John Little examines the importance of TSCM and ensuring that no one else is listening into your private conversations

AN END TO EA

Eavesdropping is historically a medieval term from when most dwellings were single storey, the roof rafters supported on the top of the walls, the roofing material laid on the rafters. Thus, anyone standing under the eaves would be able to hear what was being said in the house through the air gap between wall and roof. Sun Tzu's *The Art of War*, written around 500 BC refers to intelligence and intelligence gathering. There are references to espionage in the *Old Testament* and eavesdropping is depicted in the Bayeux Tapestry. Meanwhile, a "Tap" of telegraph/telephone lines is known to go back to the nineteenth century.

The view of eavesdropping can vary with culture, in some societies it is considered fair game, part of the rules of engagement, it is up to you to defend yourself. From the standpoint of an information defender, one must take the view that eavesdropping is part of the human condition.

A bug is the generic term for a device that will enable listening into a source of information. Traditionally this is listening to the spoken word. Miniature radio microphones appeared thanks to the development of the transistor. Bugs have since evolved to include video transmission following the development of miniature cameras, and keystroke data attacks in computer keyboards.

The unprecedented proliferation of mobile phone technology has been harnessed by bug manufactures. The GSM bug can be accessed from anywhere a cellphone is available – which is to all intents and purposes everywhere in the world. The devices themselves are very inexpensive, the trillion-dollar global network is something we do not have to pay for, just make the occasional call or text – small change.

When a new type of bug appears, it does not replace the devices that are already out there, it simply adds to the threat. These bugs are not bio-degradable – they just need fresh batteries. Consider, therefore, the cumulative effect of 60 years of bug production. Cyber attack is rightfully a matter of grave concern, but it does not replace the threat of the traditional concept of eavesdropping, which is still as large a concern as ever.

In the beginning, bugging devices were difficult to acquire, the man on the street would not know where to find them – if they even knew they existed. They were relatively expensive, and the technology adequate meaning that it did require expertise to deploy. The equipment to find them was of a similar level of technology.

Over the last 10 years there has been monumental change in this dynamic. During my 48 years of involvement in TSCM I have never seen such a dramatic shift in this threat. Bugs are now readily available to everyone on eBay, Amazon and vast numbers of suppliers across the web. Put "Bug" into any well-known search engine and the hits will go off the screen. These things are not made for stock, the sheer number of devices on offer is a testament to the size of the market. Costing as little as nine Euros they can be operated by the non-technical, for example, in the case of cellphone technology simply insert a SIM card and switch on, for a radio mic just insert a battery. Victims of technical attack span all bodies, from government and corporate to private individuals.

The law against illicit surveillance in the UK and in many countries, is not extensive. Many devices now operate on license-free frequencies, meaning that contravention of the Wireless and Telegraphy Act does not apply. The planting of a surveillance device can be carried out in such a way to avoid detection, nothing damaged or stolen. In most cases the attack is either carried out, or facilitated, by someone that has the right to enter the property. Thus, no deterrent.

Bearing in mind that intellectual property can

©Getty Images

Serbian technicians remove listening devices from the Foreign Minister's party HQ

VESDROPPING?

be considered priceless, even the more elaborate technology can result in a colossal return on investment. In short, low cost, low risk, high ROI, - it pays to bug!

If there is a loss of computer equipment it can be replaced, a software glitch is inconvenient but you can recover it. If you have your confidential information, trade secrets or data base stolen, you are finished. There are many assessments of the financial impact of industrial and officially sanctioned espionage, but the word "billions" is common.

Defense in depth is a common concept but defense in breadth is the approach that I believe is required. Attack spans a host of technologies – audio, RF, GSM, ultra-sonic, visible light, invisible light, inductive – that can be line born, spatial, structural (water works quite well). The level of technology is an aspect all too often over looked, meaning that low-tech as well as hi-tech must be in the scope of defense.

The primary parts of Technical Surveillance Counter Measures should cover Audio, RF, Physical, all linked by Training. The line between IT Security and TSCM is constantly changing with TSCM teams steadily increasing the overlap between the two disciplines. This frequently involves a team member who has the appropriate background which is very different to TSCM in the traditional form.
Without thorough training in task procedure, equipment deployment and operation, a sweep is nothing more than a tick in a box. Therefore training must include Health and Safety legislation and in some cases Expert Witness capability.

Continuous Professional Development is vital in this ever-changing technological arena. To this end the TSCM Institute (TSCMi) was formed some years back after the development of the National Occupational Standards (NOS) for TSCM – something that is unique to the UK. Contributions from some 20 TSCM practitioners created these standards, so they are representative of the industry.

TSCM is a dynamic technological area and remaining fully aware is a challenge. The awareness at the upper echelons of organisations, is often sadly lacking and – as I have observed on a number of occasions – the view is that: "I am so important, I could be bugged, but I naturally should be bugged with technology befitting my station in life". Well, have I got news for you, the attacker has no such illusions of grandeur and is going for a result. For professional attack teams, the first line of attack is a pair of wires – the wired microphone. Very reliable, high-quality product (the recovered speech), low-tech, low-cost, and many sweep teams are not even looking for them. Hence for many years Shearwater TSCM has produced the Bloodhound, a wired microphone detector.

The TSCMi is a source of help for the Security Manager. This year, a B-Tech 4 course will be available – "TSCM for Security Managers" written by the TSCMi and operated by Perpetuity Training. This is aimed at making the Security Manager aware of TSCM and how to recognise and assess a professional Sweep Service provider.

The onslaught of modern technology installed in many buildings can result in potential weaknesses that can be exploited by the attacker. No access would be necessary, just a listening post within range. Specialist knowledge would be required, generally not a task for a casual interloper, but the right expertise is available, possibly former operatives of intelligence organisations from many parts of the world… for a price.

Some years back, a bug in a crematorium was my most bazar task to date, and a long way from KGB bugs in the mid-seventies. Initially, I had difficulty

AN END TO EAVESDROPPING?

accepting that this request was not a hoax. At the outset, I look for three factors – Asset, Risk and Threat. After some discussion I found nothing to represent any of these, I looked towards personnel – any problems? Yes, a member of middle management had been dismissed some six months previous. (Risk). He had since gained employment with the "competition". I immediately had visions of hordes of marauding Funeral Directors body snatching in the streets! Not so, the competition was regarding the other business, crematoriums provided as a turnkey business, suitable site, planning, architect, building construction and grounds. I do not consider this profession exciting, but it does have regular work.

An aggressive foreign competitor (Threat) had engaged my client's dismissed manager. It was from this manager's former house in the grounds that it was discovered that conversations taking place in the chapel, where all business discussions took place, could be overheard with the house telephone. Over the previous six months, three contracts had been lost by a small margin (Asset).

After a search, it was found (with a Shearwater Bloodhound) that the Acoustic Loop – an EU directive for the hearing impaired for meeting places – had been inappropriately installed a year before. The building leaked, no intentional bug, but an exploitable weakness.

The Merlin MK3 is the latest version of Shearwater TSCM's Merlin, the MK1 first release was in the late nineties. The Mark 3, although in appearance not so different from the MK1 and 2 is a much more advanced TSCM spectrum analyser tailored to counter the RF component of the present-day eavesdropping threat. Its key features include 30GHz bandwidth, ultra-fast scan (up to 350GHz per second), Wi-Fi Control (iPad included as standard), Ethernet remote control, hot-swop batteries, recordable waterfall (scan and demod), multi-format control for Mac, PC, tablet and smartphone, digital video demodulation and IQ recording and analysis.

The 30GHz bandwidth is part of the futureproofing concept, to cope with tomorrow's technology. The speed of scan for the ever more agile devices becoming available. Wi-Fi control facilitates rapid deployment, the Merlin being battery powered – and the operator could be the other side of the wall. Ethernet architecture is fundamental to Merlin, thus remote control. The recordable waterfall in scan mode is there to aid the detection of "Store and Forward/Burst" devices, while the second recordable waterfall in the demodulation section is there to assist with the detection of Store and Forward/Burst transmissions. In addition, on one deployment a movement detector was discovered with this facility, a most useful feature as many GSM devices are movement triggered. Digital Video demodulation is on hand to view and eliminate DVBT and ATSC television signals.

The modular receiver is a Shearwater development. There are two inbuilt quad-core computers, one with Linux operating system for the receiver, the other for the Shearwater scanning software. Merlin is Kestrel compatible. The fold up antenna array is complimented with separate inputs for HF/VHF antennas and included is a directional antenna that can connected to the 30 GHz AUX input.

A Mains monitoring interface is included in the Peli/Storm custom lined transport case.

Armed with such a device the chances of vital information – that could give your rivals the advantage – being listened in on without your knowledge is vastly reduced, giving you the peace of mind to carry on with your business in a secure environment.

John Little's background is in the Foreign and Commonwealth Office and he now owns the established company Shearwater TSCM, based in Bletchley Park. Specialising in TSCM equipment design and manufacture, training and Sweep services, he is a Founder Member of the TSCMi, and Fellow of the Security Institute.

The Shearwater Bloodhound can be used to sniff out hidden listening devices