After intensive lobbying by the cellular telephone industry, monitoring of car telephone transmissions was made illegal by federal law on January 1, 1987. This law is generally considered to be unenforceable and definitely should not be relied upon for privacy.

Again. All these attacks are preventable. You do not have to be a victim.

Graduation Day

Congratulations! Your business knowledge is now more complete than ever before. No longer will your ideas, plans, strategies, hard work, and privacy disappear mysteriously. No longer will you stand helpless as the opposition picks your pocket. No longer will you live in fear that stockholders will revolt, and judges won't take you seriously. You will not have to standby and wonder if your electronic eavesdropping sweeps are being conducted properly. And yes, you now know the qualities to seek when enlisting the aid of professional counterespionage counsel. You are prepared. Go forth and prosper.

A final word...
You may see yourself in this article. If you do, do not discuss electronic eavesdropping or espionage concerns (in person or via telephone) while in suspected areas. Do not leave this article or other counterespionage literature in these areas either. Continue conducting business in a normal manner while developing your defense. The element of surprise is an important part of electronic eavesdropping detection.

About the author…

Kevin D. Murray - CPP, CFE, BCFE has been solving electronic eavesdropping, security and counterespionage matters for business and government since 1973.

His many written works include: the Electronic Eavesdropping Detection section of The Protection of Assets Manual; articles for Security Management magazine; and Business Snoops... and The Top 10 Spybusting Tips They Don't Want You To Know.

Electronic Eavesdropping Detection and Industrial Espionage - The Missing Business School Courses formed the basis for his college course: Electronic Eavesdropping Detection & Industrial Espionage. Created for the John Jay College of Criminal Justice in New York City.

Mr. Murray is a Board Certified Forensic Examiner; a Board Member of the International Association of Professional Security Consultants and is a Board Certified member of the American Society for Industrial Security.

The Murray Associates corporate client family keeps Kevin and his technical staff quite busy. However, there is always time to make a new friend, and room for one more family member.

He is on the Internet at:
www.spybusters.com
and may be reached at 908-832-7900,
PO Box 668, Oldwick, NJ 08858 (USA),
or via e-mail at murray@spybusters.com

Murray Associates services are available throughout North America and selected foreign countries.

MURRAY ASSOCIATES

MANAGEMENT CONSULTANTS TO BUSINESS & GOVERNMENT ON ELECTRONIC EAVESDROPPING DETECTION & BUSINESS ESPIONAGE PREVENTION