

Electronic Eavesdropping Devices

The Hardware Side of the Offensive

By Felipe Guillen

January 2004

INTRODUCTION. The use of electronic eavesdropping devices (“bugs”) to covertly listen in on the confidential discussions of competing companies as illegal as it may be in the U.S., is never the less an old and oft practiced tactic. A key element of its success and primary reason for its continued and expanded use by today’s less than ethical firms and individuals, is the fact that it is a tactic rarely detected by most victims – and the end results of its use are nothing less than stunning! Companies not specifically prepared to detect and counter the use of this aggressive and financially destructive assault when used against their firm, will stand no chance of surviving the losses that will follow.

M/WBE firms are not only **not** immune to this form of illicit business aggression, but may be especially targeted for compromise by such tactics by those who realize that many privately owned enterprises are in fact the least prepared to protect themselves from this insidious form of “silent theft”. Most major companies on the other hand, are well aware of the dangers associated with this class of aggression and take the necessary precautions to insulate themselves from many forms of such discreet assault. This article will detail just what type of electronic hardware or eavesdropping devices, makes business espionage the successful and ever evolving threat to business that it is today. While it would be beyond the scope of this article to describe every type of modern eavesdropping device, it will none the less detail the more easily obtained and thus used devices in circulation today by both the amateur and Pro.

THE THREAT. Bugging devices come in many forms and are designed for specific duties. Some bugs for example are designed to primarily intercept and transmit **telephone conversations**, while others specialize in the interception of **office conversations**. There are also hybrids, that intercept both office and phone conversations – room conversations when the phone is “on-hook”, and phone conversations when the phone is “off-hook” or in use. In addition, there are also **video** class bugging devices, which broadcast both the picture and sound of the victims activities. All however have several characteristics that are common among the bug family, they are all miniature in size, easily and rapidly concealed, and transmit a clear and clean broadcast signal of the intercepted conversations and/or video.

Unfortunately, bugs are easily obtained by even the general public, with incredibly effective models starting at cut-rate prices – typically only forty dollars and up. Worse, the vendors of these devices almost always provide a quick instructional to the buyers, on how to properly conceal the bugs – as well as selling the buyer concealable receiving and recording equipment. The receiving equipment allows the buyer to easily and covertly receive and tape the transmitted signals, at their desk, parked vehicle, nearby Listening Post (LP) such as a nearby office, residence, building etc., - **unattended**. Thereby allowing the eavesdropper to review the day’s recordings from the comfort of their home later that evening. Optionally, they may choose instead to employ a long term recorder which would record for a week or even month, before needing a new tape. The choice is up to the buyers and their intentions.

The combination of easily obtained effective bugging devices, free instruction and the low cost for a complete receiving system, has significantly increased the use of such illicit equipment and tactics – as well as notably increased the losses and damage sustained by the victimized firms and individuals. As this type of activity leaves no readily identifiable “footprint” (unless a full Sweep Survey is performed), victims rarely know that they have been victimized by an eavesdropper and his/her electronic spies.

Bugging devices typically smaller than a postage stamp (and only a tenth the size and even smaller in the case of professional class devices), can operate for days or weeks on their internal battery supply, or permanently when connected to the phone line or AC lines. Their broadcast range can extend to only a quarter mile or so – to several miles if the eavesdropper chooses to install longer range devices.

Favored concealment areas for these micro-miniature bugging devices include but are not limited to; ceilings, walls, telephone instruments, computers, FAX machines, electrical fixtures including lights – switches and outlets, within office furniture and desks, in wall hangings such as pictures, within decorative figurines and other office adornments and curios, in conference room teleconferencing and projection equipment etc., where ever targeted conversations may be present and intercepted. While the professional operative is **far** better at device concealment than the average amateur, amateurs are steadily causing more and more damage to their targets as improvements to modern transmitting devices - rapidly help make up for many of the short falls in their tactical and technical expertise.

Many bugging devices begin transmitting only when they detect conversation in the offices (or on the phone), and will then go back to a “stand-by” or dormant mode when conversation stops – awaiting the next discussion to resume their broadcasts. This not only conserves battery power in the case of battery operated devices, but also conserves recording tape at the receiving end since extraneous office sounds are ignored. Miniature tape recorders and the modern crop of micro-chip based (non-tape) voice recorders are also be employed for bugging operations, though they are usually shunned due to the higher risks associated with their use - as that they must be constantly retrieved before the collected conversations can be played back. Transmitting type bugs on the other hand, need only be placed once thus requiring gaining access to the victims offices/phones only one time – to receive a remote and constant broadcast of all future office and/or phone conversations (the exception being battery operated devices, which would require a periodic replacement of their batteries – though they are usually long life).

A common misconception with regards to telephone bugs, is that if their phones are in fact bugged - the victim will hear “clicking” or other like noises during a conversation. Unless the eavesdropper is a bungling amateur, no noise what so ever will be heard by the victim. Today’s telephone bugs need not even make any physical contact with the phone wiring, but need only to be brought within about an inch or two of the targeted wiring to successfully and discreetly obtain a complete intercept of all conversation. Further, these bugs may be placed either inside of a telephone instrument, or anywhere along the wire run including wire rooms, other internal building locations or floors or even outside of the building such as at phone wiring boxes/panels, poles, etc., – they do not need an actual phone instrument to operate!

Vehicles are not immune from electronic compromises either. Today, vehicles are easily tracked in “real time” to provide their actual location – as well as intercepting the conversations held within their confines. Many private investigator types routinely use todays electronic devices to accomplish these goals.

THE SOLUTION. Protection from these forms of compromise (industrial espionage) must be multi-faceted - i.e., based on both prevention and detection/verification strategies. Proper intelligence security controls must be implemented in all executive offices to help prevent initial compromises and violations of the firms sensitive data and discussions. These controls are threat specific to each clients particular risk exposures, and are determined only after a comprehensive vulnerability assessment has been performed of the facility and offices to be secured and the potential aggressors identified.

Detection and verification programs are second tier components, designed to insure that the protective protocols and controls are in fact effective - and that sensitive information and discussions are actually being protected. This phase includes such critical procedures as the execution of detailed **Spectrum Analysis Sweep Surveys**. These surveys are special procedures designed to detect the transmission signals of concealed eavesdropping transmitters operating from within the confines of the executive offices, phones, vehicles, residences, etc. The positive detection of any such radio signals would confirm the existence of an active surveillance program, and verification that a breach of the security precautions has in fact been successful. This phase employs advanced, specialized detection equipment and procedures to conduct the signal detection and tracking portions of the Sweep Survey.

If a signal detection has in fact been made, positive proof has then been established that the checked offices and areas are in fact under some form of surveillance and observation by as of yet unknown entities. The next step would involve specific procedures to identify the location of the concealed transmitting devices. These subsequent procedures are performed during the initial Sweep Survey.

NOTE: Professional operatives as a rule employ multiple eavesdropping devices placed in various key locations of the targeted offices and conference rooms, including phones/lines. Amateurs can be quite unpredictable and may or may not use multiple devices – though odds are they too will place more than one device, owing to the low per unit cost of today's modern collection of bugs.

This potential for successful penetrations and compromise of even secured facilities (often attributable to carelessness by key personnel, unenforced security policies and procedures, and/or "inside" help), is the reason that scheduled intervals of interim verification Re-Sweep Surveys - must be chosen so as to limit the window of potential loss. For example, if verification Re-Sweep Surveys are scheduled for only once per year – the available loss window (a.k.a. "Vulnerability Capitalization") is one year. Effectively, an entire year's worth of sensitive internal discussions and information may be lost before the next Sweep Survey is performed, where the existence of concealed transmitting devices would be made known.

The appropriate interval of Re-Sweep Surveys must be determined by each firm's senior management, and the acceptable window of potential loss (should security controls in fact be breached) be defined as would be considered to be acceptable by them. Elements or "Threat Multipliers" which would have a direct bearing on this decision include; [1] the level of known or suspected competitive and/or aggressive activity directed against the company, [2] the extent and effectiveness of the security controls as adopted and maintained (enforced) by the company, [3] the type of business or sensitivity of the work being performed by the company, [4] the degree of cooperation exhibited by the employees and executives of the company in maintaining security controls, [5] whether or not the company is involved in any current or future legal or court actions and/or internal company instability or turmoil, [6] recent defection of key personnel to competitors, [7] company planned acquisitions or take over attempts, etc.

Thus the reason for a multi-theatre based intelligence security program is clearly demonstrated. Unfortunately, the complexity and loss magnifiers comprising the potential for information losses via acts of industrial espionage – clearly rules out the possibility of security controls being a quickly deployed "one size fits all" format of pre-packaged solutions. The extensive risk variables and avenues of vulnerability mandate that preventative solutions be carefully arrived at, only after a comprehensive and detailed assessment has been made of each client's unique situation and business status.

The remainder of the required follow-up actions and protocols to be executed when a breach of security is in fact verified, we regretfully cannot discuss further here – as this would involve the disclosure of proceedings whose effectiveness would be compromised if carelessly disclosed. Suffice it to say that these follow-up protocols are intended to maximize loss control efforts, while also addressing the issue of personnel and parties which may be responsible for the commission of these illicit activities.

Help insure that you and your firm are properly protected against the insidious and increasing acts of business espionage. Perform an audit of your current internal security controls, and insure that you have a viable and effective intelligence security program in effect. Remember, case histories are **replete** with examples of firms that did not have appropriate controls and programs in place for the protection of their proprietary information – and subsequently found it difficult and in many cases even impossible, to prosecute personnel which were found to have committed acts of espionage against their firm. Courts have reasoned that if the claimed stolen information and data was in fact of a critical and confidential nature, the company would have demonstrated this by its actions in properly and continuously monitoring and protecting the information - by enacting and maintaining appropriate, observable security controls!

FOR ADDITIONAL INFORMATION. The author can be contacted at:

Mr. Felipe (Phil) Guillen, President
OMEGA, Inc.
P.O. Box 964
Tinley Park, IL 60477 708-429-1563

OMEGA is a Minority-Owned Business
Copyright 2004 Felipe Guillen. Used with permission.