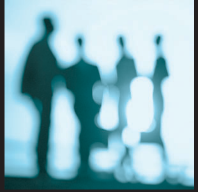
A Threat To Business



What Is Electronic Surveillance?

Before examining electronic surveillance and countermeasures techniques it is important to identify precisely what is meant by electronic eavesdropping or technical surveillance and what types of material are most at risk. Many executives seriously undervalue the importance of information within their own organisation. Information is the most important and valuable asset to any organisation but often the same degree of protection is not given to the spoken or written word as is given to physical assets. Information on prices, competitors, staff, plans, acquisitions, new products and new technology, in approximately that order, is most at risk.

We define eavesdropping as a predetermined attempt to obtain information that would normally be withheld. It is hard to quantify exactly the number of people and organisations involved in such activity. We also have to recognise that eavesdropping is another form of research that most people use at one time or another in their personal or working lives. How many times do we ourselves 'innocently' eavesdrop on the next table at a restaurant and how many letters or reports are casually read over a secretary's shoulder when being typed? True, much information gathered in this way is trivial and not too sensitive. But isn't that the nature of espionage activity anyway? Apart from private investigators who offer their services professionally we should also consider as a possible threat professionals in selling, marketing, science, engineering, journalism and purchasing who are paid to research and gather information.

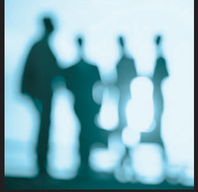
For example, in the case of a company takeover, it would be perfectly acceptable for a chief executive to ask for a detailed report on the activities and performance of the target company.

Such a request could then be acted upon in several perfectly legitimate ways by enquiries as to previous years' peformance, questions asked of employees, main customers and suppliers, and, possibly visual surveillance of the target company's premises and directors' homes for analysis of movements. These activities do not transgress any law and would normally be considered prudent attempts to establish the viability of the takeover action. The vast majority of company executives would not seriously consider extending such activities beyond the law.

However, it is possible to envisage a scenario where other techniques could be employed, often without the knowledge or agreement of the person originally authorising the investigation. A competitive situation has been created by company executives who have commissioned private investigators or consultants to advise or provide information on organisations of interest. How results are obtained is not of immediate interest to the executive but more the quantity and accuracy of information provided by the investigator. From the proliferation of reported bugging incidents and the recent rapid growth in the sale of electronic bugging equipment, it is apparent that more and more investigators and consultants are resorting to electronic and often illegal means to improve the quality of service to their clients.

AUDIOTEL INTERNATIONAL

A Threat To Business



The use of electronic methods brings to the investigator a whole new dimension. He is able to acquire information in real time directly from the source, be it from a meeting, telephone conversation, computer hard disk or any other communication path. Depending on the bugging method, the quality of this intercepted material can be very high indeed. Other investigative methods depend on information being relayed second or third hand with the possibility of it having been corrupted in transferral or having been altered in some way to mislead deliberately.

A feeling often evident is that countermeasures is strictly the province of the electronics engineer or technician making a periodic survey of the target area. Nothing could be further from the truth. In reality this type of inspection forms only a small part of effective countermeasures. It makes no sense to have a room checked for devices and then leave that room unguarded.

A wider perspective must be taken. We are familiar with the need for asset protection. We now need to look at information as requiring a similar level of investment in its protection.

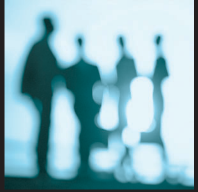
Countermeasures against the eavesdropping threat are organised in-house as much as possible with the use of outside consultants only for specialised tasks. It follows, therefore, that someone within the organisation should become familiar with surveillance and countermeasures techniques. Audiotel International, run a regular seminar describing in detail the threat and available countermeasures.

Prior technical knowledge is not needed to understand the basic principles. It is however necessary to identify the objectives of a regular countermeasures survey. That is, which areas and information are to be protected and with what periodicity. As in other areas of security, a high level of protection is given by good physical security and commonsense procedures. In addition, there is a wide choice of electronic equipment available to improve and extend the level of protection.

The time taken to carry out a survey for bugging equipment may be wasted if measures are not taken subsequently to prevent installation of equipment and countermeasures equipment is not on site to check for bugs on a regular basis. Examples of good procedure would be keeping sensitive areas locked, document security and careful use of telephones. It should be recognised that information can also be lost through photocopying and theft of paperwork, theft of unshredded wastepaper, an employee passing information for money, under duress or for ideological reasons, and overhearing conversation in public places.

AUDIOTEL INTERNATIONAL

A Threat To Business



Audiotel International strongly recommend that the implementation of standard procedures is incorporated into a general security policy circulated to the appropriate personnel. It is essential that countermeasures are understood and viewed in context. For example, there is little point in investing in equipment if confidential information is casually thrown away. Senior personnel must appreciate the need for electronic countermeasures and implement them as an integral part of the security policy.

The rapid and recent increase of equipment and services which has led to some confusion in this area means that today's security manager and company executive need to acquaint themselves fully with the basic elements of bugging and countermeasures techniques.

The effect of technology is felt with each new advance. Whatever makes communication easier will also make it easier to lose information.

AUDIOTEL INTERNATIONAL