



MURRAY
ASSOCIATES

C O U N T E R E S P I O N A G E C O N S U L T A N T S T O B U S I N E S S A N D G O V E R N M E N T

SECURITY ALERT WIRELESS MICROPHONES

A CASE HISTORY

Our client, an international corporation, planned to hold their annual sales meeting at a resort, hotel and conference center. A year's worth of effort involving new products, marketing strategies and pricing would be discussed that week. Very confidential information.

Security was going to be tight. Rooms would be swept for electronic eavesdropping devices. Access to meeting rooms would be controlled. Paperwork would be collected after each session. Participants would be briefed on industrial espionage awareness.

Their security manager had left nothing to chance.

In the early morning hours before the opening of the meeting, our electronic countermeasures team detected a strong radio transmission emanating from the main conference room. The signal permeated half the hotel room wing and reached out into the parking lot.

A wireless stage microphone, belonging to the audio-visual contractor, was found near the podium.

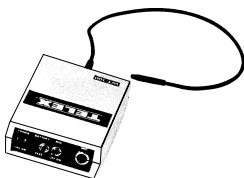
HOW IT WORKS

Basically a miniature FM radio station, a wireless microphone is worn by a public speaker. The sound of the person's voice is transmitted to a nearby radio receiver, amplified and played through loudspeakers so the audience can hear more easily. In some cases it is also used to establish a link to a video camera, or tape recorder.

Unfortunately, these radio transmissions do not stop at the receiver. Wireless microphones can transmit for distances of 1000 feet to a mile. *Any* receiver tuned to the same frequency can listen in.

Wireless microphones are among the latest gadgets to catch the fancy of public speakers. Along with laser pointers, and large screen computer displays, wireless microphones allow the presenter more freedom of movement. In many meeting situations they are a welcome addition. But, not when the discussions are confidential.

WIRELESS MICROPHONE
Range: .25 miles.*



* From the manufacturer's specification sheet.



DON'T BUG YOURSELF

Commercial wireless microphones are *designed* to broadcast crystal clear audio, and their signals travel much further than most people realize. Anyone can exploit this. Competitors, the press, even employees who are not invited to senior level meetings, for example.

When targeting your meetings, the opposition will set up radio receivers and tape recorders in one of the hotel's rooms, or in an unoccupied car parked nearby. They are betting you will use wireless microphones, cellular telephones, and make a variety of other simple security mistakes. You will never see them.

In our *case history*, the audio/visual aids contractor *was* told not to use wireless microphones. They didn't. The microphone we found was packed in their excess gear, left near the podium. Was it left operating inadvertently, or was someone paid to leave it on? Probably the latter. The battery was fresh. Although the intent can not be proved, it does not really matter. The entire meeting would have been broadcast in either case.

ESPIONAGE IS PREVENTABLE

Ban wireless microphones from your meetings. Be explicit and be firm. Do not allow this equipment in the room, even if it will not be used. (Since guest speakers often bring their own equipment, be sure to advise them of your rule too.)

When securing meeting rooms, and during the meetings themselves, be sure to check the radio frequency spectrum for all types of emissions which could carry room audio from your location. Common wireless microphone frequencies fall in the range of: 150-200 MHz, 450-452 MHz and 947-952 MHz.

Bugs, wireless mikes designed specifically for surveillance use, do not have assigned frequencies and can be found anywhere from 25 MHz on up.

Also...

- Avoid using a public address system of any kind if possible. If not...
- Use a podium system at low volume. If necessary...
- Use the hotel's direct wired microphone and room speakers, at low volume.
- Don't use cell, cordless, rail or air phones for confidential calls. All are radios.
- Call us to secure your next meeting. There is much more to do.

Eavesdropping on wireless microphones at conference centers is only one spy trick. There are hundreds more. Remember – Espionage is Preventable. For further information about pro-active programs to combat espionage, electronic eavesdropping and wiretapping please contact us.

908-832-7900
www.spybusters.com
Box 668, Oldwick, NJ 08858