"Spying at Work -- espionage, who, how, why, how to stop it"

[youtube:http://uk.youtube.com/watch?v=kooznkqQ1GQ]

Surveillance is getting easier. Bugs are getting better. The other day I was lecturing to twenty senior executives from a major international high technology company on the future. During a fast moving multimedia presentation, which included virtual reality, videoconferencing, Internet television, Cyberbanking, and a host of other related technologies, I bugged one of the participants. Right under their noses - as a demonstration in a country where such a demonstration of surveillance was legal. Even as they watched me pace around them, one of them was now carrying a minute transmitter capable of being picked up half a mile away. The device would have landed up being carried into the next meeting or the hotel bedroom. Devices today are so sensitive that even with a receiver the participants were unable to decide who was carrying the transmitter. Everyone could hear the sound of his or her own breathing. They were shocked.

Surveillance devices can be turned on/off from a mile away.

That means a board room will test negative when screened for surveillance devices just minutes before a vital meeting, and afterwards, although the bug may have been transmitting every word spoken during the entire course of the meeting. These kind of surveillance devices are extremely difficult to detect, requiring equipment that is complex, expensive, and time-consuming to use. In theory every room used for sensitive meetings needs a screening every time it is used. The only possible exception could be rooms that remain permanently locked except when used by a very select group of people. But a sophisticated screening to detect non-transmitting bugs may take several hours. Remember that most commercial breaches of security are created by staff themselves who agree to betray their own companies for money.

And just in case you were still under the delusion that a swept room is secure, devices are available using lasers which allow someone to listen to a conversation taking place half a mile away using equipment operating at that distance. Laser light reflects off window glass, carrying with it vibrations from noise inside the room.

Then there are the cameras.

A high quality colour video camera operating in bright or dim light can now be squeezed into a screw head. The centre of a Phillips screw is more than large enough to contain the lens of

such a camera, which can therefore be concealed in any light switch, or any area of any room where a Phillips screw head is visible.

Networking means that every word spoken in one room in Australia can be heard in precise detail in any other country of the world day and night, using local telephone calls and Internet encryption.

Most companies are still in the Stone Age when it comes to commercial security. Most of their attention has focused on such things as password protection for systems, or identity passes at the security gate. Those measures are useless against the constant threat of commercial espionage -- a boom industry judging by the rapidly growing turnover of company making these devices. Counter espionage has often become the same technologies turned against one's own staff. Bugging of friends, rooms, cars or even homes has now become a routine part of commercial self protection. Of course one of the big markets for all this is the divorce industry with spouses trying to catch each other out, or to lay jealous fears to rest.

So what happens to privacy?

Privacy died a long time ago. In some countries use of concealed transmitters is against the law yet these things are widely available for decreasing cost. When it comes -- say -- to mergers or acquisitions, or other price sensitive market information, a single phrase may acquire a commercial value of several million dollars all more. Thus theft of "words spoken" has become one of the highest value crimes that can possibly be committed. We urgently need international agreement that covert electronic surveillance is illegal except for enforcing law and order. The sale of these devices should be banned in every nation - they can all be bought in the UK with total freedom. The market will still be there but it will send a clear message.

So how can you protect yourself?

Firstly, you should assume that whatever room you are using is insecure unless otherwise proven. You should also assume that participants in meetings may occasionally be wired themselves, and that participants leaving a room in the course of a meeting may be hearing every word said after they have left. It's the oldest trick in the book. Regard with suspicion any small gift that the donor might expect you to keep in your office, or put in your pocket. Examples included expensive pens, paper weights or any other object. Strangely enough, a meeting in a restaurant which is busy and noisy could actually turn out to be safer than your own boardroom or videoconference suite.