How to Combat the Threat

Combating the Threat

The best security measures should not obstruct an organisation's main functions but still meet the threat adequately. The choice of services and equipment is important. Choose wrongly and a false sense of security will prevail. Each new advance in communications technology brings with it added risks for the security manager.

Those who remain complacent of the dangers may well become victims of the electronic spy - though they may never know it!

- Preventing installation
- Constructing a safe room
- Physically searching for eavesdropping devices
- Interfering with operation of the device or making information unintelligible
- Using special countermeasures equipment to detect and locate devices

Preventing Installation

Since some eavesdropping techniques demand installation of a device in or near the target area then denying access eliminates the threat from these techniques. In an active business environment it is possible to prevent any unauthorised access without creating an unworkable environment. Sensible physical security measures can reduce the threat to a particular target area substantially forcing the eavesdropper to take greater risks or switch to a less successful eavesdropping method.

Constructing a Safe Room

Safe rooms are used extensively within embassies. The safe room is surrounded by sound/vibration absorbing material and metal shielding to prevent passage of sounds and radio signals respectively. Any cabling linking the safe room to its surrounds are either disconnected during occupation or filtered and monitored to remove/check any signals passing along them. Since the safe room is compact and totally enclosed physical security measures to prevent any unauthorised access are easier to implement.

AUDIOTEL INTERNATIONAL

How to Combat the Threat

Within an industrial environment the construction of a safe room of this type is usually impractical. It may, however, be practical to designate an existing room a safe area and by improving physical security measures and using physical and electronically aided searches substantially reduce the risk of that room being compromised.

Physical Search

A complete physical search of a target area is very time consuming and generally impractical. If, for example, a microphone and cable were buried in a wall during re-building or decoration work then it would have a very high degree of immunity to discovery by physical search. Likewise, it is not practical to check a telephone line along its length to the local telephone exchange.

Physical search is useful if restricted to areas more easily accessed. For example, a suspended ceiling offers an excellent hiding place for microphones, tape recorders etc. Such areas can be searched quite easily. Ducting carrying power and communications cables are usually also accessible. During building or decoration work it is practical to check work during the evening or lunch breaks to ensure no illicit equipment is being installed.

Interference Methods

Within this context 'interference methods' describe any technique that either renders the device inoperable (jamming equipment is used) or renders that information gathered unintelligible (scrambling/encryption equipment is used).

Jamming equipment designed to counter specific types of eavesdropping device is offered by some suppliers. In general such equipment is ineffective or dangerous in its operation.

For example, some equipment for tracing telephone taps and microphones incorporates a high voltage pulse generator. The principle of operation is that a high energy pulse will destroy any eavesdropping device attached some distance away on the pair of wires. Use on public and private telephone networks is potentially damaging and dangerous to personnel. In addition, it is relatively simple to include high voltage protection within an eavesdropping device.

Noise masking techniques, in which broad band acoustic noise is emitted at the boundaries of a room, can help prevent casual or deliberate listening by someone just outside of the room. In general, noise masking would not be effective against a well-placed eavesdropping microphone.

AUDIOTEL INTERNATIONAL

How to Combat the Threat

Optical jamming is more practical. The simple precaution of closing curtains prevents any optical signal passing through the window.

The use of scrambling/encryption equipment to protect both speech and data communications is the only effective way of countering many speech and machine interception methods. With respect to use of a telephone scrambler then provided that room conversation is not being overheard and the scrambling equipment itself has not been compromised then telephone conversations can be secure.

Use of Countermeasures

Special countermeasures equipment can provide good protection against a range of threats. Such equipment is designed to detect and, where practical, locate any offensive device. It is usual that the existing security staff within an organisation are responsible for implementing countermeasures. It is essential, therefore, that any countermeasures equipment used has been designed for non-technical personnel. Good equipment is available for:

- Detecting and locating radio transmitters hidden in or near any target area. Such equipment must be capable of detecting transmissions over a range of 15 KHz to above 1.5 GHz (1,500 MHz) within a target area from innocent sources originating from outside the area.
- Checking cables for the presence of room audio signals.
- Checking cables for the presence of any carrier transmission relaying room conversation.

Equipment is offered by companies for detecting telephone taps. Some taps do affect the electrical characteristics of a telephone line such that the change is distinguishable from other changes that might occur due to innocent causes. However, well designed taps are, for practical purposes, not capable of detection by these means. The limited protection offered by tap detection equipment must be understood if such equipment is used.

It is our understanding that, at present, no special countermeasures equipment is available for detection of optical transmissions. However, a combination of physical measures such as drawing curtains and searching easily accessed areas offers a good level of protection.

AUDIOTEL INTERNATIONAL