Corporate and industrial espionage present a serious security threat. Gavin Saul explains how to ensure you choose the right provider of technical surveillance countermeasures to protect your privacy and critical information

SWEEPING STANDARDS

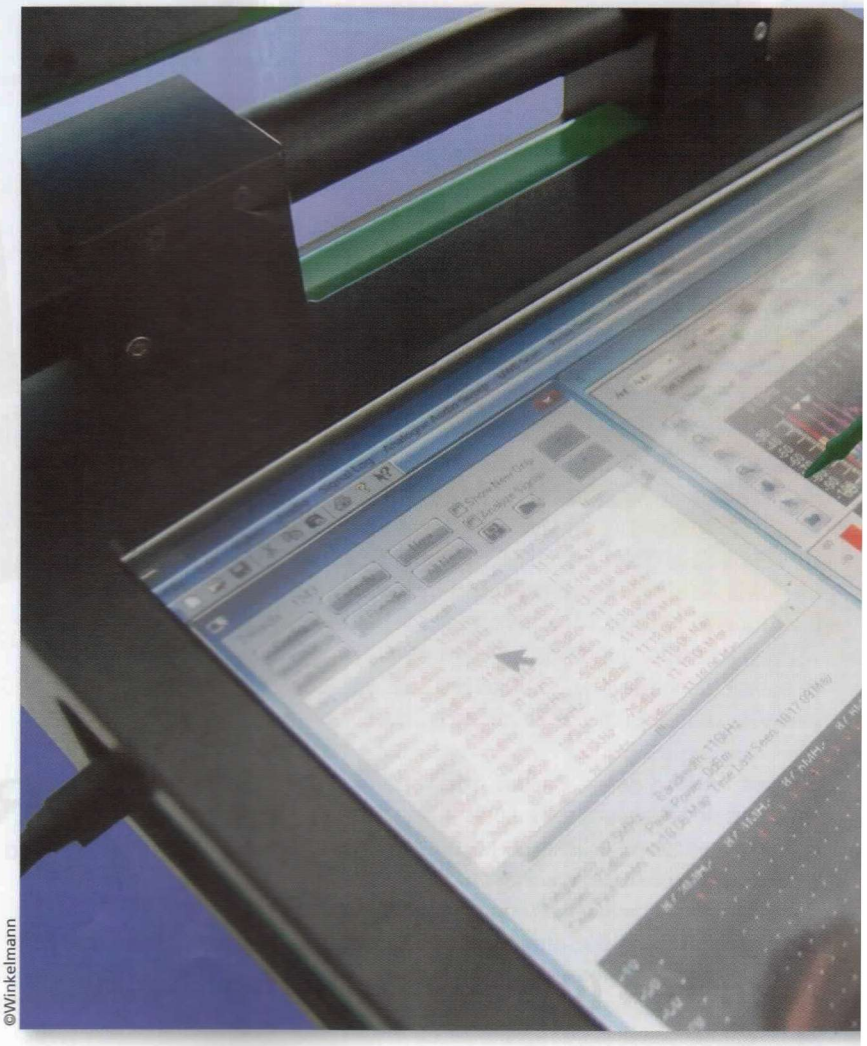
When it comes to espionage, the first area that all prospective service users must understand is that of threat. Very often I hear the phrase: "We just need a quick check; our threat is commercial not governmental". This is the first mistake, and a mistake that knocks on throughout the provision of service. A commercial threat would intimate that the level of attack against an organisation or individual would consist of amateur or semi-professional persons who only have access to commercially available hardware with which to mount an attack. This is just not the case.

The reality of today's commercial threat is that former government-trained individuals are operating in a commercial capacity, using highly sophisticated techniques and equipment. The motive and model for any attack is based on reward. Take, for example, an organisation which has as its target a competitor's contract information for a £5m contract. If their aim is to use this information to obtain the contract itself, then an investment of ten per cent of the profit of this contract would be a worthwhile investment. If the profit was £2m, then £200,000 would pay for the very best government standard black market devices and the services of criminal operators trained to Special Forces or government standards in disciplines such as covert method of entry and covert installation. Even in some high-profile divorce cases, I have seen highly sophisticated attacks and devices usually only seen in covert military and law enforcement operations. And let's not forget that international espionage by foreign intelligence services does not just target other nations' intelligence services. Foreign industry is and always will be a viable target.

With that in mind, it is imperative that any service provider be of the very highest standard that can be afforded. Investment in a professional TSCM team is an investment in the protection of current and future strategic and operational business processes.

The vast majority of commercial organisations ignore the threat of technical surveillance, however. Instead, they invest large information security budgets in IT security and fail to secure their information from even the most basic of technical surveillance attack. As an example, imagine – even with all of your firewalls and IT protection systems – a £50 device installed inside a keyboard will transmit all keystrokes to an attacker, giving them access to every keystroke made, including usernames and passwords. An infected mobile phone in your working area will give access to all your calls, text messages and emails, and allow the attacker to listen in to your conversations. Similarly, an audio transmitter or recorder in your boardroom can relay crystal clear audio of your most sensitive meeting to an attacker

Raptor reaction: operators should be using the latest equipment to hunt down the latest surveillance technology



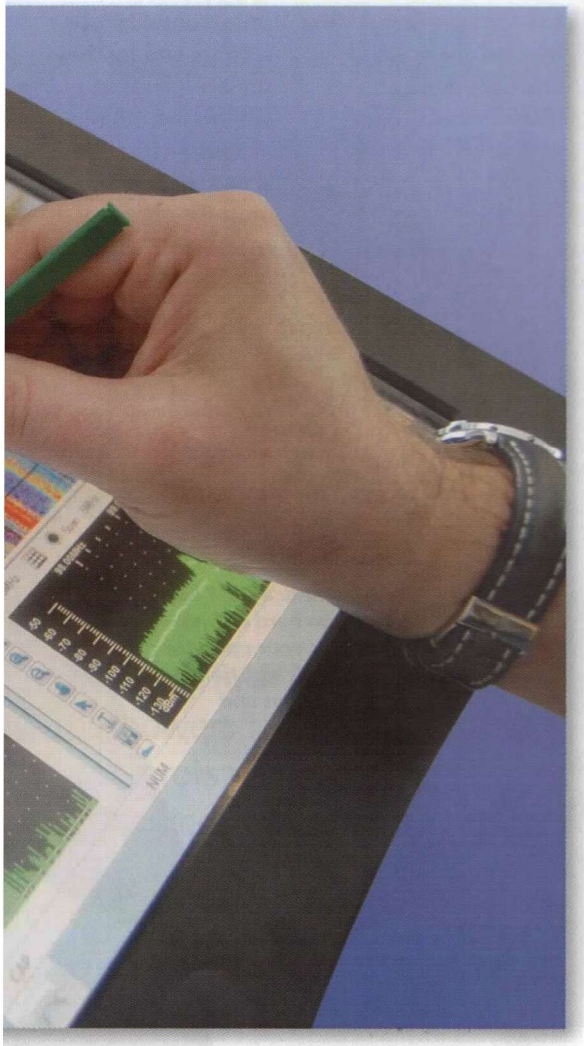
©Winkelmann

at the other side of the world. A tracker the size of a match box can give live information of your location and audio of your conversations to an attacker interested in who your meeting with and where.

The current global standards of TSCM operators are no better or worse than those faced by any other service-based industry. There are extremely professional operators and conversely there are out-and-out rogue traders, and even some who will work for criminal elements themselves and mount attacks on you while in the trusted position of securing your business. So how can you tell the professional from the "wand waving" types who will take your money and leave you in a worse security situation than when you hired them?

The first consideration should be your perceived threat. What is it you are trying to protect and from who? Too many companies do not consider these factors before they make initial contact with TSCM providers. Is the threat specific or general? Do you have a specific event, meeting or area you wish to protect or check? Who would want to attack you and why? If the threat is general, then you should undertake contracted TSCM services as part of your overall information security and risk management strategy. These decisions will allow you to narrow your service requirement and lessen the area of concern to be able to budget for a better standard of service.

It is not always a good idea to take recommendations from colleagues. There have been many cases of less-professional TSCM operators being able to network their services as they are



TSCM operator checklist

- **Make enquiries about experience and training.**

Your technical surveillance countermeasures service provider should be able to furnish proof of TSCM training at one of the few recognised training institutions in the world.

- **Make enquiries about the equipment utilised for the survey**

The equipment should at a minimum include the following instruments and tests:

- An Orion or Hawk Non-Linear Junction Detector (NLJD) to detect active or passive electronic circuitry that may be hidden in walls, furniture artefacts, etc.
- A spectrum analyser or hybrid counter-surveillance receiver such as the OSCOR or Raptor RXI with a sweep capability above the traditional ceiling of 6GHz.
- Telephone line analysers, the appropriate software programmes and other equipment capable of analysing electronic, digital and VoIP telephones and lines.
- Specialised amplifiers, wire-tracing devices, multi-meters, sound activating and masking sources, multi-meters, light sources and a good stepladder.
- Security marking equipment, pens, etc.

- **Do they offer reports, analysis and recommendations?**

On completion of the survey, a report should be submitted detailing the tests conducted and the findings of the survey. The report should include a record of the signals found and analysed, telephone voltages and measurements obtained as well as other electronic and energy signals detected and evaluated.

- **Do they provide a certificate of quality?**

The service provider should carry calibration certificates or a certificate of quality regarding the equipment they use during a survey on your premises. This certificate issued by the manufacturer of the equipment or its representative should state the following:

- The equipment is of the latest generation software and version.
- It is in proper calibration and operating procedures as defined by the manufacturer's specifications and factory standards.
- It has been tested at the manufacturer or its authorised representative's facility within the past 12 to 18 months.

This is necessary to prevent your premises being checked with old and outdated equipment.

- **Other things to consider**
  - Is the individual or company offering the services recognised by the industry as specialists in technical surveillance countermeasures?
  - Are they prepared to have their findings verified?
  - Will they testify in court on your behalf?
  - Are they members of professional institutions dealing specifically with countermeasures and counter-intelligence, such as the Espionage Research Institute (ERI – USA) and Business Espionage Controls and Countermeasures Association (BECCA – UK)?

SWEEPING STANDARDS

likeable people who look and talk a good service to the untrained seeker of services.

A good place to start is to seek professional bodies like the Technical Surveillance Counter Measures Institute (TSCMi). Self-regulating, peer validation bodies such as this vet their members, their skills and professionalism to a level acceptable for operation, and only suitably qualified practitioners with the relevant technical, operational and ethical standards will be granted full membership. Without that kind of assurance, it is far more difficult to vet a service provider. There are a plethora of companies offering TSCM services on the Internet, making various claims and guarantees. Virtually all private investigators offer some kind of "bug sweep" service.

If you have to shop for services from the Internet or other open sources, the first question to ask is: "What equipment do you use?" This will give a good indication as to the level of professionalism of the service provider. For example, any professional organisation will have RF detection equipment to detect and locate active transmitter-based threats. The specifications for this equipment vary hugely and can be used by some as marketing gimmicks, but in essence it should scan to at least 6GHz and at least 12GHz for higher threat levels. The equipment should, for higher levels of threat, have the ability to detect mains carrier devices, frequency hopping, spread spectrum and burst transmissions and allow the operator to be able to make comparison sweeps, analyse frequencies over time and analyse the local signals and pinpoint their location to discount them as a threat. These units cost from around £6,000 to over £100,000. Winkelmann, REI, Systemware, Shearwater, Audiotel and Anritsu all make TSCM-based RF detection systems and are respected suppliers in the industry; eBay is not!

The next piece of equipment essential for a professional service is the Non-Linear Junction Detector (NLJD), a piece of equipment used to detect hidden electronics. Any professional will have an NLJD – it is the only effective way to find hidden electronics. NLJDs cost from around £4,000 to around £20,000. Some will claim they use physical search alone to find hidden electronics – this is a sure sign of an unprofessional operator, unless they can prove the power of X-ray vision (which some no doubt will).

The next equipment capability a professional service provider will have will be telephone and line analysis equipment. This is essential to detect and locate telephone and conductor-based threats such as telephone transmitters, wired microphone systems and "taps" on telephone and data conductors. This suite of equipment should have the ability to allow the user to carry out: electrical measurements, audio testing, time or frequency domain reflectometry (TDR, FDR), RF testing and line tracing as a minimum.

And last but not least, the operator must have a full physical search kit. The fact that at least all of this equipment is held by the service provider is, if nothing else, an indicator that there has been a substantial investment made in equipment. The average for a professional high-level sweep team is around £120,000 of equipment.

But equipment alone does not guarantee of a good delivery of service. The next question asked should concern the operator's training. Allowing untrained operators to carry out services is unprofessional and can be dangerous. All operators should have some kind of formal training. Bragging openly about their list of named clients is not proof of training – it is just proof that at some point in the future, your organisation will also be compromised by them bragging they're working for you.
A professional service provider will also deliver a full written report post-service which is full and detailed so as to provide evidence and guarantee of the level of service. Also check the service provider has the relevant insurance, professional indemnity and public liability.

The last point in selecting a professional TSCM service provider is probably the most controversial in the industry and involves control testing – the means of testing a TSCM service provider to ensure they are capable of detecting and locating hostile technical surveillance attacks. This should be welcomed by the service provider; let's face it, if they are not willing to undergo testing to prove their proficiency then how competent will they be in declaring an area clear from attack? Control tests should never be carried out during an actual operation. It is far better to arrange a control test prior to any service being undertaken. The attack used in the test should be viable – that is, it should be an effective technical surveillance attack. But beyond that, if a service provider refuses a control test or cannot find a viable control attack, then they should not be considered for any form of operational tasking.

With all of these simple criteria met, it is likely you will have a professional provider of service. But in all cases, you get what you pay for...

Gavin Saul is an independent TSCM operator, working operational, strategic and training tasks for government, law enforcement and commercial organisations in the UK and worldwide. He is security cleared, has more than ten years' experience in the private arena and is a full member of the TSCM Institute.

Steve Whitehead is the Managing Member of Eavesdropping Detection Solutions, a business division of CBIA based in South Africa. Steve specialises exclusively in risk management and corporate counterintelligence matters and teaches the disciplines at various institutions in South Africa. He is one of the world's most experienced consultants in this unique field.

©Winkelmann

Tiny find: a GSM bug can be hard to find unless your operator has the right training, equipment and experience